Aleksandar T. Lipkovski

ALGEBRAIC GEOMETRY
(Selected Topics)

Contents

0. Introduction

First version of the present text appeared as one-semester course lecture notes in algebraic geometry. The course for graduate students of mathematics, of geometrical, topological and algebraic orientation, took place in the spring semester of 1994/95, and was organized on the initiative of Z. Marković, head of Mathematical Institute in Belgrade, with great support from my colleagues from the Belgrade GTA Seminar[1], especially R. Živaljević and S. Vrećica.

I had a difficult task. In a short course one should have reached some relevant topics of algebraic geometry. Basics of algebraic geometry require an ample preliminary material, mostly from commutative algebra, homological algebra and topology. I tried to avoid this and to include only a minimal amount of such material. Consequently, the style of writing is laconic, with many references to existing (excellent) textbooks in algebraic geometry, but on the other side, it is consistent, in order to be readable, with some effort of course. The scope of the course should include some of the interesting and important results in algebraic geometry. Two such results are included, both classical but very important: the 27 lines on a cubic surface and the Riemann–Roch theorem for curves. I leave to the reader to judge, whether my task has been solved, and to which extent.

The present text could serve different purposes. It could be used as an introduction for nonspecialists, who would like to understand what is going on in algebraic geometry, but are not willing to read long textbooks. It could also be used as a digest for students, who are preparing to take a serious course in algebraic geometry. Nowadays, algebraic geometry became an indispensable tool in many closely related or even far standing disciplines, such as theoretical physics, combinatorics and many others. Specialists in these fields may also find this text useful.

1. Rational algebraic curves

In the course of Calculus one evaluates indefinite integrals of the form

$$\int R(x, \sqrt{ax^2 + bx + c})dx \tag{1}$$

Supported by Ministry of Science and Technology of Serbia, grant number 04M03/C

[1] GTA stands for: Geometry, Topology, Algebra

where $R(x, y)$ is a rational function with two arguments. These are the simplest integrals with so called quadratic irrationalities. Some readers remember that these integrals are being calculated with the help of so-called Euler substitutions. There are three such substitutions (the types are not distinct):

Type I. If $a > 0$, one puts $\sqrt{ax^2 + bx + c} = t - \sqrt{a}x$

Type II. If $c > 0$, one puts $\sqrt{ax^2 + bx + c} = xt + \sqrt{c}$

Type III. If the polynomial has real roots λ and μ, $ax^2 + bx + c = a(x - \lambda)(x - \mu)$, and we use $\sqrt{ax^2 + bx + c} = t(x - \lambda)$.

In all three cases, the differential $R(x, y)dx$ is being rationalized and the integral evaluated in elementary functions.

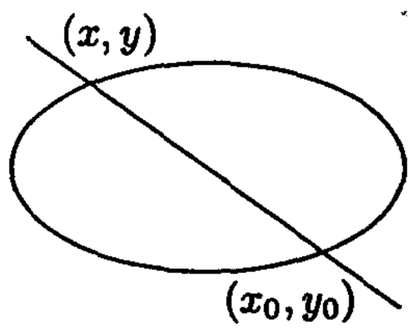
The Euler substitutions are described in traditional calculus textbooks, such as [30, p. 59]. A few students understand what is the real meaning of these substitutions. However, they have fine geometrical interpretation. Introduce the curve of second order

$$y^2 = ax^2 + bx + c \tag{2}$$

and its point (x_0, y_0). After the translation to that point, the equation of the curve is

$$(y - y_0)^2 + 2y_0(y - y_0) = a(x - x_0)^2 + 2ax_0(x - x_0) + b(x - x_0)$$

Let $y - y_0 = t(x - x_0)$ be the line through that point with variable slope t (see the figure)



The other, variable intersection point of the line and the curve (2) is obtained from the system

$$(t^2 - a)(x - x_0) = (2ax_0 + b) - 2y_0t$$
$$y - y_0 = t(x - x_0)$$

whose solution (x, y) depends rationally on t (for almost all t):

$$x = x_0 + \frac{(2ax_0 + b) - 2y_0t}{t^2 - a}$$
$$y = y_0 + t(x - x_0)$$

After substitution in the integral, one obtains rational function of argument t and the integral evaluates easily:

$$\int R(x, \sqrt{ax^2+bx+c})dx = \int R(x(t), y(t))x'(t)dt = \cdots$$

Euler substitutions can be deduced from this general algorithm by different special choices of the point (x_0, y_0).

Type III. The point $(x_0, y_0) = (\lambda, 0)$ lies on the curve and we put $y = t(x-\lambda)$.

Type II. The point $(x_0, y_0) = (0, \sqrt{c})$ lies on the curve and we put $y-\sqrt{c} = xt$.

Type I. Here the situation is slightly more complicated. In the case $a > 0$ the curve (2) is a hyperbola with asymptotic directions $(\sqrt{a}, \pm 1)$. As starting point (x_0, y_0), one takes the point at the infinity of one of these two directions. Then the lines through that point are exactly the lines $y = \sqrt{a}x + t$ parallel to the asymptote. Each of these lines intersects the curve in one more point (x, y) and we use $y = \sqrt{a}x + t$.

From previous discussion one can see that the expressibility of the integral (1) in elementary functions is based on the following specific property of the conic (2). There exist rational functions $x = \xi(t)$; $y = \eta(t)$ of one argument t such that for different parameter values t, the corresponding point $(\xi(t), \eta(t))$ lies on the curve. In this way one obtains all (but one) points of the curve. More specifically, for each point $(x, y) \neq (x_0, y_0)$ on the curve (2) it is sufficient to draw a line through (x_0, y_0) with the slope $t = (y-y_0)/(x-x_0)$. We say that in such case curve (2) has rational parametrization. One can easily show that every plane curve of second order has a rational parametrization. Such curves have been called *unicursal*. Today one rather uses the term *rational curves*.

Let us now apply the above principle of evaluation of the integral (1) with irrationalities of the type $\sqrt{P(x)}$ where $P(x)$ is a polynomial of degree greater than 2. In this case, along with the integral

$$\int R(x, \sqrt{P(x)})dx \tag{3}$$

one should consider the curve

$$y^2 = P(x) \tag{4}$$

Here we have different behavior. Some of the curves (4) do admit rational parametrization, and some of them do not.

Examples. 1. It is obvious that the curve $y^2 = x^3$ has rational parametrization (which one?).

2. The curve $y^2 = x^3 + x^2$ also has rational parametrization $x = t^2 - 1$, $y = t(t^2-1)$, It is obtained when one finds the intersection points of the curve and the lines $y = tx$ through $(0, 0)$.

3. The curve $y^2 = x^3 + ax^2 + bx + c$ has rational parametrization if and only if the polynomial $x^3 + ax^2 + bx + c$ has multiple root.

When rational parametrization of the curve (4) exists, the integral (3) could be transformed into integral of rational function. How one evaluates the integral when there is no such parametrization? Interesting and complicated theory is obtained already when degree of the polynomial $P(x)$ equals 3 or 4. It is sufficient to consider only the latter case, since degree 3 could be transformed to degree 4 by rational transformations.

Example. For a given curve

$$y^2 = x^3 + ax^2 + bx + c \tag{5}$$

the right-hand side polynomial of degree 3 has at least one real root. Applying the translation along x axis one could make this root 0 i.e., one could put $c = 0$. After substitution $y = tx$ we get

$$x^2 + (a - t^2)x + b = 0$$

$$\left(x + \frac{a - t^2}{2}\right)^2 + b - \left(\frac{a - t^2}{2}\right)^2 = 0$$

The rational parametrization

$$x = u - \frac{a - t^2}{2} \quad y = t\left(u - \frac{a - t^2}{2}\right) \tag{6}$$

transforms the curve (5) in the curve of degree 4 with equation

$$u^2 = \frac{1}{4}t^4 - at^2 + \left(\frac{a^2}{4} - b\right)$$

The parametrization (6) is rationally invertible — it has a rational inverse

$$t = \frac{y}{x}, \quad u = x + \frac{a - (y/x)^2}{2}$$

This is a very important fact, as we will see later.

2. Plane algebraic curves. Polynomials in many variables

Now we should make the term "plane algebraic curve" more precise. Let K be field, so-called ground field, and $K[x, y]$ polynomial ring in two variables with coefficients in K.

Definition. Plane algebraic curve in the affine plane $K^2 = \mathbb{A}^2_K$ is the set of points in the plane defined by algebraic polynomial equation

$$X = \{(x, y) \in K^2 \mid f(x, y) = 0\}$$

where $f(x,y) \in K[x,y]$. This set is denoted $X = V(f)$.

Even such simple definition leads to several problems. Naturally, one would like to establish a one-to-one correspondence between sets and their equations. However, already in the real analytic geometry there exist examples where basically different equations define the same set, or equations define sets that seem unnatural to call "curves". So, in the real plane, equations $x = 0$ and $x^2 = 0$ define the x-axis, equations $x^2 + y^2 = 0$, $(x^2 + y^2)^2 = 0$ and $x^6 + y^4 = 0$ define the point $(0,0)$, and equation $x^2 + y^2 + 1 = 0$ defines the empty set. Immediately, two questions arise:

first, how to treat objects which are produced by this definition but do not agree with our intuitive notion of "curve";

second, in which extent is the set $X = V(f)$ determined by the polynomial f and how to modify the definition in order to get one-to-one correspondence.

These problems are present already in the course of analytical geometry for first-year undergraduates. Problem with curves which "are not curves" is being bypassed by calling them "degenerate", etc. The question, in which extent is equation determined by the set of points, is usually not treated at all. The first problem can be easily solved: one should consider complex numbers instead of real ones. This is known as the *complexification process*. In the general case, one should take the algebraic closure of the given field. The "empty" curves like $V(x^2 + y^2 + 1)$ then disappear. In the sequel the ground field Kwill always be algebraically closed, unless the opposite is explicitly stated. Usually, it will be the field of complex numbers $\mathbb{C}$.

As to the second problem, it is being answered by the following fact, known as Study's lemma[2]. Note that when polynomial f divides polynomial g, then $g = fh$ and every root of $f$is at the same time the root of g, that is $V(f) \subset V(g)$. In the case of algebraically closed field the converse is also true.

Lemma. *Let K be algebraically closed field and $f(x,y) \in K[x,y]$ irreducible polynomial. If the polynomial $g(x,y) \in K[x,y]$ has a zero in every point of the curve $X = V(f)$ (i.e., if $V(f) \subset V(g)$), then f divides g.*

Proof. Let $g \neq 0$ (in the opposite, f divides g). Then also $f \neq 0$. If f is constant, then f divides g. Suppose f is not constant, but an actual polynomial, say in y: $f(x,y) = a_0(x)y^n + \cdots \in (K[x])[y]$ with $a_0 \neq 0$, $n > 0$. Let us show that g is then also an actual polynomial in y. If $g = g(x) \in K[x]$, then $0 \neq a_0 g = a_0(x)g(x) \in K[x]$ and there should exist $\xi \in K$ such that $a_0(\xi)g(\xi) \neq 0$. Since K is algebraically closed, there exists $\eta \in K$ such that $f(\xi,\eta) = 0$, which is a contradiction to the choice of ξ. Therefore, $g(x,y) = b_0(x)y^m + \cdots \in (K[x])[y]$ with $b_0 \neq 0$, $m > 0$.

Let now $R = R(f,g) \in K[x]$ be the resultant of polynomials f and g with respect to y. Let $\xi \in K$ be such that $a_0(\xi) \neq 0$. Since K is algebraically closed, there exists $\eta \in K$ such that $f(\xi,\eta) = 0$. Then also $g(\xi,\eta) = 0$ and therefore $R(\xi) = 0$. In such way, $a_0 R = 0 \in K[x]$. Since $a_0 \neq 0$, it must be $R = 0$, which

[2]Eduard Study (1862–1930), German geometer (Fubini–Study metric in projective space)

means that f and g have a nontrivial common factor. However, f is irreducible and therefore f must divide g.

Corollary. *Irreducible factors of curve's equation are determined uniquely (up to ordering). If $f = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ is a factorization in irreducible factors, then $V(f) = V(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}) = V(p_1 p_2 \dots p_k)$.*

This proof can easily be generalized for more than two variables.

We see that in the case of algebraically closed field, one of all possible equations of a given curve is determined uniquely by the condition that it has no multiple factors i.e., it is reduced.

Study's lemma is a special case of a very important theorem, which could be considered also as a generalization of the main theorem of algebra. It is a famous Hilbert's[3] Nullstellensatz, which in its classical version states that "nontrivial" system of algebraic equations over an algebraically closed field always has a solution. Here "nontrivial" means that it is not possible to algebraically deduce a contradiction from the system. More precisely:

If the field $K$is algebraically closed and $f_1, \dots, f_k \in K[x_1, \dots, x_n]$ are polynomials in n variables such that there are no polynomials $g_1, \dots, g_k \in K[x_1, \dots, x_n]$ for which it would be $g_1 f_1 + \dots + g_k f_k = 1$, then the system of algebraic equations

$$f_1(x_1, \dots, x_n) = 0$$
$$\dots$$
$$f_k(x_1, \dots, x_n) = 0$$

has a solution.

It is known that polynomial ring in one variable over a field is a PID (principal ideal domain): it is even Euclidean. This is a consequence of the existence of Euclidean gcd division algorithm. However, in polynomial rings in two variables this is no more true. For instance, ideal (x, y) cannot be generated by single polynomial. However, in 1868 Gordan[4] proved that it is possible to find a finite generating set of polynomials in every ideal. His proof was constructive – he described a construction of such basis. Many mathematicians tried to generalize Gordan's construction to the case of more than two variables, but nobody could overcome computing difficulties, and for twenty years this problem, known as Gordan's problem, remained open. In 1888 Hilbert proved in his famous basis theorem that every ideal in the polynomial ring with n variables has a finite basis. His proof was existential, not constructive. It has been said that Gordan, after he saw Hilbert's proof, said: "Das ist nicht Mathematik. Das ist Theologie!"[5]. Only when later Hilbert found a constructive proof, Gordan was satisfied and said that theology has its merits. Only after this, existential proofs in mathematics became legitimate.

---

[3] David Hilbert (1862–1943), German mathematician. Most famous for his list of problems for 20. century

[4] Paul Albert Gordan (1837–1912), German mathematician

[5] "This is not mathematics. This is theology!"

The notion of resultant was used in the proof of Study's lemma. Let us briefly describe it here.

Let A be a UFD (unique factorization domain, factorial ring), say polynomial ring over a field, and let $f, g \in A[x]$ be two polynomials with coefficients in A, $f = a_0x^m + \cdots + a_m$, $g = b_0x^n + \cdots + b_n$ (we allow also the possibility $a_0, b_0 = 0$). Since $A[x]$ is also a UFD, we are interested in their common divisors. The definition of a common divisor easily leads to the following lemma.

Lemma. *Polynomials f and g have nontrivial common divisor $\Leftrightarrow$ there exist polynomials $u, v \in A[x]$, $u, v \neq 0$ such that $\deg u < \deg f$, $\deg v < \deg g$ and $vf = ug$.*

If one writes this condition explicitly, one has $u = c_0x^{m-1} + \cdots + c_{m-1}$, $v = d_0x^{n-1} + \cdots + d_{n-1}$ and from equality $vf = ug$ one deduces

$$\sum_{i=0}^{m} a_ix^{m-i} \cdot \sum_{j=0}^{n-1} d_jx^{n-j-1} - \sum_{i=0}^{n} b_ix^{n-i} \cdot \sum_{j=0}^{m-1} c_jx^{m-j-1} = \cdots$$

$$= \sum_{k=0}^{m+n-1} \sum_{i+j=k} (a_id_j - b_ic_j)x^{(m+n-1)-k} = 0$$

and comparing the coefficients for x one obtains system of $m+n$ linear equations

$$\sum_{i+j=k} (a_id_j - b_ic_j) = 0 \quad (k = 0, \ldots, m+n-1)$$

or explicitly

$$\begin{array}{rrrrrrrrr}
a_0d_0 & & & & -b_0c_0 & & & & = 0 \\
a_1d_0 & +a_0d_1 & & & -b_1c_0 & & -b_0c_1 & & = 0 \\
\multicolumn{9}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\
a_md_0 & & & & & & & -b_1c_{m-1} & = 0 \\
& & a_0d_{n-1} & & -b_{n-1}c_0 & & & & = 0 \\
& & a_1d_{n-1} & & -b_nc_0 & & & & = 0 \\
\multicolumn{9}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\
& & & & a_md_{n-1} & & & -b_nc_{m-1} & = 0
\end{array}$$

with $m+n$ indeterminates $c_0, \ldots c_{m-1}, d_0, \ldots, d_{n-1}$. This system has nontrivial solution if and only if its determinant equals 0.

Definition. Determinant of this system, i.e., the determinant

$$R(f,g) = \left|\begin{array}{ccccccc}
a_0 & a_1 & \ldots & a_m & & & \\
 & a_0 & a_1 & \ldots & a_m & & \\
 & & & & \ldots & & \\
 & & & a_0 & a_1 & \ldots & a_m \\
b_0 & b_1 & \ldots & b_n & & & \\
 & b_0 & b_1 & \ldots & b_n & & \\
 & & & & \ldots & & \\
 & & & b_0 & b_1 & \ldots & b_n
\end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} n \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} m \end{array}$$

is called *resultant* of polynomials f, g with respect to x.

The resultant is a polynomial in coefficients a_i and b_j of degree $m+n$, homogeneous in each group of indeterminates. Preceding discussion proved the following theorem.

Theorem. *Polynomials f and g have nontrivial common divisor if anf only if $R(f,g)=0$.*

Applications. 1. Solution of systems with two polynomial equations. Let $f,g \in K[x,y] = (K[x])[y]$ be two polynomials and $R(f,g) = R(x) \in K[x]$. If (x_0,y_0) is a solution of the system

$$f(x,y)=0, \quad g(x,y)=0$$

then $R(x_0)=0$. One consequence is, if the system has infinitely many solutions, then polynomials f and g have a nontrivial common divisor $h=\gcd(f,g)$ and the ideal $(f,g)=(h)$ is principal.

2. Parameter elimination. Suppose curve X is described by its rational parametrization

$$x = P_1(t)/Q_1(t)$$
$$y = P_2(t)/Q_2(t)$$

Let $f(x,t)=P_1(t)-Q_1(t)x$, $g(y,t)=P_2(t)-Q_2(t)y$ and let $R=R(f,g)\in K[x,y]$ be the resultant of these polynomials. Then

$$(x_0,y_0)\in X \Leftrightarrow \exists t_0 : f(x_0,t_0)=g(y_0,t_0)=0 \Leftrightarrow R(x_0,y_0)=0$$

This means that the equation of X is $R(x,y)=0$.

Example. Find the equation of the curve that has a parametrization $x=t^2$, $y=t^3-t$. Here $f=t^2-x$, $g=t^3-t-y$ and

$$R(f,g)=\begin{vmatrix} 1 & 0 & -x & 0 & 0 \\ 0 & 1 & 0 & -x & 0 \\ 0 & 0 & 1 & 0 & -x \\ 1 & 0 & -1 & -y & 0 \\ 0 & 1 & 0 & -1 & -y \end{vmatrix} = y^2-x^3+2x^2-x$$

Therefore, the equation of X is $y^2=x^3-2x^2+x$. One could obtain it also without use of the resultant, but the present method is generally applicable.

3. Transcendence degree. Hilbert's Nullstellensatz

Let K be a field and L its extension. Subset $S\subset K$ is *algebraically independent* over K if there is no polynomial relation between elements in S, i.e., if there is no polynomial $f\in K[x_1,\dots,x_n]$ such that $f(c_1,\dots,c_n)=0$ for some

$c_1, \dots, c_n \in S$. Family of algebraically independent sets is ordered by inclusion. Maximal elements of this family i.e., maximal algebraically independent sets are called *transcendence bases* of L over K. For example, in the field of rational functions $K(x_1, \dots, x_n)$ the set $\{x_1, \dots, x_n\}$ is one of its transcendence bases over K. Note that, if S is a transcendence basis of L over K, then L is algebraic over $K(S)$. Main statements about transcendence bases are analogous to corresponding statements about (linear) bases in vector spaces over fields.

Theorem. *A. Let L be the field generated over K by the set M and let $N \subset M$ be its algebraically independent subset. There exists a transcendence basis B between N and M. In other words, algebraically independent set can be extended to transcendence basis by adding elements from a given generating set.*

Theorem. *B. Every two transcendence bases of the field L over K have the same cardinality.*

Cardinality of any (and every) transcendence basis of L over K is called *transcendence degree* of that field extension.

Our next goal is to prove Hilbert's Nullstellensatz. That will be done in few steps.

Step 1. Let K be algebraically closed and L its finitely generated extension. There exist elements $z_1, \dots, z_{d+1}$ in L such that

1. they generate L over K,
2. $z_1, \dots, z_d$ are algebraically independent,
3. z_{d+1} is algebraic over $K(z_1, \dots, z_d)$.

Proof. Follows from the known theorem on the primitive element.

Step 2. Let K be algebraically closed field and $F_1, \dots, F_m \in K[t_1, \dots, t_n]$ polynomials. If the system of equations $F_1 = 0, \dots, F_m = 0$ has a solution in finitely generated extension L over K, then it has a solution in K also.

Proof. L is of the form $L = K(x_1, \dots, x_r, \eta)$ where $x_1, \dots, x_r$ are algebraically independent over K and η is algebraic over $K(x_1, \dots, x_r)$. Let $F(x_1, \dots, x_r, y) \in K(x_1, \dots, x_r)[y]$ be the minimal polynomial of η. Let now $(\xi_1, \dots, \xi_n)$ be the solution of the system in L^n. One has $\xi_i = C_i(x_1, \dots, x_r, \eta)$ for some polynomials $C_i(x_1, \dots, x_r, y) \in K(x_1, \dots, x_r)[y]$. Since F is minimal, there exist polynomials Q_i such that

$$F_i(C_1(x_1, \dots, x_r, y), \dots, C_n(x_1, \dots, x_r, y)) = F(x_1, \dots, x_r, y)Q_i(x_1, \dots, x_r, y)$$

identically with respect to $x_1, \dots, x_r, y$. Since K is infinite, there exist elements $\alpha_1, \dots, \alpha_n \in K$ such that all denominators in coefficients of polynomials $F, Q_1, \dots, Q_r, C_1, \dots, C_n \in K(x_1, \dots, x_r)[y]$ and also the highest order coefficient of polynomial F are different from 0 after substitution $x_i = \alpha_i$. Since K is algebraically closed, there exists $\beta \in K$ such that $F(\alpha_1, \dots, \alpha_r, \beta) = 0$. Then $\gamma_i = C_i(\alpha_1, \dots, \alpha_r, \beta)$ is the solution in K^n.

Step 3. If polynomials $F_1, \dots, F_m \in K[t_1, \dots, t_n]$ do not generate the unit ideal, then the system $F_1 = 0, \dots, F_m = 0$ has a solution in the field K.

Proof. Ideal $(F_1, \dots, F_m)$ is contained in some maximal ideal M. Therefore the quotient $L = K[t_1, \dots, t_n]/M$ is a field. Let the image of t_i in L be ξ_i. Obviously, $L = K(\xi_1, \dots, \xi_n)$ and $(\xi_1, \dots, \xi_n)$ is a solution of our system in the field L. According to Step 2, there exists a solution in K.

Step 4. If the polynomial G equals zero in all zero-points in K^n of polynomials $F_1, \dots, F_m$, then for some r, $G^r \in (F_1, \dots, F_m)$.

Proof. Introduce a new variable u and consider polynomials $F_1, \dots, F_m$, $uG - 1$ in the polynomial ring $K[t_1, \dots, t_n, u]$. According to assumption, they do not have common roots in K, and therefore (Step 3) generate the unit ideal: there exist polynomials $P_1, \dots, P_m, Q \in K[t_1, \dots, t_n, u]$ such that $P_1F_1 + \dots + P_mF_m + Q(uG-1) = 1$. This identity remains true after the substitution $u = 1/G$. Eliminating the denominator, one obtains the necessary statement. This proves the Hilbert's Nullstellensatz.

4. Algebraic sets and polynomial ideals

Definition of algebraic sets in higher dimensional space generalizes the notion of plane algebraic curves. Intuitively, algebraic set is a solution set of system of polynomial equations: If $f_1, \dots, f_m \in K[x_1, \dots, x_n]$, the set $V(f_1, \dots, f_m) = \{x \in K^n \mid f_1(x) = \dots = f_m(x) = 0\}$ of solutions of the system $f_1(x) = \dots = f_m(x) = 0$ is called *algebraic set* in the affine space K^n. For $m = 1$ (one equation), the corresponding set $V(f)$ is called *hypersurface.*

Even for plane algebraic curves it was not easy to establish a one-to-one correspondence between solution sets and equations: different equations could represent the same algebraic set. Instead of systems, let us consider their left-hand sides, that is, finite sets of polynomials. Instead of finite sets, it is useful to consider arbitrary sets of polynomials.

We shall use the notations $A = K[x_1, \dots, x_n]$ for ground polynomial ring and $X = K^n = \mathbb{A}^n_K$ for ambient affine point space in the whole section.

Definition. For any subset $S \subset K[x_1, \dots, x_n]$, algebraic set in X defined by S is the set $V(S) = \{\xi = (\xi_1, \dots, \xi_n) \in X \mid \forall f \in S,\ f(\xi) = 0\} \subset X$.

In this way one obtains the correspondence between subsets in A and subsets in X, that is, the mapping of partitive sets $V : \mathcal{P}(A) \to \mathcal{P}(X)$. Let us establish its elementary properties.

Lemma 1. *(a)* $S \subset T \Rightarrow V(T) \subset V(S)$ *(more equations, less solutions).*

(b) $V(\emptyset) = X$, $V(A) = \emptyset$. *(c)* $V(S_1 \cup S_2) = V(S_1) \cap V(S_2)$.

(d) $V(f_1, \dots, f_m) = V(f_1) \cap \dots \cap V(f_m)$ *(every algebraic set is the intersection of hypersurfaces).*

One can easily show that even for arbitrary unions $V(\bigcup_\alpha S_\alpha) = \bigcap_\alpha V(S_\alpha)$. Does the analogous statement hold for intersections, at least for finite ones?

Lemma 2. *If $I = (S)$ is the ideal generated by $S \subseteq A$, then $V(S) = V(I)$.*

According to the Hilbert basis theorem, the ring A is Noetherian, $I = (f_1, \dots, f_m)$ and $V(S) = V(I) = V(f_1, \dots, f_m)$. Therefore, every set $V(S)$ is algebraic set, described by finite set of equation.

One sees, that the mapping V defines (anti)epimorphism of partially ordered sets

$$V : \text{ideals in} A \to \text{algebraic sets in } X$$

When do the different ideals define the same algebraic set? Here the main role is played by the Hilbert's Nullstellensatz. It could be stated in the following manner:

$$\text{if } V(I) = \emptyset, \text{ then } I = A$$

and its generalized form:

$$\text{if } V(I) \subset V(f), \text{ then } f \in \sqrt{I}$$

Here $\sqrt{I} = \operatorname{Rad} I = \{a \in A \,|\, \exists r > 0 : a^r \in I\} \subset A$ is the *radical* of the ideal I. Construction of radical of a given ideal is possible in every commutative ring and has the following main properties, which could be easily proved.

Lemma 3. *(a) $\sqrt{I}$ is ideal in A; (b) $I \subset J \Rightarrow \sqrt{I} \subset \sqrt{J}$; (c) $I \subset \sqrt{I}$; (d) $\sqrt{\sqrt{I}} = \sqrt{I}$.*

Proposition. $V(I) = V(J) \Leftrightarrow \sqrt{I} = \sqrt{J}$

Proof. The direction $\Leftarrow$ follows from the easy fact that $V(I) = V(\sqrt{I})$. Let us prove the opposite direction $\Rightarrow$. If $V(I) \subset V(J)$ and $J = (f_1, \dots, f_m)$, one has $V(I) \subset V(f_1) \cap \dots \cap V(f_m) \Rightarrow f_1, \dots, f_m \in \sqrt{I} \Rightarrow J \subset \sqrt{I} \Rightarrow \sqrt{J} \subset \sqrt{\sqrt{I}} = \sqrt{I}$. $\sqrt{I}$ is the greatest element in the family of all ideals that define the algebraic set $V(f)$. It coincides with its own radical. The ideal I is a *radical ideal*, if it coincides with its radical: $I = \sqrt{I}$. In such way, the restriction of the mapping V

$$V : \text{radical ideals in } A \to \text{algebraic sets in } X$$

becomes a bijection, that is, (anti)isomorphism of ordered sets.

Example. In the case of hypersurface $V(f)$, if one factorizes the polynomial f into irreducible factors $f = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, it is easy to see that $\sqrt{(f)} = (f_{red})$ where $f_{red} = p_1 \dots p_k$. This agrees with earlier results on equations of plane algebraic curves, and motivates the notation of radical as a root.

If one considers the mapping V restricted to ideals only, its behavior with respect to unions and intersections becomes better.

Lemma 4. *(a) $\bigcap_\alpha V(I_\alpha) = V(\bigcup_\alpha I_\alpha) = V(\sum_\alpha I_\alpha)$; (b) $V(I_1) \cup V(I_2) = V(I_1 \cap I_2) = V(I_1 I_2)$.*

Proof. (a) follows from Lemma 2. Let us now prove (b). Since for any two ideals in the ring A one has $I_1 I_2 \subset I_1 \cap I_2 \subset I_1, I_2$ and the mapping V is (anti)monotonic, $V(I_1) \cup V(I_2) \subset V(I_1 \cap I_2) \subset V(I_1 I_2)$. If $x \notin V(I_1) \cup V(I_2)$, then there exist $f_1 \in I_1, \quad f_2 \in I_2$ such that $f_1(x) \neq 0$ and $f_2(x) \neq 0$. Therefore $(f_1 f_2)(x) \neq 0$ and $x \notin V(I_1 I_2)$.

The last property extends directly to finite unions of algebraic sets.

Lemmas 1, 2 and 4 show that the family AlgSets X of all algebraic sets in X is closed with respect to finite unions and arbitrary intersections, and it contains whole X and the empty set $\emptyset$. Therefore, this family is the family of closed sets of some topology on $X = K^n = \mathbb{A}^n_K$, called *Zariski topology*. Let us have a closer look on this topology.

It follows from Lemma 1(d), that the basis of this topology is the family of complements of hypersurfaces $D(f) = X \setminus V(f)$, so called *basic* or *principal open sets*. This indicates that the Zariski topology is very coarse: open sets are unions of complements of hypersurfaces.

For $n = 1$ the set $V(f)$ is finite, since it is the zero set of a polynomial in one variable. Therefore, in addition to the whole space and the empty set, closed sets in K^1 are only finite sets of points.

Finite sets are closed also for $n = 2$. Are there other closed sets? If the set $V(f_1, \dots, f_m)$ is not finite, it follows from Study's lemma that polynomials $f_1, \dots, f_m$ have nontrivial gcd h, therefore $f_i = h g_i$ and $V(f_1, \dots, f_m) = V(h) \cup V(g_1, \dots, g_m)$. The set $V(g_1, \dots, g_m)$ is finite, and $V(h)$ is a plane algebraic curve. In this way, closed sets are finite sets of points, plane algebraic curves and their unions.

The Zariski topology is compact, in the sense that every open covering contains a finite subcovering. If $\emptyset = \bigcap_\alpha V(I_\alpha) = V(\bigcup_\alpha I_\alpha) = V(\sum_\alpha I_\alpha)$, then applying the Nullstellensatz and the basis theorem one has $1 = f_1 g_1 + \dots + f_k g_k$ for some $f_i \in I_{\alpha_i}$ and therefore $\emptyset = V(I_{\alpha_1} + \dots + I_{\alpha_k}) = V(I_{\alpha_1}) \cap \dots \cap V(I_{\alpha_k})$.

One could introduce the inverse operation for V. If $Y \subset X$ is a subset, consider the set of all polynomials that are "annihilated" on this set:

$$I(Y) = \{f \in A \,|\, \forall x \in Y,\ f(x) = 0\}$$

It is easy to check the main properties of this operation.

Lemma 5. *(a) $I(Y)$ is ideal in A; (b) $Y \subset Z \Rightarrow I(Z) \subset I(Y)$; (c) $I(\emptyset) = A$, $I(X) = (0)$.*

Proposition. *(a) $J \subset I(V(J)) = \sqrt{J}$ for every ideal J in A;*
(b) $Y \subset V(I(Y)) = \overline{Y}$ for any subset Y in X (closure in the Zariski topology).

In this way, we obtained the mapping

$$I : \text{algebraic sets in } X \to \text{radical ideals in } A$$

as an inverse to the mapping V.

First step in classification of closed algebraic sets is the attempt to represent them as unions of simpler subsets. Lemma 4(b) shows that this is connected with product of ideals. It is known that, in a Noetherian ring, every ideal can be represented as a product of primary ideals, and every radical ideal as a product of prime ideals. This is a generalization of the factorization theorem for polynomials, and it is equivalent to it in the case of principal ideals:

$$\sqrt{(f)} = \sqrt{(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m})} = (p_1 p_2 \dots p_m) = (p_1)(p_2)\dots(p_m)$$

An arbitrary ideal I is *primary* if $ab \in I \wedge a \notin I \Rightarrow b \in \sqrt{I}$ and *prime* if $ab \in I \Rightarrow a \in I \vee b \in I$. Every prime ideal is radical. Decomposition of radical ideal in the product of primes is connected with decomposition of algebraic sets in intersection of irreducible ones:

Definition. Algebraic set $Y \subset X$ is *irreducible* if it can not be represented as union $Y = Y_1 \cup Y_2$ of two its proper algebraic subsets $Y_1, Y_2 \subset Y$, $Y_1, Y_2 \neq Y$.

Proposition. *Algebraic set Y is irreducible $\Leftrightarrow$ ideal $I(Y)$ is prime.*

Proof. If $Y = Y_1 \cup Y_2$ where $Y_i \neq Y$, then $\exists f_i \in I(Y_i) \setminus I(Y)$. However, $I(Y) = I(Y_1)I(Y_2)$ and $f_1 f_2 \in I(Y)$, so the ideal $I(Y)$ is not prime. Conversely, if this ideal is not prime, then $\exists f_i \notin I(Y)$ such that $f_1 f_2 \in I(Y)$. Let $I_i = I(Y) + (f_i)$ be ideals and $Y_i = V(I_i) = Y \cap V(f_i)$ corresponding closed sets $(i = 1, 2)$. Then $Y = Y_1 \cup Y_2$ is a nontrivial decomposition, since

$$x \in Y \Rightarrow (f_1 f_2)(x) = 0 \Rightarrow f_1(x) = 0 \vee f_2(x) = 0 \Rightarrow x \in Y_1 \vee x \in Y_2$$

Proposition. *Every algebraic set can be decomposed in finite union of irreducible algebraic sets $Y = Y_1 \cup \dots \cup Y_k$, where $Y_i \not\subset Y_j$ for $i \neq j$. Such representation is determined uniquely (up to permutation).*

Mapping V defines a bijection between prime ideals and irreducible algebraic sets

$$V : \text{prime ideals in } A \to \text{irreducible algebraic sets in } X$$

Set of all prime ideals in commutative ring A is called (prime) *spectrum* of the ring A and denoted $\operatorname{Spec} A$.

This (anti)isomorphism of ordered sets sends minimal irreducible algebraic sets in X (thus points) to maximal elements of the set $\operatorname{Spec} A$ (thus maximal ideals in the ring A). Recall that the ideal of the ring A is *maximal* if it is not contained in any proper ideal except itself, that is, if it is a maximal element in the set of all proper ideals in A. One has $V(I) = \{\xi\} = \{(\xi_1, \dots, \xi_n)\} \Leftrightarrow I = (x_1 - \xi_1, \dots, x_n - \xi_n) \Leftrightarrow I \subset A$ is maximal. We obtained a bijection

$$V : \text{maximal ideals in } A \to \text{points in } X$$

The set of all maximal ideals in the commutative ring A is called *maximal spectrum* and denoted $\operatorname{Max} A$ or $\operatorname{Specm} A$. One could identify $X \cong \operatorname{Max} A$, at least as

sets of points. However, the meaning of this identification is much deeper than simple bijection of sets, which becomes visible in the general theory of schemes. On the base of maximal (or prime) spectrum of the ring one could recover the full geometrical structure of the corresponding algebraic set.

5. Regular functions and mappings. Rational functions. Dimension. Singularities

In the description of geometrical objects there are always natural functions on these objects[6]. For example, on vector spaces natural functions are linear functions, on topological spaces — continuous ones, on smooth manifolds — smooth functions, on complex varieties — holomorphic ones. What are the natural functions on algebraic sets? By analogy with other geometrical objects, it should be polynomial or rational functions. Such "naive" definition should be made more precise.

Let us start with polynomial functions. Let $V \subset X$ be algebraic set and $I \subset A$ corresponding radical ideal.

Definition. The function $f : V \to K$ is a polynomial or regular function on V if it is defined by a polynomial, that is, if there is a polynomial $F \in A = K[x_1, \dots, x_n]$ such that $\forall x \in V$, $f(x) = F(x)$.

All polynomial functions build a ring (and a K-algebra) with respect to usual operations of addition and multiplication of functions. Since two polynomials F and G define the same function $\Leftrightarrow \forall x \in V$, $F(x) - G(x) = 0 \Leftrightarrow F - G \in I$, this ring could be identified with quotient ring A/I of the polynomial ring by the defining ideal of the algebraic set V.

Definition. The ring A/I is called ring of regular functions or coordinate ring of the algebraic set V and denoted $K[V]$.

Examples. (a) If $V = \{x\}$ is a point, its corresponding ideal M is maximal and $A/M \cong K$ is the ground field: function in a point is uniquely determined by its value. More generally, for n points, $K[V] \cong \underbrace{K \oplus \cdots \oplus K}_{n}$.

(b) For $V = X$ one has $I = (0)$ and $K[V] = A$, which is natural.

(c) If $V = V(y - x^2)$ is a parabola in the plane, its coordinate ring is isomorphic to polynomial ring in one variable, that is, to coordinate ring of a straight line: $K[V] = K[x, y]/(y - x^2) \cong K[x]$.

(d) If $V = V(y^2 - x^3)$ is a semicubic parabola (a cusp curve), one has $K[V] = K[x, y]/(y^2 - x^3) \cong K[x] + K[x] \cdot y$. This is a K-algebra without zero-divisors, generated by two elements.

The ring $K[V]$ is always a finitely generated K-algebra. Could it be characterized by pure algebraic method? Since ideal I is radical, this algebra does not contain nontrivial nilpotent elements — it is *reduced*, as one says. The converse also holds: for any finitely generated reduced algebra B there exists an algebraic

[6] It can be said that the definition of functions describes the corresponding geometrical object. This is formalized via ringed spaces — spaces with structure sheaf of rings

set V such that $K[V] \cong B$. It is enough to chose generators of B over K, that is, represent the algebra in the form $B = K[b_1, \dots, b_m]$ and consider the epimorphism from the corresponding polynomial ring $A = K[x_1, \dots, x_m] \to K[b_1, \dots, b_m] = B$, $x_i \mapsto b_i$. Its kernel I is the defining ideal for the algebraic set V. The choice of generators from the geometrical point of view corresponds to embedding of the algebraic set V into some affine space K^m and vice versa.

The properties of algebras $K[V]$ are analogous to the properties of polynomial ring. The main point is that in these rings two Hilbert's theorems hold — the basis theorem and the Nullstellensatz. These algebras are Noetherian, as quotients of Noetherian rings. The analogon of the Nullstellensatz is: if $g_1, \dots, g_m \in K[V]$ and $f \in K[V]$ are such that $f(x) = 0$ for every $x \in V$ which satisfies the system $g_1(x) = \cdots = g_m(x) = 0$, then for some r, $f^r \in (g_1, \dots, g_m) \subset K[V]$. Both theorems, as well as other properties, follow from the known properties of quotient rings, the main of which is that for any commutative ring B and its ideal I, natural epimorphism $h : B \to B/I = B'$ defines an order-preserving bijection between ideals in B/I and these ideals in B which contain I, in which radical ideals correspond to radical ideals, prime to prime ideals, maximal to maximal ideals. If J' is an ideal in B', the corresponding ideal in B is $J = h^{-1}(J') \supset I$ and one has $B/J \cong (B/I)/(J/I) = B'/J'$. Let $B = A$ be the polynomial ring, $B' = K[V]$ the coordinate ring and $I = I(V)$ the ideal of some algebraic set V. Ideal $J \supset I$ corresponds to the closed set $V(J) = W \subset V$. Ideal $J/I = I(W)/I(V)$ of algebraic subset W in algebraic set V is denoted by $I_V(W)$. Therefore, here we also have the corresponding bijections

$$\begin{aligned} \text{algebraic subsets in } V &\Leftrightarrow \text{radical ideals in } K[V] \\ \text{irreducible algebraic subsets in } V &\Leftrightarrow \text{prime ideals in } K[V] \\ \text{points in } V &\Leftrightarrow \text{maximal ideals in } K[V] \end{aligned}$$

The Zariski topology on V is induced from $X = K^n$. Its open base is also built by principal open sets $D(g) = V \setminus V(g), \quad g \in K[V]$.

Using regular functions one can define mappings which connect algebraic sets and play the role of morphisms in the corresponding category. Let $U \subset K^n$, $V \subset K^m$ be two algebraic sets and $\varphi : U \to V$ a mapping. Composition with φ defines a mapping

$$\varphi^* : \text{functions on } V \to \text{functions on } U$$

in the usual way, by the formula $\varphi^*(f) = f \circ \varphi$.

Definition. We say that φ is a *regular mapping*, if φ^* transforms regular functions into regular functions, that is, if $f \in K[V] \Rightarrow \varphi^*(f) \in K[U]$.

Proposition. *(a) φ is a regular mapping $\Leftrightarrow$ it is defined in coordinates with m regular functions, that is, there exist $f_1, \dots, f_m \in K[U]$ such that $\varphi(x) = (f_1(x), \dots, f_m(x)) \in V$ for all $x \in U$.*

(b) If φ is regular, $\varphi^* : K[V] \to K[U]$ is an algebra homomorphism.

(c) Conversely, for any algebra homomorphism $h : K[V] \to K[U]$ there is a regular mapping $\varphi : U \to V$ such that $\varphi^* = h$.

(d) The mapping

$$\begin{array}{ccc} U & & K[U] \\ \varphi\downarrow & \longmapsto & \uparrow\varphi^* \\ V & & K[V] \end{array}$$

is a contravariant functor. The category of algebraic sets and regular mappings is equivalent to the category of finitely generated K-algebras without nilpotents (so called affine K-algebras) and homomorphisms.

Proof. (a) If $y_i \in K[V]$ are coordinate functions (images of generators of polynomial ring in which the algebraic set V is defined) and $\varphi^*(y_i) = f_i \in K[U]$, then for $\forall x \in U$, i-th coordinate of the point $\varphi(x)$ is $y_i(\varphi(x)) = \varphi^*(y_i)(x) = f_i(x)$ and $\varphi(x) = (f_1(x), \dots, f_m(x))$. Conversely, if φ is a mapping of that form and $g \in K[V]$ a regular function on V, then for $\forall x \in U$, $\varphi^*(g)(x) = g(\varphi(x)) = g(f_1(x), \dots, f_m(x))$ is a polynomial function of coordinates x, that is, a regular function.

(b) is obvious.

(c) Let again $y_i \in K[V]$ be coordinate functions and $h(y_i) = f_i \in K[U]$. Define for $x \in U$, $\varphi(x) = (f_1(x), \dots, f_m(x))$ and prove that $\varphi(x) \in V$. Indeed, if $F \in I(V)$, then $F(y_1, \dots, y_m) = 0$. One has $0 = h(F(y_1, \dots, y_m)) = F(h(y_1), \dots, h(y_m)) = F(f_1, \dots, f_m)$ and $F(\varphi(x)) = h(F)(x) = 0$, and this means exactly that $\varphi(x) \in V$. For $x \in U$ and $g \in K[V]$ one has $\varphi^*(g)(x) = g(\varphi(x)) = g(f_1(x), \dots, f_m(x)) = g(h(y_1)(x), \dots, h(y_m)(x)) = h(g)(x)$ i.e., $\varphi^* = h$.

(d) This is also straightforward.

Definition. *Isomorphism of algebraic sets*[7] is isomorphism in the categorical sense, that is, a regular mapping which has inverse regular mapping. In this equivalence of categories, it corresponds to isomorphism of algebras, i.e., $U \cong V \Leftrightarrow K[U] \cong K[V]$.

Examples. 1. Projection $\varphi(x, y) = x$ is a regular mapping of the hyperbola $V = \{xy = 1\}$ in the line $\mathbb{A}^1$, but not an isomorphism (not even a set bijection). Corresponding algebras are $K[x, y]/(xy - 1) \ncong K[t]$.

2. Mapping $\varphi : \mathbb{A}^1 \to V = \{y^2 = x^3\}$, $t \mapsto (t^2, t^3)$ is regular and a set-theoretic bijection. However, it is not an isomorphism. The corresponding homomorphism of algebras $\varphi^* : K[V] = K[x, y]/(y^2 - x^3) \to K[t] = K[\mathbb{A}^1]$ is defined by $x \mapsto t^2$, $y \mapsto t^3$. Its image is $\operatorname{Im}\varphi^* = K[t^2, t^3] \subsetneq K[t]$. Since φ is a bijection, it has inverse mapping

$$\psi : V \to \mathbb{A}^1, \quad \psi(x, y) = \begin{cases} y/x, & (x, y) \neq (0, 0) \\ 0, & (x, y) = (0, 0) \end{cases}$$

[7] ***Biregular*** isomorphism, as opposed to ***birational*** isomorphism which will be introduced later.

but it fails to be regular in the point $(0,0)$. One could give the following informal interpretation. Algebra $K[V]$ is smaller than $K[\mathbb{A}^1]$, since in the latter there is a polynomial function with derivative in 0 different from 0, and in the former there is no such function: mapping is "leveling" all tangent vectors in 0.

3. Parabola $y = x^k$ is isomorphic to the line $\mathbb{A}^1$. The corresponding isomorphisms are $\varphi(x,y) = x$, $\psi(t) = (t, t^k)$.

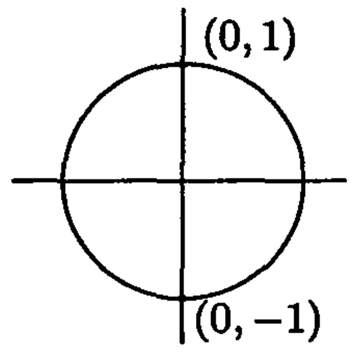
4. Let $V = \{y^2 = x^3 + x^2\}$ be the alpha-curve. As we already know, it has a rational parametrization $\varphi(t) = (t^2 - 1, t^3 - t)$. The parametrization defines a regular mapping $\varphi : \mathbb{A}^1 \to V$. Is this an isomorphism? More generally, is there an isomorphism of V and $\mathbb{A}^1$?

The examples show that, despite our wish to work only with polynomials, the involvement of rational functions is inevitable. Usual rational functions are not functions in a precise sense of the word - they have not to be defined everywhere. We are interested in rational functions on a given algebraic set, say curve C with equation $f(x,y) = 0$. Rational functions on the whole plane are the elements of the fraction field $K(x,y)$ of the polynomial ring $K[x,y]$. Two such rational functions may define the same function on C.

Example. On the circle $C : x^2 + y^2 = 1$ one has $x^2 = (1-y)(1+y)$, so the two rational functions

$$\varphi_1(x,y) = \frac{1-y}{x},$$

$$\varphi_2(x,y) = \frac{x}{1+y}$$



on C coincide in their common functional domain. Note that the domains of these two functions on C are different: the first is not defined in points $(0,1)$ and $(0,-1)$, the second only in $(0,-1)$. They coincide in the Zariski open subset $U = C\backslash\{(0,1),(0,-1)\}$ of the curve C (see fig.

Definition. Let $V \subset \mathbb{A}^n$ be irreducible closed set with coordinate ring $K[V]$. The fraction field $K(V)$ of the domain $K[V]$ is the *field of rational functions* on V (or simply the *function field* of V), and its elements *rational functions* on V.

Let $V \subset \mathbb{A}^n$ be a closed set, $x \in V$ a point, U its open neighborhood and $r : U \to K$ a function in the neighborhood. Function r is *regular at the point* x if there exist polynomial functions $f, g \in K[V]$ such that $g(x) \neq 0$ i.e., $x \in D(g)$ and $r = f/g$ on $U \cap D(g)$.

Proposition. *This local definition of regularity is consistent with the previous global one. In other words, if the function $r : V \to K$ is regular in every point $x \in V$, then $r \in K[V]$.*

Proof. From the definition, for every x there is a representation $r = f_x/g_x$ on $D(g_x)$. Due to compactness, $V = \bigcup_{x \in V} D(g_x) = D(g_1) \cup \cdots \cup D(g_m)$, or

$(g_x \,|x \in V) = (g_1, \dots, g_m)$ where $g_i = g_{x_i}$. Since $V(g_1, \dots, g_m) = \emptyset$, from the analogon of Nullstellensatz one has $(g_1, \dots, g_m) = 1$, or $g_1h_1 + \cdots + g_mh_m = 1$. Consider the polynomial function $f = f_1h_1 + \cdots + f_mh_m \in K[V]$. Since $g_ig_j = 0$ on $V(g_ig_j)$ and $f_ig_j = f_jg_i$ on $D(g_ig_j) = D(g_i) \cap D(g_j)$, then $g_ig_j(f_ig_j - f_jg_i) = 0$ on whole V. If we write $r = f_i/g_i = f_ig_i/g_i^2$, then we have $f_ig_j = f_jg_i$ on whole V. Therefore $f_j = 1 \cdot f_j = \sum_i f_jg_ih_i = \sum_i f_ig_jh_i = f \cdot g_j$ and $r = f \in K[V]$.

Definition. Let $V \subset \mathbf{A}^n$ be closed set, $K[V]$ its coordinate ring and $K(V)$ field of rational functions. If $x \in V$ is a point, all rational functions $r \in K(V)$ regular in x build a ring denoted by $\mathcal{O}_{x,V}$ or $\mathcal{O}_x$ and called the *local ring* of V at the point x. *Regular function* on whole V is a function, regular in every point of V. All regular functions on V also build a ring $\mathcal{O}(V)$. The preceding statement proves that $\mathcal{O}(V) = K[V]$. One has also $\mathcal{O}(V) = \bigcap_{x \in V} \mathcal{O}_{x,V} \subset \mathcal{O}_{x,V} \subset K(V)$.

The ring $\mathcal{O}_{x,V}$ consists of all rational functions from $K(V)$ which has a representation where x is not a zero of the nominator (a pole of the function). All regular functions which have a zero in x build a maximal ideal in $K[V]$ and the ring $\mathcal{O}_{x,V}$ is its minimal extension in which all elements of the complement of this ideal become invertible.

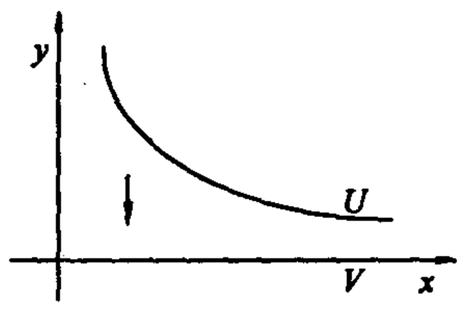
We could already note the importance of the principal open sets, which form the basis of the Zariski topology. The following result shall confirm this opinion.

Proposition. *Principal open sets are affine: they are isomorphic to affine closed sets.*

Proof. Let $V \subset \mathbb{A}^n$ be an affine closed set with coordinate ring $K[V]$, $f \in K[V]$ a regular function and $D(f) = V \setminus V(f) = \{x \in V \,|f(x) \neq 0\}$ principal open set. Let $J = I(V) \subset K[x_1, \dots, x_n]$ be the ideal of V and F defining polynomial for f. Introduce a new indeterminate y and consider the ideal $I = J + (yF - 1) \subset K[x_1, \dots, x_n, y]$. If $U = V(I) \subset \mathbb{A}^{n+1}$ is a closed set, then

$$K[U] = K[x_1, \dots, x_n, y]/\,(J + (yF - 1)) \cong (K[x_1, \dots, x_n]/J)\,[f^{-1}] = K[V][f^{-1}]$$

that is, $D(f) \cong U$. Geometrically, this is analogous to projection of the hyperbola on the axis (see the figure).



From the proof one can see that the principal open set $D(f)$ is the affine closed set corresponding to subalgebra $K[V][f^{-1}] \subset K(V)$. This subalgebra consists of all rational functions which in the denominator have only powers of f. In other words, it is a minimal extension of the algebra $K[V]$ in which the set $\{f, f^2, f^3, \dots\} \subset$

$K[V]$ becomes invertible. This construction, as well as the above construction of the local ring at the point, is called the *localization* of the ring with respect to multiplicative subset. It is very common in commutative algebra. Its oldest version is the construction of domain's fraction field, when all nonzero elèments become invertible.

Rational functions are used to define rational mappings, specific for algebraic geometry. Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be two algebraic sets, and X irreducible.

Definition. Rational mapping $f : X \dashrightarrow Y$ is a mapping defined by m rational functions $f_1, \ldots, f_m \in K(X)$ with the formula $x \mapsto (f_1(x), \ldots, f_m(x))$ in every point $x \in X$ in which all functions are regular.

Rational mapping is not everywhere defined, only on an open set. The notation should also stress the fact, that we have a partial function here. It is however, uniquely defined by its values in the domain of definition. In other words, if one has two rational mappings (on different open sets), which coincide on some nonempty open set, then they are equal.

If the image of rational mapping $f : X \dashrightarrow Y$ is dense in Y, it defines a mapping of rational functions on Y to rational functions on X (by simple change of variables). In this way one has a monomorphism of fields $K(Y) \hookrightarrow K(X)$. Similarly to regular mappings and corresponding ring homomorphisms $K[Y] \to K[X]$, a functorial connection is defined between rational mappings and homomorphisms (i.e. inclusions) of function fields. That means that isomorphisms of fields correspond to "isomorphism" rational mappings.

Definition. Rational mapping is a *birational isomorphism*, if it has inverse rational mapping (inverse here means that the compositions are identities on nonempty open subsets!). Algebraic sets X and Y are *birationally isomorphic*, if there is a birational isomorphism between them, i.e., if $K(X) \cong K(Y)$. Algebraic set X is *rational*, if it is birationally isomorphic to affine space, that is, if $K(X) \cong K(x_1, \ldots, x_n)$.

As a result, there are two different equivalence relations and two classifications of algebraic sets. One is the finer classification up to isomorphism, or classification of coordinate rings, the other is the coarser birational classification, or classification of function fields.

Example. The alpha-curve $y^2 = x^3 + x^2$ is rational: it has a rational parametrization which defines isomorphism of its function field with the field of usual rational functions in one variable $K(x)$. The same holds for semicubic parabola $y^2 = x^3$. However, if in the plane cubic curve $y^2 = P_3(x)$ the right-hand-side polynomial has no multiple roots, it is not rational.

How should one properly define dimension of algebraic set? There are several characterizations of geometrical notion of dimension. The oldest description of dimension is probably one from the Euclid's "Elements": the point is the border of the line, the line is the border of the surface,... One says that the algebraic set V is of dimension d if d is a maximal length of strictly increasing chain $\{x\} = V_0 \subset V_1 \subset \cdots \subset V_d = V$ of irreducible subvarieties in V. Due to connection between

irreducible subvarieties in V and prime ideals in $K[V]$, d is at the same time the maximal length of strictly increasing chain $(0) = I_0 \subset I_1 \subset \cdots \subset I_d$ of proper prime ideals in $K[V]$.

Definition. *Krull dimension* of commutative ring A is the maximal length of strictly increasing chain of proper prime ideals in A.

So, the dimension of algebraic set equals to Krull dimension of its coordinate ring. For example, $\operatorname{Krull\,dim} K[x_1, \ldots, x_n] = n$, in accordance to our intuition.

In courses of commutative algebra it is shown that Krull dimension of the affine algebra (finitely generated reduced algebra over the ground field) is equal to the transcendence degree of the corresponding fraction filed i.e. function field: $\dim V = \operatorname{Krull\,dim}\ K[V] = \operatorname{tr\,deg}_K K(V)$ [1, p. 150]. What is the geometrical meaning of this equality? If $\operatorname{tr\,deg}_K K(V) = d$, then one could chose d algebraically independent elements such that field extension $K(V) \supset K(x_1, \ldots, x_d) = K(\mathbf{A}^d)$ is algebraic. This extension defines a regular mapping $V \to \mathbf{A}^d$, so-called *normalization* of the algebraic set V. Normalization is a finite morphism, which means also that it is a finite covering, i.e., over each point of $\mathbf{A}^d$ there are at most d points of V. This gives us another geometrical explanation of dimension.

Every local ring $\mathcal{O}_{x,V}$ $(x \in V)$ has the same dimension $\dim V$. In local rings (rings with only one maximal ideal) there exists a connection between dimension and the maximal ideal itself: $\dim_K \mathcal{M}/\mathcal{M}^2 \geq \operatorname{Krulldim} \mathcal{O}$. The ring $\mathcal{O}_{x,V}$ (and the point x) is *regular*, if the exact equality holds. What is the meaning of the vector space $\mathcal{M}/\mathcal{M}^2$? It consists of linear parts (i.e., differentials) of all functions, regular and equal to zero in x. Therefore, its dual vector space $(\mathcal{M}/\mathcal{M}^2)^*$ plays the role of the tangent space to the algebraic set V at the point x. The above inequality means that there can exist points which are not regular in the sense that the dimension of the tangent space is strictly greater than the dimension of V itself. Such points are special points. If V is defined by its global equations, they can be characterized in the following way.

Definition. Point $x \in V$ is a *singular point* (*singularity*) of algebraic set $V = V(f_1, \ldots, f_k) \subset \mathbf{A}^n$ if it is a solution of the following system:

$$f_i(x) = \frac{\partial f_i}{\partial x_1}(x) = \cdots = \frac{\partial f_i}{\partial x_n}(x) = 0 \quad (i = 1, \ldots, k).$$

In other words, the singular points are the points where the rank of the Jacobi matrix $\left(\frac{\partial f_i}{\partial x_j}(x)\right)_{\substack{i=1,\ldots,k \\ j=1,\ldots n}}$ drops down. In regular points this rank is equal to codimension of V.

The algebraic definition of singular point, independent of the embedding of V in ambient affine space, was introduced by Zariski[8]. He also proved equivalence with above traditional analytical definition.

---

[8]Oscar Zariski (1899–1986), italian and american algebraic geometer.

Algebraic sets without singularities, nonsingular varieties, are the closest analogons of smooth manifolds or complex-analytic varieties. The presence of singular points complicates the structure of algebraic varieties and makes them interesting.

Example. There are two typical plane singular cubics, which correspond to simplest types of singularities. These are the alpha-curve $y^2 = x^3 + x^2$ with a nodal point (a "node"), and the semicubic parabola $y^2 = x^3$ with a cuspidal point (a "cusp").

The theory of singularities of algebraic varieties is a very deep theory, which itself requires a long introduction. There are many aspects of studying singularities, such as classification by discrete invariants, topological structure, resolution of singularities, etc. One fruitful method for investigation of singularities of hypersurfaces is given by a combinatorial-geometrical invariant called Newton polyhedron. It was introduced by Newton, but it attracted proper attention only recently, mainly in the work of Arnold's singularity group, in the 1970's (see [2]). Some simple, though interesting combinatorial connections between singularity and its Newton polyhedron were studied by the author [17].

6. Projectivization. Projective varieties

Besides the algebraic closure of the ground field, there is one more problem in correspondence between the curve as a set of points on one side, and its equation on the other. If the degree of the curve's equation is d, the number of intersection points with an arbitrary straight line is at most d, but it can also be less.

Let C be a plain curve of degree d, defined by equation $f(x, y) = 0$ where f is a polynomial of degree d. If $L: x = a + bt,\ y = c + dt$ is a straight line, the intersection of C with L is determined by the equation

$$f(a + bt, c + dt) = g(t) = a_0(a, b, c, d) \cdot t^d + \cdots$$

It can happen that some of the roots are multiple, that is, some intersections have higher order. The notion of intersection multiplicity resolves this problem (this, however, is not trivial). However, it can happen that the degree of the equation in t is strictly less than d, since the coefficient of the highest order term equals 0. In the case of hyperbola and its asymptotic lines, the intersection point has "gone to infinity". Therefore, the points at the infinity should be introduced. It is done with the process of projectivization.

There are many equivalent ways to define projective space. A common one is to define the n-dimensional projective space $\mathbb{P}^n$ over the field K as the set of all one-dimensional subspaces, that is, the set of all lines through the origin in the vector space K^{n+1}. If one considers a unit sphere in this space, each line intersects the sphere exactly in two antipodal points. For this reason, in topology, $\mathbb{P}^n$ is defined mostly as the sphere $S^n \subset K^{n+1}$ with its antipodal points identified. We are interested in analytical approach to this construction: ***n-dimensional projective space*** $\mathbb{P}^n = \mathbb{P}^n_K$ over K is the quotient of the set $K^{n+1} \setminus \{0\}$ by the equivalence relation, induced by homothety: $(x_0, x_1, \ldots, x_n) \sim (\lambda x_0, \lambda x_1, \ldots, \lambda x_n)$

where $\lambda \neq 0$. Points in projective space are the corresponding equivalence classes, denoted $x = (x_0 : x_1 : \ldots : x_n)$. Therefore, $(x_0 : x_1 : \ldots : x_n) = (\lambda x_0 : \lambda x_1 : \ldots : \lambda x_n)$. Numbers x_i are *homogeneous coordinates* of the point x. Since there is always a coordinate different from 0, the space $\mathbb{P}^n$ is covered by sets $\mathbb{A}^n_i = \{x \in \mathbb{P}^n \,|\, x_i \neq 0\} = \{x = (x_0 : \ldots : \underset{i}{1} : \ldots : x_n)\} \cong K^n$, each of them isomorphic to the affine space $\mathbb{A}^n$. These are the *affine charts* of the projective space. The transition from homogeneous coordinates of the point $x = (x_0 : x_1 : \ldots : x_n)$ in $\mathbb{P}^n$ to coordinates $(1 : x_1/x_0 : \ldots : x_n/x_0) \cong (x_1/x_0, \ldots, x_n/x_0)$ in the affine chart $\mathbb{A}^n_0 \cong \mathbb{A}^n$ is called *dehomogenization* in x_0, and the converse transition from coordinates $(y_1, \ldots, y_n)$ in $\mathbb{A}^n$ to coordinates $(1 : y_1 : \ldots : y_n)$ in $\mathbb{P}^n$ homogenization.. The complements of affine charts $\mathbb{P}^n \setminus \mathbb{A}^n_i = \{x \in \mathbb{P}^n \,|\, x_i = 0\} = \left\{x = (x_0 : \ldots : \underset{i}{0} : \ldots : x_n)\right\} = \mathbb{P}^{n-1}_i \cong \mathbb{P}^{n-1}$ are isomorphic to the projective space of dimension $n-1$, that is $\mathbb{P}^n = \mathbb{A}^n_i \cup \mathbb{P}^{n-1}_i$. This decomposition is easily seen on the previous model also. If in the space K^{n+1} one considers the i-th coordinate hyperplane $X_i : x_i = 0$ and its parallel hyperplane $Y_i : x_i = 1$, then one could divide the lines through the origin into two types: the lines which intersect hyperplane Y_i and the lines which are parallel to it. Lines in the first family correspond to points of this hyperplane, and they form an affine space $Y_i \cong K^n = \mathbb{A}^n$. The other family of lines is the set of all one-dimensional subspaces of the vector space $X_i \cong K^n$. They form a projective space $\mathbb{P}^{n-1}$ of dimension $n-1$. Points in this projective space, that is, lines in X_i, represent the "points at infinity" of the corresponding parallel lines in the "finite" part Y_i. The whole projective space $\mathbb{P}^n$ is the (disjoint) union of its "finite" part $Y_i \cong \mathbb{A}^n$ and its "points at infinity" complement $\mathbb{P}^{n-1}$. Note that the distinction between finite points and points at infinity of the space $\mathbb{P}^n$ is only formal, since it depends on coordinates. Every point could be made finite or infinite by corresponding change of coordinates.

The next step is to define algebraic subsets in projective space. However, there is a small difference comparing to affine case. Polynomial equations in homogeneous coordinates in $\mathbb{P}^n$ can always be considered to be homogeneous. If $f \in K[s_0, s_1, \ldots, s_n]$ is a polynomial over K in $n+1$ indeterminates $s_0, s_1, \ldots, s_n$, then it is represented as a sum of its homogeneous components $f = f_0 + f_1 + \cdots + f_r$. If now $\xi = (\xi_0 : \xi_1 : \ldots : \xi_n)$ is a point in $\mathbb{P}^n$ for which $f(\xi) = 0$, then $f(\lambda\xi_0, \ldots, \lambda\xi_n) = f_0(\xi_0, \ldots, \xi_n) + \lambda f_1(\xi_0, \ldots, \xi_n) + \ldots + \lambda^r f_r(\xi_0, \ldots, \xi_n) = 0$ for all $\lambda \in K^*$. Since the field K is infinite, it follows that all $f_i(\xi_0, \ldots, \xi_n) = 0$.

The transition from homogeneous polynomial $f(s_0, \ldots, s_n) \in K[s_0, \ldots, s_n]$ to polynomial $f(1, t_1, \ldots, t_n) \in K[t_1, \ldots, t_n]$ is called *dehomogenization*, and the transition from polynomial $g(t_1, \ldots, t_n) \in K[t_1, \ldots, t_n]$ to homogeneous polynomial $s_0^{\deg g} \cdot g(s_1/s_0, \ldots, s_n/s_0) \in K[s_0, s_1, \ldots, s_n]$ (this is a homogeneous polynomial!) *homogenization* with respect to s_0.

Closed algebraic set $V \subset \mathbb{P}^n$ is the set of common zeros of the finite (or infinite) set of polynomials $f \in K[s_0, \ldots, s_n]$. The correspondence between closed sets V and ideals I is the same as in the affine case, only the ideals obtained are not arbitrary, but with every polynomial they contain also all its homogeneous

components.

Definition. Ideal $I \subset K[s_0, \dots, s_n]$ is homogeneous if: $f \in I \Rightarrow$ all homogeneous components of f belong to I.

Every homogeneous ideal has a basis of homogeneous polynomials. Therefore, every closed set in projective space can be defined by homogeneous equations.

Another difference is the absence of Hilbert's Nullstellensatz: there are homogeneous ideals defining the empty set. They can be easily described.

Lemma. $V(I) = \emptyset \Leftrightarrow$ *for some* k, $I \supset I_k := (s_0, \dots, s_n)^k$.

Proof. The direction $\Leftarrow$ is obvious since $V(I_k) = \emptyset$. Conversely, let I be homogeneous and $V(I) = \emptyset$. Let $I = (f_1, \dots, f_r)$ be some homogeneous basis, $\deg f_i = m_i$. Dehomogenized system

$$\begin{aligned} f_1(1, t_1, \dots, t_n) &= 0 \\ \dots & \qquad (t_i = s_i/s_0) \\ f_r(1, t_1, \dots, t_n) &= 0 \end{aligned}$$

has no solutions, since an eventual solution would give a point in $V(I)$. From the Nullstellensatz, one has $1 = f_1(1,t)g_1(t) + \dots + f_r(1,t)g_r(t)$ in the ring $K[t_1, \dots, t_n]$. Homogenizing in s_0, that is multiplying by $s_0^{m_0}$, one has $s_0^{m_0} \in I$. Therefore, all $s_0^{k_0}, \dots, s_n^{k_n} \in I$. If now $m = \max(m_0, \dots, m_n)$ and $k = (m-1)(n+1)+1$, then in every monomial $s_0^{k_0} \cdot \dots \cdot s_n^{k_n}$ with $k_0 + \dots + k_n \geq k$ at least one exponent $k_i \geq m \geq m_i$, and $I_k \subset I$.

Let $V \subset \mathbb{P}^n$ be a projective closed set. The process of dehomogenization in s_0 corresponds to intersection with affine chart $\mathbb{A}_0^n$. In other words, intersection $V \cap \mathbb{A}_0^n$ of the projective closed set V and an affine chart is an affine closed set. Its equations are obtained by dehomogenizing the equations of V with respect to s_0. It should be noted that $V \cap \mathbb{A}_0^n$ is closed as subset in $\mathbb{A}_0^n$ and open as subset in V. Conversely, let $W \subset \mathbb{A}_0^n \cong \mathbb{A}^n$ be an affine closed set. Homogenizing its equations with respect to s_0 one obtains equations of a projective closed set $V = \overline{W} \subset \mathbb{P}^n$ which represents the closure of the set W with respect to Zariski topology in $\mathbb{P}^n$, *projective closure* of W. It is obtained by adding the "points at infinity" to its "finite" part $W = V \cap \mathbb{A}_0^n$.

The coordinate ring of the projective closed set $V \subset \mathbb{P}^n$ is defined in the same way as in the affine case. It is a quotient ring $K[V] = K[s_0, \dots, s_n]/I(V)$. Since the ideal $I(V)$ is homogeneous, this ring is graded (in the affine case it may not be so). Its elements can not be interpreted as functions on V. Their value in points of V is not determined, since it depends on the choice of homogeneous coordinates. Also, the elements of its fraction field, "rational" functions, are not proper functions. Only those among them which originate from rational functions of degree 0 (that is, quotient of two polynomials of the same degree) define functions which have values in points of V, even then not all, but only the points in which the denominator is different from 0. Therefore, the definition of rational and regular function has to be changed, and one should use the local definition of regularity.

Lemma. (& definition). *Rational function in projective closed set $V \subset \mathbb{P}^n$ is the fraction of degree 0 in the field of fractions of the ring $K[V]$. The set $K(V)$ of all such fractions of degree 0 is a field, the field of rational functions of a projective closed set V. If $x \in V$, the rational function $r \in K(V)$ is regular in the point x if it has a representation $r = f/g$, $f, g \in K[V]$, $x \notin V(g) \subset V$. All functions regular in a given point x build a ring, denoted $\mathcal{O}_{x,V}$ or $\mathcal{O}_x$ and called local ring of V in x. Regular function on whole V is a function, regular in each point of V. All regular functions on V also build a ring $\mathcal{O}(V)$. One has $\mathcal{O}(V) = \bigcap_{x \in V} \mathcal{O}_{x,V} \subset \mathcal{O}_{x,V} \subset K(V)$.*

In the case of affine sets there are many regular functions, since $\mathcal{O}(V) = K[V]$. However, in the projective case, it is not so.

Proposition. *The only global regular functions on irreducible projective closed set V are constants: $\mathcal{O}(V) = K$.*

Proof. Let $K[V] = K[s_0, \dots, s_n]/I(V)$ and $x_i = s_i \bmod I(V)$ coordinate functions on V. Then $V = \bigcup_{i=1}^n D(x_i)$ since $\bigcap_{i=1}^n V(x_i) = V((x_0, \dots, x_n)) = \emptyset$. One could renumber coordinates in such way that $x_0, \dots, x_m \neq 0$, $x_{m+1}, \dots, x_n = 0$. Let $r \in \mathcal{O}(V)$ be global regular function. Then in every $D(x_i)$ function r has representation $r = f_i/x_i^{n_i}$ where $n_i = \deg f_i$. Let now $k = n_0 + \dots + n_m$. If the sum of exponents is $k_0 + \dots + k_m = k$, then the function $x_0^{k_0} \cdots x_m^{k_m} \cdot r \in K[V]$ (since at least one $k_i \geq n_i$). It follows that, if $K[V]_k$ is the subset of all homogeneous elements of degree k, then $r^l \cdot K[V]_k \subset K[V]_k$ for all $l \in \mathbb{N}$. Particularly, $r^l \cdot x_0^k \in K[V]_k$. This means that the ring $K[V][r]$ is finitely generated $K[V]$-submodule of a finitely generated (and Noetherian) $K[V]$-module $K[V] + 1/x_0^k \cdot K[V]$. Therefore r is integral over $K[V]$, that is, $r^p + a_1 r^{p-1} + \dots + a_p = 0$ for some $a_i \in K[V]$. By taking homogeneous components of degree 0 in the ring of fractions of the ring $K[V]$, one sees by coefficient comparison that a_i could be replaced by their homogeneous components of degree 0 i.e., constants from K. Therefore, r is algebraic over an algebraically closed field K, and $r \in K$.

The definition of regular and rational mappings is the same as in the affine case. Regular mapping of projective varieties $f : X \to Y$ is a mapping which takes regular functions on Y in regular functions in X. Rational mapping $f : X \dashrightarrow Y$ can be defined in more ways. It is given by regular mapping $f : U \to V$ where $U \subset X$ and $V \subset Y$ are open sets, and two such mappings are identified if they agree on a common open set. Rational mapping is not a function in the proper sense. As a function it is defined on some maximal open subset, the domain of the rational mapping. If $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$, rational mapping $f : X \dashrightarrow Y$ can be described by $m+1$ homogeneous forms $F_0, \dots, F_m$ of the same degree in $n+1$ indeterminates $x_0, \dots, x_n$, or by $m+1$ rational functions $f_0, \dots, f_m$ on X. Some important examples will be stated later.

Besides affine and projective closed sets, their open subsets also naturally appear. This is the most general type of variety we met by now.

Definition. Open subset of projective closed subset is called *quasiprojective variety.*

Affine and projective closed sets are both quasiprojective varieties. All previously defined notions are transferred to quasiprojective varieties: regular functions (local definition), rational functions, local ring of the functions, regular in a given point, field of rational functions. Also, the notions of regular and rational mapping are transferred, as well as the notions of isomorphism and birational isomorphism. Two irreducible varieties are birationally isomorphic if and only if they contain two isomorphic open subsets [33, p. 69].

Definition. Quasiprojective variety isomorphic to an affine (projective) closed set, is called *affine* (*projective*) *variety*.

These notions are introduced in order to study varieties independently of their embedding in the ambient space. As opposed to affine closed sets, the notion of affine variety is invariant with respect to isomorphism.

A property of a geometrical object is local, if every point of it has an open neighborhood in which this property holds. For example, being a closed set is a local property. In the study of local properties, we can always restrict ourselves to affine varieties.

Proposition. *If X is quasiprojective variety and $x \in X$, then x has a neighborhood isomorphic to an affine variety.*

Proof. Let $X \subset \mathbb{P}^n$, $X \cap \mathbb{A}^n = Y \setminus Z$ where $Y, Z \subset Y$ are closed in $\mathbb{A}^n$. Since $x \in Y \setminus Z$, there exists a polynomial $F \in K[\mathbb{A}^n]$ such that $F \in I(Z)$ and $F(x) \neq 0$. Then $V(F) \supset Z$ and $D(F) = Y \setminus V(F)$. Let the ideal $I(Y) = (F_1, \dots, F_m) \subset K[\mathbb{A}^n]$. Consider the closed set $W = V(F_1, \dots, F_m, y \cdot F - 1) \subset \mathbb{A}^{n+1}$. Then the projection $\mathbb{A}^{n+1} \to \mathbb{A}^n$ defines a mapping $\varphi : W \to D(F)$ and $\psi : D(F) \to W$ by $(x_1, \dots, x_n) \mapsto (x_1, \dots, x_n, 1/F(x_1, \dots, x_n))$.

Finally, let us state two important theorems which will be used in the sequel. In both cases, theorems are proved by local technique of reduction to affine case, and then by algebraic calculation in the polynomial ring.

The first theorem states that projective varieties behave better than affine with respect to regular mappings. Regular image of an affine variety need not be closed (example: a projection of hyperbola onto axis). This can not happen for projective varieties.

Theorem. (on closed image, [33, p. 76]). *The image of the projective variety X under a regular mapping $f : X \to Y$ is a closed set in Y.*

The second theorem is analogous to the corresponding theorem from differential geometry. A regular mapping foliates the domain into disjoint preimages of points—fibres over points. What is the dimension of each fibre? In differential geometry, it is equal to the difference between dimensions of the domain and its image. In algebraic situation this is the case "almost everywhere", that is, on an open subset.

Theorem. (on dimension of fibres, [33, p. 97]). *Let $f : X \to Y$ be regular mapping of an irreducible variety X of dimension n onto an irreducible variety Y of*

dimension m. Then $m \le n$, fibres $f^{-1}(y)$ over $y \in Y$ have dimension $\dim f^{-1}(y) \ge n - m$ *and the equality holds over a nonempty open set $U \subset Y$.*

7. Veronese and Grassmann varieties. Lines on surfaces

7.1. The Veronese variety. Homogeneous polynomials $F(x_0, \dots, x_n) = \sum_{i_0+\dots+i_n=m} a_{i_0\dots i_n} x_0^{i_0} \dots x_n^{i_n}$ of degree m in $n+1$ indeterminates form a vector space of dimension $d_m^n = \binom{n+m}{m}$. The form F defines a projective hypersurface $H = \{F = 0\} \subset \mathbb{P}^n$ of degree m. Two forms define the same hypersurface if and only if they are proportional. Therefore, all projective hypersurfaces of degree m form a projective space $\mathbb{P}^{d_m^n-1}$ of dimension $d_m^n - 1 = \binom{n+m}{m} - 1$, with homogeneous coordinates $(v_{i_0\dots i_n} \mid i_0 + \dots + i_n = m)$.

Define a regular mapping $\mathcal{V}_m^n : \mathbb{P}^n \to \mathbb{P}^{d_m^n-1}$ by $(u_0 : \dots : u_n) \mapsto v_{i_0\dots i_n} = u^{i_0} \dots u^{i_n}$. Its image $\mathcal{V}_m^n(\mathbb{P}^n) = V_m^n \subset \mathbb{P}^{d_m^n-1}$ is called *Veronese variety.* It is defined by equations $v_{i_0\dots i_n} \cdot v_{j_0\dots j_n} = v_{k_0\dots k_n} \cdot v_{l_0\dots l_n}$ $(i_0 + j_0 = k_0 + l_0, \dots, i_n + j_n = k_n + l_n)$. Namely, if these equations define the variety X_m^n, then obviously $V_m^n \subset X_m^n$. Conversely, one deduces from these equations that on X_m^n at least one coordinate of the form $v_{0\dots m\dots 0}$ is different from zero, say $v_{m0\dots 0} \ne 0$. Then in the open set $\{v_{m0\dots 0} \ne 0\} \supset X_m^n$ the mapping

$$\begin{aligned} u_0 &= v_{m,0,\dots,0} \\ u_1 &= v_{m-1,1,\dots,0} \\ &\dots \\ u_n &= v_{m-1,0,\dots,1} \end{aligned}$$

is regular and inverse for $\mathcal{V}_m^n : \mathbb{P}^n \to \mathbb{P}^{d_m^n-1}$. So, $\mathcal{V}_m^n : \mathbb{P}^n \cong \mathcal{V}_m^n(\mathbb{P}^n) = V_m^n \subset \mathbb{P}^{d_m^n-1}$. The dimension of the Veronese variety V_m^n is n.

Example 1. For $n = 1$, $m = 3$, $\mathcal{V}_3^1 : \mathbb{P}^1 \hookrightarrow \mathbb{P}^3$. The equations of $V_3^1 \subset \mathbb{P}^3$ are

$$v_{03}v_{30} = v_{12}v_{21}, \quad v_{03}v_{21} = v_{12}^2, \quad v_{30}v_{12} = v_{21}^2$$

where $(v_{03} : v_{12} : v_{21} : v_{30})$ are the homogeneous coordinates in $\mathbb{P}^3$. Dehomogenization on $v_{03} \ne 0$, with notations $x = v_{12}/v_{03}$, $y = v_{21}/v_{03}$, $z = v_{30}/v_{03}$, gives

$$z = xy, \quad y = x^2, \quad xz = y^2$$

or $y = x^2$, $z = x^3$ since the ideal $(z - xy, y - x^2, xz - y^2) = (y - x^2, z - x^3)$. Therefore, the Veronese curve $V_3^1 \subset \mathbb{P}^3$ is exactly the *space cubic* (or the *normal curve*) $t \mapsto (t, t^2, t^3)$.

Example 2. More generally, if $n = 1$, the Veronese mapping $\mathcal{V}_m^1 : \mathbb{P}^1 \hookrightarrow \mathbb{P}^m$ is $(x : y) \mapsto (x^m : x^{m-1}y : \dots : y^m)$. The system of equations for Veronese curve can be written as $V_m^1 = \{(x_0 : x_1 : \dots : x_m) \mid (x_0 : x_1) = (x_1 : x_2) = \dots = (x_{m-1} : x_m)\}$ or

$$\operatorname{rank} \begin{pmatrix} x_0 & x_1 & x_2 & \dots & x_{m-1} \\ x_1 & x_2 & x_3 & \dots & x_m \end{pmatrix} \le 1$$

In the affine chart the corresponding curve has rational parametrization $t \mapsto (t, t^2, \dots, t^m)$.

Example 3. If $F(x_0, \dots, x_n) = \sum_{i_0+\dots+i_n=m} a_{i_0\dots i_n} x_0^{i_0} \dots x_n^{i_n}$ is a form of degree m and $H = \{F = 0\} \subset \mathbb{P}^n$ corresponding hypersurface, then $\mathcal{V}_m^n(H) = V_m^n \cap E$ where E is a hyperplane $\sum_{i_0+\dots+i_n=m} a_{i_0\dots i_n} v_{i_0\dots i_n} = 0$ in $\mathbb{P}^{d_m^n-1}$. Using this fact it is easy to see that a complement of a hypersurface in $\mathbb{P}^n$ is an affine variety (that is, isomorphic to an affine closed set).

It is not difficult to prove that the Veronese variety $\mathcal{V}_m^n(\mathbb{P}^n) = V_m^n \subset \mathbb{P}^{d_m^n-1}$ is not contained in any linear subspace of $\mathbb{P}^{d_m^n-1}$.

7.2. The Grassmannian. Let V be the vector space of dimension n. The set $\mathrm{Gr}(r, V)$ of all r-dimensional subspaces of the space V is called the *Grassmannian* of V (of corresponding dimension). If $L \in \mathrm{Gr}(r, V)$ is one such subspace and $e_1, \dots, e_r$ its basis, it defines an element $e_1 \wedge \dots \wedge e_r \in \Lambda^r V$ of the exterior power of the vector space V. If $e_1', \dots, e_r'$ is another basis of L, then $e_1' \wedge \dots \wedge e_r' = \alpha \cdot e_1 \wedge \dots \wedge e_r$ where $\alpha = \det C_{e \to e'} \neq 0$ is the determinant of the transition matrix. This means that the element $e_1 \wedge \dots \wedge e_r \in \Lambda^r V$ defines a point in the projectivization. $\mathbb{P}(\Lambda^r V)$, which does not depend on the choice of base, but only on the subspace L. In this way one obtains a mapping $P : \mathrm{Gr}(r, V) \to \mathbb{P}(\Lambda^r V)$, $L \mapsto P(L)$. It is easily seen that this is an injection, that is, $\mathrm{Gr}(r, V) \hookrightarrow \mathbb{P}(\Lambda^r V)$. If $e_1, \dots, e_n$ is a basis in V, $\{e_{i_1} \wedge \dots \wedge e_{i_r}\}$ is a basis in $\Lambda^r V$, the dimension of this vector space equals $\binom{n}{r}$, and dimension of its projectivization equals $\binom{n}{r} - 1$. If $L \in \mathrm{Gr}(r, V)$, one has $P(L) = \sum_{i_1 < \dots < i_r} p_{i_1 \dots i_r} \cdot e_{i_1} \wedge \dots \wedge e_{i_r}$. The homogeneous coordinates $\{p_{i_1 \dots i_r}\}$ of the point $P(L) \in \mathbb{P}(\Lambda^r V)$ are called the *Plücker*[9] *coordinates* of the subspace $L \in \mathrm{Gr}(r, V)$. However, the mapping P is not surjective. Let us determine the image $\mathrm{Im}\, P$. This reduces to a question, could one explicitly describe conditions that a vector $x \in \Lambda^r V$ is decomposable, that is, has the form $x = f_1 \wedge \dots \wedge f_r$. In order to solve it, one introduces a new operation in the exterior algebra of a vector space, a mapping $V^* \times \Lambda^r V \to \Lambda^{r-1} V$ which "reduces" exterior degree, by the following inductive definition.

Let $u \in V^*$ be a linear function on V. For $x \in \Lambda^0 V = K$ define $u \lrcorner x = 0$. For $x \in \Lambda^1 V = V$ define $u \lrcorner x = (u, x) = u(x)$. In the general case, for vectors of the form $x \wedge y \in \Lambda^r V \quad (r \geq 2)$ (which generate whole $\Lambda^r V$) one defines $u \lrcorner (x \wedge y) = (u \lrcorner x) \wedge y + (-1)^r x \wedge (u \lrcorner y)$, and extends it linearly on arbitrary vectors. Finally, this mapping can be iteratively defined for vectors $u = u_1 \wedge \dots \wedge u_k \in \Lambda^k V^* \quad (k \geq 2)$ and linearly extended on arbitrary vectors $u \in \Lambda^k V^*$. One obtains a linear map $\Lambda^k V^* \times \Lambda^r V \to \Lambda^{r-k} V$, $(u, x) \mapsto u \lrcorner x$, called *cancellation*[10].

Example. For $r = 1$ and $x, y \in V$ one has $u \lrcorner (x \wedge y) = u(x) \cdot y - u(y) \cdot x$. Particularly, for $x \neq 0, \quad x^* \in V^*$ and $x^* \lrcorner (x \wedge y) = y$, which justifies the term.

---

[9] Julius Plücker (1801-1868), German geometer, who first introduced homogeneous coordinates and coordinate method in projective geometry. He was teacher of Felix Klein.

[10] in Russian "свёртка"

The following lemma shows the connection between cancellation and the Plücker coordinates and can be proved straightforwardly.

Lemma. *Let $e_1, \dots, e_n$ be a basis in V and $e_1^*, \dots, e_n^*$ its dual basis in V^*. If $\{p_{i_1 \dots i_r}\}$ are Plücker coordinates of the vector x in e, then $p_{i_1 \dots i_r} = e_{i_r}^* \lrcorner (\dots (e_{i_1}^* \lrcorner x) \dots)$.*

Proposition. *A given vector $x \in \Lambda^r V$ is of the form $x = f_1 \wedge \dots \wedge f_r$ for any $u \in \Lambda^{r-1} V^*$ one has $(u \lrcorner x) \wedge x = 0$.*

Proof. Let us describe the proof in the case $n = 4$, $r = 2$. The direction $\Rightarrow$ is checked easily. Prove the opposite direction. Let $x = p_{12} e_1 \wedge e_2 + p_{13} e_1 \wedge e_3 + \dots \neq 0$ in some basis e_1, e_2, e_3, e_4 and, say, $p_{12} = 1$. Let u_1, u_2, u_3, u_4 be the dual basis in V^*. From previous properties one has $u_2 \lrcorner (u_1 \lrcorner x) = p_{12} = 1$, $(u_1 \lrcorner x) \wedge x = 0$, $u_2 \lrcorner ((u_1 \lrcorner x) \wedge x) = 0$, therefore $0 = (u_2 \lrcorner (u_1 \lrcorner x)) \wedge x - (u_1 \lrcorner x) \wedge (u_2 \lrcorner x) = x - (u_1 \lrcorner x) \wedge (u_2 \lrcorner x)$, and one has $x = (u_1 \lrcorner x) \wedge (u_2 \lrcorner x)$.

Vectors f_1 and f_2 in the decomposition $x = f_1 \wedge f_2$ can be described explicitly. Namely, if $x = e_1 \wedge e_2 + p_{13} e_1 \wedge e_3 + p_{14} e_1 \wedge e_4 + p_{23} e_2 \wedge e_3 + p_{24} e_2 \wedge e_4 + p_{34} e_3 \wedge e_4$ ($p_{12} = 1$) and if $f_1 = u_1 \lrcorner x = \dots = e_2 + p_{13} e_3 + p_{14} e_4$, $f_2 = u_2 \lrcorner x = \dots = -e_1 + p_{23} e_3 + p_{24} e_4$, then one sees that $x = f_1 \wedge f_2 \Leftrightarrow p_{34} = p_{13} p_{24} - p_{14} p_{23}$.

Note that it suffices to check the condition $(u \lrcorner x) \wedge x = 0$ only for basis vectors $u \in \Lambda^{r-1} V^*$, which leads to a system of polynomial equations with respect to indeterminate Plücker coordinates. Therefore, the Grassmannian $\mathrm{Gr}(r, V) \cong \mathrm{Im}\, P \subset \mathbb{P}(\Lambda^r V)$ has a natural structure of a projective algebraic variety, which parametrizes the set of all $(r-1)$-dimensional projective subspaces of a $(n-1)$-dimensional projective space. It is clear that this variety does not depend on the choice of the space V but only on its dimension n and therefore it is usually denoted $\mathrm{Gr}(r, n)$. In the sequel we shall be interested mostly in the case $n = 4$, $r = 2$, that is, the case of the Grassmannian $\mathrm{Gr}(2, 4)$ of all projective lines in a projective space. Here the defining system could be explicitly written down and it simplifies to single equation:

$$p_{12} p_{34} - p_{13} p_{24} + p_{14} p_{23} = 0$$

This equation defines a hypersurface $\Pi \subset \mathbb{P}^5$, *Plücker hypersurface.*

Lemma. *If vectors $f_1 = x_1 e_1 + \dots + x_4 e_4$, $f_2 = y_1 e_1 + \dots + y_4 e_4$ form a base of the plane L, then $f_1 \wedge f_2 = \sum (x_i y_j - x_j y_i) e_i \wedge e_j$ and Plücker coordinates of the corresponding line are $p_{ij} = x_i y_j - x_j y_i$. The plane $L = \mathrm{Span}\{f_1, f_2\} = \{u \lrcorner (f_1 \wedge f_2) \mid u \in V*\}$. If u has coordinates $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ in the dual base u_1, u_2, u_3, u_4, that is, $u = \alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3 + \alpha_4 u_4$, then $u \lrcorner (f_1 \wedge f_2) = u(f_1) f_2 - u(f_2) f_1 = \sum_i \alpha_i x_i \sum_j y_j e_j - \sum_i \alpha_i y_i \sum_j x_j e_j = \sum_i \left(\sum_j \alpha_j p_{ij} \right) e_i$ and projective coordinates of an arbitrary point of the corresponding projective line are $z_i = \sum_j p_{ij} \alpha_j \quad (i = 1, \dots, 4)$.*

7.3. Lines on surfaces in projective space. We have seen that surfaces of a given degree m in projective space $\mathbb{P}^3$ are parametrized by points of projective

space $\mathbb{P}^k$ with $k = \binom{m+3}{3} - 1$. Lines in projective space $\mathbb{P}^3$ are parametrized by points of Plücker hypersurface $\Pi \subset \mathbb{P}^5$. We are interested in conditions when some surface contains some lines. Consider the product $\mathbb{P}^k \times \Pi$ and its subset $\Gamma = \{(\xi, \eta) \mid \eta \subset \xi\} \subset \mathbb{P}^k \times \Pi$ of all pairs (ξ, η) where ξ is a surface and η a line contained in it.

Proposition. *The set* $\Gamma = \{(\xi, \eta) \mid \eta \subset \xi\} \subset \mathbb{P}^k \times \Pi$ *is closed, i.e., it is a projective variety.*

This follows directly from the following lemma.

Lemma. *Let* $\eta \in \Pi$ *be a line in* $\mathbb{P}^3$ *with Plücker coordinates* p_{ij} $(1 \le i < j \le 4)$ *and* $\xi \in \mathbb{P}^k$ *a surface of degree* m *with coefficients* $q_{i_0 i_1 i_2 i_3}$ $(\sum i_k = m)$. *The condition* $\eta \subset \xi$ *is algebraic with respect to* p *and* q, *homogeneous on each group of indeterminates separately.*

Proof. Coordinates of arbitrary point on the line η are $z_i = \sum_j p_{ij}\alpha_j$ $(i = 1, \dots, 4)$ with indeterminate $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. If $F(z_1, z_2, z_3, z_4) = 0$ is a homogeneous equation of the surface ξ, then $\eta \subset \xi$ if and only if the equality $F\Big(\sum_j p_{1j}\alpha_j, \sum_j p_{2j}\alpha_j, \sum_j p_{3j}\alpha_j, \sum_j p_{4j}\alpha_j\Big) = 0$ holds for all α_i. This gives homogeneous equations for p and q.

Consider two projections $\varphi : \Gamma \to \mathbb{P}^k$, $(\xi, \eta) \mapsto \xi$ and $\psi : \Gamma \to \Pi$, $(\xi, \eta) \mapsto \eta$. These are regular mappings. The second projection ψ is surjective, since any line is contained in at least one (say, reducible) surface of degree m. Let us calculate the dimension of the fibre $\psi^{-1}(\eta) = \{(\xi, \eta) \mid \xi \supset \eta\}$. A coordinate transformation in $\mathbb{P}^3$ allows us to suppose that the equations for η are $z_0 = z_1 = 0$. Then the equation of the surface ξ which contains this line has to be of the form $F(z) = z_0 G(z) + z_1 H(z)$. The set of all such homogeneous forms in the space of all forms of degree m in 4 indeterminates forms a linear subspace of dimension l. The form $F(z) = \sum_{i_0 + \dots + i_3 = m} q_{i_0 \dots i_3} z_0^{i_0} \dots z_3^{i_3}$ is of the form $z_0 G(z) + z_1 H(z) \Leftrightarrow$ in each summand $i_0 \ge 1$ or $i_1 \ge 1$, and this is a complement of the condition $i_0 = i_1 = 0$. Therefore $l =$ (the number of forms in 4 indeterminates) $-$ (the number of forms in 2 indeterminates) $= \binom{m+3}{3} - \binom{m+1}{1} = \frac{1}{6}m(m+1)(m+5)$. Now $\dim \psi^{-1}(\eta) = \frac{1}{6}m(m+1)(m+5) - 1$. All fibres have the same dimension and Γ is irreducible. According to the theorem of dimensions of fibres, $\dim \Gamma = \dim \psi(\Gamma) + \dim \psi^{-1}(\eta) = \frac{1}{6}m(m+1)(m+5) + 3$. Consider now the projection φ. According to the theorem on closed image, $\varphi(\Gamma) \subset \mathbb{P}^k$ is a closed subset of dimension $\dim \varphi(\Gamma) \le \dim \Gamma$. For a given surface ξ of degree m the fibre $\varphi^{-1}(\xi) \subset \Gamma$ consists of all pairs (ξ, η) for which the line η lays on the surface ξ. Obviously, if $\dim \Gamma < k = \binom{m+3}{3} - 1$, φ cannot be surjective, that is, there are surfaces of degree m which do not contain lines. For $\xi \in \varphi(\Gamma)$, from the theorem of dimension of fibres it follows that $\dim \varphi^{-1}(\xi) \ge \dim \Gamma - \dim \varphi(\Gamma)$. Compare the values of k and $\dim \Gamma$ for different m:

m	1	2	3	4
k	3	9	19	34
$\dim \Gamma$	5	10	19	33

If $m \geq 4$, then $\dim \Gamma < k$. This means that there is always a surface of degree $m \geq 4$ on which there are no lines at all. Consider more closely the cases $m = 1, 2, 3$. For $m = 1$, surfaces of degree 1 are planes, parametrized by points of $\mathbb{P}^3$ (principle of projective duality!). On any plane there are infinitely many lines—dimension of the fibre is ≥ 2. For $m = 2$, surfaces of degree 2 are quadrics, parametrized by points of $\mathbb{P}^9$. On any quadric there are infinitely many lines - dimension of the fibre is ≥ 1. The case $m = 3$ is most interesting. Cubic surfaces are parametrized by points of the space $\mathbb{P}^{19}$. Here the dimension of non-empty fibres is ≥ 0. Now prove that this lower bound is reached, that is, there exists a cubic surface with only finitely many lines. Consider the surface $xyz = 1$. In the finite part of the space, $\mathbb{A}^3$, it does not contain any line, whereas in the plane at infinity $\mathbb{P}^2$ it contains three lines $xyz = 0$. This means that $\dim \varphi(\Gamma) = \dim \Gamma = 19$ and that φ is surjective! We have just proved the following theorem.

Theorem. *Any cubic surface contains a line. The set of cubic surfaces that contain only finitely many lines is open in* $\mathbb{P}^{19}$.

This is a classical result, showing a very specific method of proof in classical algebraic geometry: one example has proved the theorem. Cubic surfaces have been extensively studied. One of the most complete monographs on the subject is [21].

8. Twenty-seven lines on a cubic surface

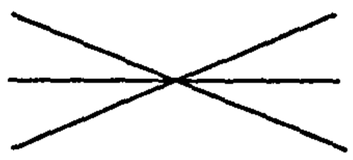
We have proved that on any cubic surface there is at least one line and that "almost all" cubic surfaces contain finitely many lines. How many? One of the most beautiful classical theorems of geometry says that any nonsingular cubic surface contains exactly 27 lines.

Let S be nonsingular cubic surface in $\mathbb{P}^3$. Note the following simple facts.

Lemma 1. *If* Π *is a plane, then* $S \cap \Pi$ *is a plane cubic curve.*

Lemma 2. *If this cubic contains a line* l*, then* $S \cap \Pi = l \cup \{\text{conic}\}$.

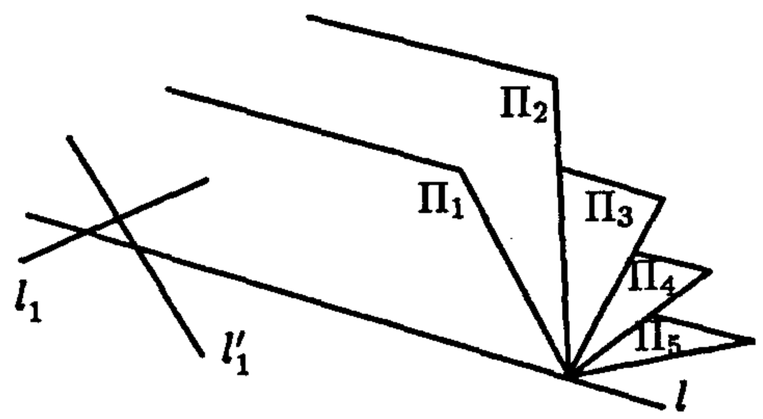
Lemma 3. *If this conic is reducible, then all three lines are different (there are no multiple lines) and their configuration belongs to one of the following two types*



Proof. Coordinates could be chosen so that $\Pi : \{t = 0\}$, $l : \{z = t = 0\}$ and $S : \{f(x, y, z, t) = 0\}$. If l is the multiple line of the intersection $S \cap \Pi$, then $f(x, y, z, t) = z^2 \cdot a(x, y, z, t) + t \cdot b(x, y, z, t)$ where a is a linear form and b a quadratic form. But then $\operatorname{Sing} S \supset \{z = t = b(x, y, z, t) = 0\} \neq \emptyset$ in $\mathbb{P}^3$.

Lemma 4. *If the point $P \in S$, then all lines l on S through P are coplanar (since all such $l \subset T_P(S)$) and there are at most three such lines.*

Lemma 5. *If the line $l \subset S$, then there exist exactly 5 planes $\Pi_1, \ldots, \Pi_5$ for which the corresponding conic $Q = (S \cap \Pi) \setminus l$ is reducible, that is, $S \cap \Pi_i = l \cup (l_i \cup l_i')$ (see the figure)*



Proof. Let us choose the coordinates so that the line l has equation $l : \{z = t = 0\}$ and write the equation of the cubic surface in the form

$$S : f(x,y,z,t) \equiv a_1(z,t)x^2 + b_1(z,t)xy + c_1(z,t)y^2 + a_2(z,t)x + b_2(z,t)y + a_3(z,t) = 0$$

where a_1, b_1, c_1 are linear forms, a_2, b_2 quadratic forms and a_3 a cubic form. A bundle of planes through l has equation $\Pi : \mu z = \lambda t$, and one obtains the following equation of the conic in the intersection $S \cap \Pi$:

$$a_1(\lambda,1)x^2 + b_1(\lambda,1)xy + c_1(\lambda,1)y^2 + a_2(\lambda,1)xt + b_2(\lambda,1)yt + a_3(\lambda,1)t^2 = 0$$

This conic is reducible if and only if the corresponding determinant

$$\Delta = \begin{vmatrix} a_1 & b_1/2 & a_2/2 \\ b_1/2 & c_1 & b_2/2 \\ a_2/2 & b_2/2 & a_3 \end{vmatrix} = 0$$

equals zero. This is an equation of the fifth degree in λ. It has at most five roots, that is, at most five corresponding planes in which the conic is reducible. Let us prove that there are exactly five such planes, i.e., that all these roots are different. This will follow from nonsingularity of the cubic surface S. We could suppose that one of the roots is $\lambda = 0$ i.e., that $\Pi = \{z = 0\}$ is one of these planes. The intersection $S \cap \Pi$ consists of three lines with one of the above two configuration types.

Type 1. We can choose coordinates in such way that the three lines in the plane $z = 0$ are $t = 0$, $x = 0$ and $x = t$. The corresponding equation f is then $f = x(x-t)t + zg$ where g is quadratic form. Comparing the corresponding coefficients, we obtain $a_1 = t + \alpha z$, $a_2 = -t^2 + zd_1$ where d_1 is linear form, and $z | b_1, c_1, b_2, a_3$. Since S is nonsingular at the point $(0:1:0:0)$, one has $c_1 = \gamma z$, $\gamma \neq 0$.

Type 2. We can choose coordinates in such way that the three lines in the plane $z = 0$ are $t = 0$, $x = 0$ and $y = 0$. The corresponding equation f is then

$f = xyt + zg$ where g is quadratic form. Comparing the corresponding coefficients, we obtain $b_1 = t + \alpha z$ and $z \mid a_1, c_1, a_2, b_2, a_3$. Since S is nonsingular at the point $(0:0:0:1)$, one has $a_3 = \gamma z t^2 + \cdots$, $\gamma \neq 0$.

In both cases the determinant has the form $\Delta = z^2 h - \gamma z t^4$, and $z = 0$ is its single root.

Lemma 6. *Lines from different pairs l_i, l_i' $(i = 1, \ldots, 5)$ do not intersect. This follows from Lemma 4.*

Lemma 7. *If m is a line on S that does not intersect with l, then m intersects with exactly one line of each pair l_i, l_i' $(i = 1, \ldots, 5)$.*

Proof. Line m intersects with any plane in $\mathbb{P}^3$, therefore with Π_i. However, it can not be contained in Π_i since m does not intersect with l. Since $S \cap \Pi_i = l \cup (l_i \cup l_i')$, m has to intersect with configuration $l_i \cup l_i'$, and due to Lemma 3 it can not intersect with both of these lines.

Let now l and m be two nonintersecting lines on S. From previous results it follows that such lines exist. The line l determines 10 lines l_i, l_i' $(i = 1, \ldots, 5)$, and exactly one of the each pair intersects with m. Change the notations in such way that l_i intersect with m. The line m also determines its 10 lines, 5 pairs of lines, and exactly one of the each pair is the line l_i. Let these be the lines l_i, l_i'' $(i = 1, \ldots, 5)$. Each line l_i'' does not intersect with any of lines l_j $(j \neq i)$ and therefore has to intersect all lines l_j' $(j \neq i)$. One has a configuration of $1 + 1 + 5 + 5 + 5 = 17$ lines.

Lemma 8. *a) Any 4 nonincident lines on S do not belong to a nonsingular quadric. (In such case the whole quadric would be contained in S, and the cubic S would be reducible.)*

b) Any 4 nonincident lines in $\mathbb{P}^3$ that do not belong to a nonsingular quadric, could have at most two common incident lines.

Lemma 9. *If n is a line on S different from the mentioned 17, then it intersects with exactly three of five lines l_i.*

Proof. If n intersects with at least four, then $n = l$ or $n = m$, which is a contradiction. If n intersects with at most two, then it has to intersect with at least three of five lines l_i' (since it intersects with exactly one line of each pair). Let these be, say, lines l_1, l_2', l_3', l_4'. These four nonincident lines on S already have two common incident lines l and l_1''. It follows then from Lemma 9 that $n = l$ or $n = l_1''$ which is again a contradiction.

Lemma 10. *For any choice of three indexes $\{i, j, k\} \subset \{1, 2, 3, 4, 5\}$ there is exactly one line $l_{ijk} \subset S$ that intersects with three lines l_i, l_j and l_k.*

Proof. Choose one of the indexes, say $i = 1$ and consider the line l_1. From Lemma 5, one has 10 lines intersecting with it. Four of them are l, l_1', m, l_1''. There are six lines left. From Lemma 9, each of them intersects with exactly two of the lines l_2, l_3, l_4, l_5. Since $\binom{4}{2} = 6$, each possibility is being realized.

There are $\binom{5}{3} = 10$ new lines. These, with previous 17, add up to 27 lines on a cubic surface S.

Theorem. (Salmon, Cayley, 1849)[11] *On any nonsingular cubic surface there are exactly 27 lines.*

This remarkable theorem is among the most interesting results in geometry of the last century. The configuration of 27 lines has been extensively studied. In 1869 Wiener produced a model of a cubic surface with all its 27 lines real and visible in the model (see [35, p. 127]). The automorphism group of the configuration of 27 lines was first studied by Jordan[12][11]. The order of that group is $51840 = 2^7 3^4 5$, and it has been later classified as the Weyl group E_6. It has a simple subgroup of index 2 and of order 25920. There is a reach literature concerning 27 lines. In the 20th century it has been slowly (and unjustly) forgotten. With the renaissance of algebraic geometry in the fifties, the investigation of cubic surfaces had its culmination in papers and the book of Manin [21], and the 27 lines theorem became an inevitable part of many introductory courses of algebraic geometry. Our proof follows the book of Reid [25].

9. Number of equations. Multiple subvarieties. Weil divisors

In general, each additional equation in an affine or projective set's defining system decreases the dimension of the solution set by 1. However, it can happen that adding the equation does not change the dimension (if the equation is already contained in the ideal generated by previous ones). In other words, not all closed sets in $\mathbb{A}^n$ or $\mathbb{P}^n$ of codimension k could be defined by k equations. One has only $\operatorname{codim} V(f_1, \dots, f_k) \le k$.

Definition. The variety $X \subset \mathbb{A}^n$ of codimension k (and dimension $n-k$) is a *complete intersection* if $I(X) = (f_1, \dots, f_k) \subset K[x_1, \dots, x_n]$, and *set-theoretic complete intersection* if $I(X) = \sqrt{(f_1, \dots, f_k)}$. Clearly, each complete intersection is a set-theoretic one, but the converse does not hold. The variety X is a set-theoretic intersection if it can be represented as intersection of k hypersurfaces.

Examples. 1. [8, p. 242], [31, p. 290, ex. 4.9] In $\mathbb{A}^4$ the set $V(x_1, x_2) \cup V(x_3, x_4)$ has codimension 2, but can not be defined with two equations.

2. [31, p. 32, ex. 2.17] If $X \subset \mathbb{P}^3$ is the projective closure of the space cubic

$$x = t, \quad y = t^2, \quad z = t^3$$

the homogeneous ideal $I(X)$ can not be generated by 2 elements.

3. [31, p. 25, ex. 1.11] Affine space cubic can be defined with two equations, as intersection of two quadrics, a cylinder and a cone, since $I(X) = (y - x^2, y^2 - xz)$. However, if $X \subset \mathbb{A}^3$ is a space curve

$$x = t^3, \quad y = t^4, \quad z = t^5$$

---

[11] George Salmon (1819–1904), Irish mathematician. Arthur Cayley (1821–1895), English mathematician.

[12] Camille Jordan (1838–1922), French mathematician

then the corresponding ideal can not be generated by 2 elements. The intersection of any two of these three surfaces, besides the space curve, contains a coordinate axis. The general case of a space curve

$$x = t^{n_1}, \quad y = t^{n_2}, \quad z = t^{n_3}$$

has been treated only recently [32]. If $c_i \in \mathbb{N}$ are the least positive integers such that $n_i c_i \in n_j\mathbb{N}+n_k\mathbb{N}$ (here, the triple (i,j,k) goes through all three cyclic permutations of the triple $(1,2,3)$), then the ideal $I(X)$ has

(a) either two generators, $I(X) = (x^{c_1} - z^{c_3}, y^{c_2} - x^{r_{21}} z^{r_{23}})$ and the curve is a complete intersection. Example: $(n_1,n_2,n_3) = (4,5,6)$, $I(X) = (x^3 - z^2, y^2 - xz)$;

(b) or three generators, $I(X) = (x^{c_1} - y^{r_{12}} z^{r_{13}}, y^{c_2} - x^{r_{21}} z^{r_{23}}, z^{c_3} - x^{r_{31}} y^{r_{32}})$ and the curve is not a complete intersection. Example: $(n_1,n_2,n_3) = (3,4,5)$, $I(X) = (x^3 - yz, y^2 - xz, z^2 - x^2 y)$.

Cases (a) and (b) could be distinguished algorithmically. The case (b) however, is a set-theoretic complete intersection, since there is always a polynomial $p(x,y,z)$ such that $I(X) = \sqrt{(p, z^{c_3} - x^{r_{31}} y^{r_{32}})}$.

In codimension 1 the corresponding equality holds. Any subvariety in $\mathbf{A}^n$ or $\mathbb{P}^n$ of codimension 1 can be given by one equation: it is a hypersurface. More generally, if X is a nonsingular projective or affine variety and $Y \subset X$ a subvariety of codimension 1, then near each of its points, it is defined by one equation, that is, $\forall x \in Y \ \exists U \ni x$ such that $I(Y \cap U) = (f) \subset K[U]$ is principal. In the proof, the factorial property of the local ring of regular point is used essentially [8, p. 241], [33, t. 1, pp. 90, 134].

Let us consider the multiplicity. Already in the case of curves we have seen that one has to take it into account. Radical ideals were introduced in order to remove the nilpotents from the coordinate ring. When one considers intersections of subvarieties, it becomes more complex. Let X be a variety and $Y, Z \subset X$ two its subvarieties with corresponding ideals $I(Y), I(Z)$. Then the intersection $Y \cap Z = V(I(Y) + I(Z))$. However, the sum of two radical ideals does not have to be radical, it can contain nilpotents.

Example 1. Let $X = \mathbf{A}^2$, $K[X] = K[x,y]$ and let $Y = V(y)$, $Z = V(y - x^2)$ be irreducible curves. The ideal $I(Y) + I(Z) = (y) + (y - x^2) = (x^2, y)$ and the coordinate ring $K[Y \cap Z] = K[x,y]/(x^2,y)$ has a nilpotent x. This corresponds to the intuitively clear fact that the parabola and the line are tangent to each other in their intersection point, the multiplicity of that point being 2.

Example 2. [14, p. 28] Consider the variety $V = \{xz = yz = 0\} \subset \mathbb{A}^3$ in the affine space. One has $V = V_1 \cup V_2$, where $V_1 = \{x = y = 0\}$ is the coordinate axis and $V_2 = \{z = 0\}$ the coordinate plane. For corresponding ideals one has $I(V) = (xz, yz) = (x,y) \cdot (z) = I_1 \cdot I_2$. The ideals $I_1 = I(V_1)$ and $I_2 = I(V_2)$ are prime, $I(V)$ is radical and $V = V_1 \cup V_2$ is the irreducible decomposition of V. The corresponding coordinate ring is $K[V] = K[x,y,z]/(xz, yz)$. Consider now the plane $W = \{x = z\} \subset \mathbb{A}^3$ with the ideal $I(W) = (x - z)$, and find the intersection $V \cap W$. The corresponding ideal is $I(V \cap W) = I(V) + I(W) = (xz, yz, x - z)$, the

coordinate ring $K[V \cap W] = K[x,y,z]/(xz, yz, x-z) \cong K[x,y]/(x^2, xy)$. This is not an affine algebra: it contains a nilpotent x. This reflects the fact that in some way the origin is a double point of the intersection $V \cap W$, since it belongs to both components of the variety V.

Examples show that, although radical ideals helped to avoid varieties with multiple components, the multiplicity still appears when one considers intersections of varieties. The notion of multiplicity is one of the fundamental notions in algebraic geometry. To work with it, one must assign multiplicities to subvarieties and in this way introduce a new type of objects. The codimension 1 case is the simplest, since each such subvariety can be defined by a single equation. We will consider only this case.

Definition. Let X be an irreducible nonsingular variety. Consider the set of all its irreducible subvarieties of codimension 1, and call its elements *simple divisors*. The free abelian group generated by this set is denoted $\operatorname{Div} X$ and called the *divisor group* of the variety X, its elements are *divisors* on X. A divisor is, therefore, a formal linear combination $D = n_1 C_1 + \cdots + n_k C_k$ of irreducible subvarieties $C_1, \ldots, C_k \subset X$ of codimension 1 with integer coefficients $n_1, \ldots, n_k \in \mathbb{Z}$. If all coefficients are nonnegative, we say that the divisor is *effective* and denote this by $D \geq 0$. Each divisor can be represented as a difference of two effective divisors. The number $d = n_1 + \cdots + n_k$ is called the *degree* of the divisor $D = n_1 C_1 + \cdots + n_k C_k$ and defines an epimorphism $\deg : \operatorname{Div}(X) \to \mathbb{Z}$.

Divisors introduced by this definition are called sometimes *Weil divisors*[13], as opposed to more general *Cartier divisor*, which will be introduced later.

To a rational function $f(t) = \frac{(t-P_1)^{n_1}\ldots(t-P_k)^{n_k}}{(t-Q_1)^{m_1}\ldots(t-Q_l)^{m_l}} \in K(t)$ on the affine line $X = \mathbb{A}^1$ one could associate a divisor $D = n_1 P_1 + \cdots + n_k P_k - m_1 Q_1 - \ldots - m_l Q_l$, as a formal linear combination of zeros and poles with corresponding multiplicities as coefficients, the so-called *divisor of zeros and poles* of the rational function. The analogous construction is possible in the general case. Let X be an irreducible variety and $f \in K(X)$ a rational function on X, $f \neq 0$. If $C \subset X$ is an irreducible subvariety of codimension 1, then it is locally defined by one equation, that is, in some nonempty open set $U \subset X$ one has $C \cap U = V(p)$ where $p \in K[U]$.

Definition. 1) If the function $f \in K[U]$, that is, it is regular on U, then, since the intersection $\bigcap(p^k) = 0$, $\exists k \geq 0$ such that $p^k \mid f$, $p^{k+1} \nmid f$. This integer is uniquely determined and does not depend on the choice of local parameter p. The number k is called the *order* of (regular) function f along subvariety C and denoted $k = \operatorname{ord}_C f$.

2) If the function f is not regular, it has a representation $f = g/h$ where $g, h \in K[U]$. The *order* of (rational) function f along subvariety C is defined as the integer $\operatorname{ord}_C f = \operatorname{ord}_C g - \operatorname{ord}_C h$. This number does not depend on the choice of nonempty open set U. This follows from irreducibility of X, since two nonempty open sets always intersect and their intersection is nonempty and open.

---

[13] after André Weil (1906–), French mathematician, one of the founders of the Bourbaki group, and not after Hermann Weyl (1885–1955), German mathematician and physicist.

Lemma. *Order of function along subvariety has the following properties:*
1) $\mathrm{ord}_C(fg) = \mathrm{ord}_C f + \mathrm{ord}_C g$;
2) $\mathrm{ord}_C(f+g) \geq \min\{\mathrm{ord}_C f,\ \mathrm{ord}_C g\} \quad (f+g \neq 0)$.

Lemma. *For a given rational function f there are only finitely many irreducible subvarieties C of codimension 1 for which* $\mathrm{ord}_C f \neq 0$.

Definition. If $f \in K(X)^*$ is a rational function, the formal linear combination $(f) = \sum_{C \subset X} (\mathrm{ord}_C f) \cdot C$ has finitely many terms and represents a divisor on X. It is called the divisor of the function f. The sum of all terms with positive coefficient is the *divisor of zeros* $(f)_0$, and with negative coefficient the *divisor of poles* $(f)_\infty$ of the function f. One has $(f)_0 \geq 0$, $(f)_\infty \geq 0$ and $(f) = (f)_0 - (f)_\infty$.

The mapping $\mathrm{div} : K(X)^* \to \mathrm{Div}(X)$, $f \mapsto (f)$ is a homomorphism of groups (the first group is multiplicative, the second one additive). Namely, one has $(fg) = (f) + (g)$.

The divisor of a regular function is effective. The converse also holds.

Lemma. *If $f \in K(X)^*$, then $(f) \geq 0 \Leftrightarrow f \in K[X]$.*

Proof. Let f be nonregular in $x \in X$. One has a representation $f = g/h \notin \mathcal{O}_x$, $g, h \in \mathcal{O}_x$. Since the ring $\mathcal{O}_x$ is factorial, one could consider g and h relatively prime. Let p be a prime factor of h, which does not divide g. The variety $V(p)$ has in some open neighborhood of x codimension 1, therefore $\overline{V(p)} = C \subset X$ is a subvariety of codimension 1 and $ord_C f < 0$.

Corollary. *On a nonsingular projective variety, rational function is determined uniquely up to constant factor by its divisor.*

Proof. If $(f) = (g)$, then $0 = (f) - (g) = (fg^{-1})$ and fg^{-1} is a global regular function on a projective variety, that is, constant.

Definition. Divisors of the form (f) where f is rational function on X, are called *principal divisors.* They form a subgroup $P(X) \subset \mathrm{Div}\, X$ of principal divisors in the group of all divisors. It is the image of the homomorphism $\mathrm{div} : K(X)^* \to \mathrm{Div}(X)$.

Is every divisor principal? In other words, could one represent a given divisor as a divisor of zeros and poles of some rational function? The answer depends on variety X and it is not always affirmative. There could be also nonprincipal divisors. More precise answer is given by the factorgroup $\mathrm{Div}(X)/P(X) = \mathrm{Cl}(X)$, the *divisor class group* of the variety X. This quotient introduces a relation of linear equivalence of divisors: $D_1 \sim D_2 \Leftrightarrow D_1 - D_2 = (f)$ for some global rational function f.

Examples. 1. $\mathrm{Cl}(\mathbb{A}^n) = 0$. More generally, if the ring $K[X]$ is factorial, then $\mathrm{Cl}(X) = 0$.

2. $\mathrm{Cl}(\mathbb{P}^n) = \mathbb{Z}$. [33, t. 1, p. 188], [31, p. 175]. Each irreducible subvariety $C \subset \mathbb{P}^n$ of codimension 1 is globally defined by a homogeneous equation, that is,

by irreducible homogeneous polynomial F, of degree m. Its affine parts are of the form $C \cap \mathbb{A}_0^n = V(F/x_0^m)$. Let $D = n_1C_1 + \cdots + n_kC_k$ be an effective divisor on $\mathbb{P}^n$ (with all $n_i > 0$), forms F_i define subvarieties C_i and let $F = F_1^{n_1} \cdots F_k^{n_k}$ be the corresponding product. Then $(F) = n_1(F_1) + \cdots + n_k(F_k) = D$ (more precisely, this holds in affine chart). In other words, each effective divisor on $\mathbb{P}^n$ is a divisor of a homogeneous polynomial form. Let now D be an arbitrary divisor, $D = D_1 - D_2$ its decomposition as difference of effective divisors, and $D_i = (G_i)$ $(i = 1, 2)$ their representation by homogeneous forms. Let $d_i = \deg D_i$ and $d = \deg D = d_1 - d_2$. Consider the rational function $f = G_1/x_0^d G_2$ and its principal divisor (f). This is a global rational function of degree 0, that is, an element of the field $K(\mathbb{P}^n)$. Its principal divisor is $(f) + dH = D_1 - D_2 = D$, where H is the divisor of the hyperplane $x_0 = 0$ (the *hyperplane section divisor*). This means that $D \sim dH$ and $\mathrm{Cl}(\mathbb{P}^n) = \mathbb{Z} \cdot H \cong \mathbb{Z}$.

Theorem. [31, p. 176] *Let X be a nonsingular variety, $Y \subset X$ its subvariety and $U = X \setminus Y$. Then*

(1) the mapping $\sum n_iC_i \mapsto \sum n_i(C_i \cap U)$ is an epimorphism $\mathrm{Cl}(X) \to \mathrm{Cl}(U)$;

(2) if $\mathrm{codim}_X Y \geq 2$, then it is an isomorphism $\mathrm{Cl}(X) \cong \mathrm{Cl}(U)$;

(3) if $\mathrm{codim}_X Y = 1$, then $1 \mapsto 1 \cdot Y$ defines a mapping $\mathbb{Z} \to \mathrm{Cl}(X)$ and the sequence $\mathbb{Z} \to \mathrm{Cl}(X) \to \mathrm{Cl}(U) \to 0$ is exact.

Example. If $Y \subset \mathbb{P}^2$ is an irreducible curve of degree d, then $\mathrm{Cl}(\mathbb{P}^2 \setminus Y) \cong \mathbb{Z}_d$. This can be easily proved by the previous theorem.

10. The divisor class group of nonsingular quadric and cone

Let us now determine the divisor class group of the nonsingular quadric Q. We shall represent the quadric by the so-called Segre embedding[14]. Stop for the moment to define the product of varieties. The set-theoretic (Cartesian) product of affine spaces is again an affine space: $\mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$, and similarly for corresponding closed subsets. However, for projective closed sets, the situation is more complex. How should one define a structure of a projective variety on the set-theoretic product of two projective lines? Define the Segre embedding $S : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$, $(x_0 : x_1) \times (y_0 : y_1) \mapsto (z_{00} : z_{01} : z_{10} : z_{11})$ with $z_{ij} = x_iy_j$. The image $S(\mathbb{P}^1 \times \mathbb{P}^1)$ is on the quadric $Q = \{z_{00}z_{11} = z_{01}z_{10}\} \subset \mathbb{P}^3$. Conversely, if the point $(z_{00} : z_{01} : z_{10} : z_{11}) \in Q$, then at least one coordinate, say $z_{00} \neq 0$, and $S((z_{00} : z_{01}) \times (z_{00} : z_{10})) = (z_{00}z_{00} : z_{00}z_{01} : z_{00}z_{10} : z_{01}z_{10}) = (z_{00} : z_{01} : z_{10} : z_{11})$. So, the mapping S defines bijection $\mathbb{P}^1 \times \mathbb{P}^1 \cong Q$, which makes it possible to transport the structure of algebraic variety, induced on the quadric Q from the ambient space $\mathbb{P}^3$, on the set $\mathbb{P}^1 \times \mathbb{P}^1$. Could one define this structure independently from the embedding? Homogeneous polynomial on Q has the form $F(z_{00}, z_{01}, z_{10}, z_{11}) = F(x_0y_0, x_0y_1, x_1y_0, x_1y_1) = G(x_0, x_1; y_0, y_1)$. This is a polynomial in two groups of variables, homogeneous in each group separately. The degree in each of the groups of variables need not to be equal: if $s = \deg_y G < \deg_x G = r$, then the equation

[14] Corrado Segre (1863–1924), Italian geometer, famous by his work in birational geometry.

$G = 0$ is equivalent to the system $y_0^{r-s}G = y_1^{r-s}G = 0$. Closed subsets in $\mathbb{P}^1 \times \mathbb{P}^1$ are defined by systems of polynomial equations of the form $G(x_0, x_1; y_0, y_1) = 0$, homogeneous in each group of variables separately. Subvarieties of codimension 1 in $\mathbb{P}^1 \times \mathbb{P}^1$ are defined by one such equation, as in standard projective space. Namely, if the polynomial $F(x_0, x_1; y_0, y_1)$ is homogeneous in each group of variables separately, and if F factorizes in product of two polynomials $F = G \cdot H$, then each of the factors must have the same homogeneity property. Let us determine the divisor class group $\mathrm{Cl}(\mathbb{P}^1 \times \mathbb{P}^1)$. The given divisor $D \in \mathrm{Div}(\mathbb{P}^1 \times \mathbb{P}^1)$, in addition to the usual degree $\deg D$, has two degrees $\deg_x D$ and $\deg_y D$ in each of the groups of variables, and one has $\deg D = \deg_x D + \deg_y D$. In this way, one obtains an epimorphism $\mathrm{Div}(\mathbb{P}^1 \times \mathbb{P}^1) \to \mathbb{Z}^2$, $D \mapsto (\deg_x D, \deg_y D)$. It is straightforward to check that its kernel is exactly the principal divisor subgroup, so $\mathrm{Cl}(\mathbb{P}^1 \times \mathbb{P}^1) \cong \mathbb{Z}^2$. The pair $(\deg_x D, \deg_y D)$ is called type of the divisor D. Segre embedding $S : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ defines a homomorphism $\mathrm{Div}(\mathbb{P}^3) \to \mathrm{Div}(\mathbb{P}^1 \times \mathbb{P}^1)$ by intersection with Q. It extends to classes of divisors, and coincides with the diagonal embedding $\mathrm{Cl}(\mathbb{P}^3) = \mathbb{Z} \to \mathbb{Z}^2 = \mathrm{Cl}(\mathbb{P}^1 \times \mathbb{P}^1)$, $1 \mapsto (1, 1)$.

Example. Apply this to the case of the projective space cubic C. It has the following parametrization:

$$z_{00} = u^3, \quad z_{01} = u^2 v, \quad z_{10} = uv^2, \quad z_{11} = v^3$$

Obviously, $C \subset Q$. Is it possible to represent C as intersection of the quadric and some surface? Consider the cone $K : z_{01}z_{11} = z_{10}^2$. The intersection is $K \cap Q = L \cup C$ where L is a line. The divisor class group is $\mathrm{Cl}(\mathbb{P}^3) = \mathbb{Z} \cdot H \cong \mathbb{Z}$ where H is the divisor of the (hyper)plane section, so $K \sim 2H$. The diagonal embedding gives $K = 2 \mapsto 2(1, 1) = (2, 2) = K \cap Q$. The type of this divisor is $K \cap Q = L + C = (2, 2)$, and the type of the divisor $L = (1, 0)$. Therefore, one has the type of $C = (2, 2) - (1, 0) = (1, 2)$. Let now $Y \subset \mathbb{P}^3$ be the surface such that its intersection with the quadric is $Y \cap Q = C$. Then the type of the divisor $Y \cap Q$ is, on one side, $rC = r(1, 2) = (r, 2r)$ and on the other, $dH = d(1, 1) = (d, d)$. Since $(r, 2r) \neq (d, d)$, this means that the answer to the above question is negative: there is no surface which would intersect the quadric Q by the curve C!

Consider the cone $X = V(xy - z^2) \subset \mathbb{A}^3$, with ideal $I = I(X) = (xy - z^2) \subset K[x, y, z]$ and coordinate ring $K[X] = K[x, y, z]/(xy - z^2)$, and determine its divisor class group. The generators of the ring, the images of the indeterminates x, y, z we will denote also x, y, z. The directrisse of the cone is the line $Y = V(y, z) \subset X \subset \mathbb{A}^3$, and this is an irreducible subvariety in X of codimension 1 – a simple divisor in X. Corresponding chain of ideals in $K[x, y, z]$ is

$$(0) \subset (xy - z^2) \subset (y, z) \subset (x, y, z)$$

However, after the factorization by $I(X)$ one obtains the ideal $I_X(Y) = (y, z) \subset K[X]$, which is of height 1 but not principal! The corresponding chain of ideals is

$$(0) \subset (xy - z^2) \subset (y, z) \subset (x, y, z)$$

If $(y,z) = (f)$ in $K[X]$, then the corresponding originals in $K[x,y,z]$ would satisfy $y, z \in (f, xy - z^2)$, $f \in (y,z,xy-z^2) = (y,z)$, and this gives a contradiction when one considers f modulo ideal $(x,y,z)^2$ (that is, its linear components). So, $Y \neq 0$ in $\mathrm{Cl}(X)$! Let us prove that $2Y = 0$ in $\mathrm{Cl}(X)$, or that $2Y$ is principal. Consider the function $y \in K[X]$, and find a local equation of the set $V(y) \cap X = Y$ in the open subset $U = D(x) \cap X$. Then $K[U] = K[x,y,z,x^{-1}]/(xy - z^2) = K[x,x^{-1},z]$, $y = x^{-1}z^2$. One has $Y \cap U = V(y,z) \cap U$, the corresponding coordinate ring is $K[Y \cap U] = K[x,x^{-1},z]/(x^{-1}z^2, z) = K[x,x^{-1},z]/(z)$. The local equation of Y in U is $z = 0$, the local parameter z. The function $y \in K[U]$ has the form $y = x^{-1}z^2$. Therefore $\nu(y) = 2$ and the principal divisor is $(y) = 2Y$. Now, there is the exact sequence $\mathbb{Z} \to \mathrm{Cl}(X) \to \mathrm{Cl}(X \setminus Y) \to 0$, where the first mapping is $1 \mapsto 1 \cdot Y$. The ring $K[X \setminus Y] = K[X \cap D(y)] = K[y, y^{-1}, z]$ is factorial, so $\mathrm{Cl}(X \setminus Y) = 0$. Therefore $\mathbb{Z} \to \mathrm{Cl}(X)$ is an epimorphism and $\mathrm{Cl}(X) = \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$.

11. Group of points of nonsingular cubic. Elliptic curves

As we have seen, the degree of the divisor defines a natural homomorphism of the divisor group on the group of integers $\mathrm{Div}(X) \to \mathbb{Z}$. In some cases it factors through principal divisors (that is, the principal divisors have degree 0) and defines epimorphism $\mathrm{Cl}(X) \to \mathbb{Z}$. This was the case for projective space. This is also the case for nonsingular projective curves.

Theorem. [33, t. 1, pp. 205–209] *If X is a nonsingular projective curve, the degree of any principal divisor is* 0.

The kernel $\mathrm{Cl}^0(X)$ of $\deg : \mathrm{Cl}(X) \to \mathbb{Z}$ is an important subgroup in $\mathrm{Cl}(X)$:

Theorem. *The following statements are equivalent:*

(1) the curve X is rational;

(2) the group $\mathrm{Cl}^0(X) = 0$, that is, $\mathrm{Cl}(X) \cong \mathbb{Z}$;

(3) there exist two different points $P, Q \in X$ such that $P \sim Q$.

Proof. If $\mathrm{Cl}^0(X) = 0$, each divisor of degree 0 is principal, and for any two different points $P, Q \in X$ there is a nonconstant rational function $f \in K(X)$ such that $P - Q = (f)$. This function defines a rational mapping $\varphi : X \to \mathbb{P}^1$ and $K(X) = K(f)$, P is a zero and Q is a pole of the function f.

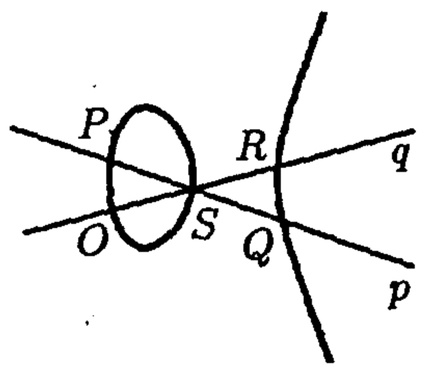
Theorem. *If X is a nonsingular cubic, then there exists a bijection $\mathrm{Cl}^0(X) = 0$, which induces the structure of Abelian group in the set of points of X.*

Proof. Let $O \in X$ be an arbitrary but fixed point. Define the mapping $X \to \mathrm{Cl}^0(X)$, $P \mapsto C_P = P - O$. It is injective since $C_P = C_Q \Rightarrow P - O \sim Q - O \Rightarrow P \sim Q$. In order to show that this mapping is also surjective, let us prove that any effective divisor $D \in \mathrm{Div}\, X$, $D > 0$, is equivalent to the divisor of the form $P + kO$, by induction on $\deg D$.

1. If $\deg D = 1$, then $D \sim P = P + 0 \cdot O$.

2. Let $\deg D > 1$. Then $D = D' + P$, $\deg D' = \deg D - 1$, $D' > 0$. By induction $D' \sim P + l \cdot O$. Then $D \sim P + Q + l \cdot O$. Find the point R such that

$P+Q \sim R+O$. We do this by a geometrical construction. Suppose that points P and Q are different, and let p be the line that they determine. Let S be the third point of intersection of that line and the cubic X. Let q be the line through O and S and let R be the third intersection point of the line q and cubic X. Then one has $P+Q+S \sim (p) \sim (q) \sim O+S+R$ and $P+Q \sim R+O$ (se the figure). In the case when some points coincide ($P=Q$ or $O=S$), one takes tangents instead of secants p and q.



We have proved that any effective divisor $D > 0$ on X is equivalent to the divisor of the form $P+kO$, where O is a fixed point. Obviously, $k = \deg D - 1$. If now D is a divisor of degree 0, then it is a difference of two effective divisors of the same degree $D = D_1 - D_2 \sim (R + k \cdot O) - (Q + k \cdot O) = R - Q$. Using the same geometrical construction as above in reverse order, one finds the point S as intersection of X and the line through R and O, and then point P as intersection of the line through Q and S (see the same figure). One obtains $P+Q \sim R+O$ or $D \sim R-Q \sim P-O = C_P$. Therefore, the mapping $P \mapsto C_P$ is bijective.

This bijection introduces a structure of an Abelian group on the set of points of the curve X. This structure is defined purely geometrically, by the constructions described above. The point O is the neutral element. If P and Q are two points of our curve, the point R is their sum, and $S = -R$. One could prove directly that this is a group. The most complicated part is the proof of associative law, elementary but long.

How many nonisomorphic nonsingular cubics do exist? We shall give the answer to this question for complex ground field $\mathbb{C}$. The equation of the plane nonsingular cubic is $y^2 = P_3(x)$ where the right-hand-side polynomial of the third degree does not have multiple roots. By translation and homothety in x one could obtain two of its three roots to be 0 and 1. In other words, $P_3(x) = x(x-1)(x-\lambda)$ where the third root $\lambda \neq 0, 1$ parametrizes all such curves. However, for different parameter values one could get isomorphic curves: curves $y^2 = x(x-1)(x+1)$ and $y^2 = x(x-1)(x-2)$ are obviously isomorphic by isomorphism $x \mapsto 1-x$.

The three element permutation group S_3 (with six permutations) acts on the root triple $(0, 1, \lambda)$. If we apply the linear transformation on x again after permutation, to obtain the root triple $(0, 1, \bar{\lambda})$, it is easy to check that $\bar{\lambda}$ could take one of the following six values: λ, $\frac{1}{\lambda}$, $1-\lambda$, $\frac{1}{1-\lambda}$, $\frac{\lambda}{\lambda-1}$, $\frac{\lambda-1}{\lambda}$. It follows directly that all six curves which correspond to these parameter values are isomorphic. Let us produce a function in λ, invariant with respect to this action and in this way

remove the six-ply ambiguity. An obvious candidate would be

$$Q(\lambda) = (\lambda+1)\Big(\frac{1}{\lambda}+1\Big)((1-\lambda)+1)\Big(\frac{1}{1-\lambda}+1\Big)\Big(\frac{\lambda}{\lambda-1}+1\Big)\Big(\frac{\lambda-1}{\lambda}+1\Big)$$
$$= -\frac{(\lambda+1)^2(\lambda-2)^2(2\lambda-1)^2}{\lambda^2(\lambda-1)^2}$$

and another

$$J(\lambda) = 1 - \frac{1}{27}Q(\lambda) = 1 + \frac{(\lambda+1)^2(\lambda-2)^2(2\lambda-1)^2}{27\lambda^2(\lambda-1)^2} = \frac{4}{27}\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$$

Definition. If X is a nonsingular cubic with the equation $y^2 = x(x-1)(x-\lambda)$ $(\lambda \neq 0, 1)$, the complex number

$$j(X) = 2^6 3^3 J = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$$

is called the *j-invariant* of the curve X.

The function $\lambda \mapsto j(X)$ defines a six-to-one covering $j : \mathbf{A}^1 \to \mathbf{A}^1$, $\Big\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\Big\} \mapsto j(X)$, branched over points 0 and 1. The value of the j-invariant classifies nonsingular cubics, as the following theorem shows.

Theorem. [15, p. 249], [31],... *a) Two cubics X are Y isomorphic $\Leftrightarrow$ $j(X) = j(Y)$.*

b) For any complex number a there is a curve X with $j(X) = a$.

Therefore, nonisomorphic nonsingular cubics are parametrized by points of complex line.

Nonsingular cubics are called also *elliptic curves.* This name originates from *elliptic integrals.* When the arc length of the ellipse (and other curves) is being calculated, the integrals of functions with radicals $\sqrt{P_4(x)}$ appear. In the spirit of lecture 1, these integrals are connected to curves $y^2 = P_4(x)$, which are birationally isomorphic to nonsingular cubics.

Classical theory of elliptic integrals culminated in the middle of the last century in the works of Legendre [15]. He reduced all elliptic integrals to the following three basic types: first type $F(\varphi) = \int_0^\varphi \frac{dx}{\sqrt{1-k^2\sin^2 x}}$, second type $E(\varphi) = \int_0^\varphi \sqrt{1-k^2\sin^2 x}dx$ and third type $G(\varphi) = \int_0^\varphi \frac{dx}{(\sin x - c)\sqrt{1-k^2\sin^2 x}}$. The arc length of the ellipse is expressed by the elliptic integral of the second type, and the first type appears in the arc length of the lemniscate. There is a family of curves with this property, discovered by Serret [28], which is connected to some interesting questions of the theory of elliptic curves and arithmetic. For more details see [23], [18].

As we have seen, the set of points of elliptic curve forms an Abelian group. What is this group?

Theorem. *As a group, the elliptic curve X is a two-dimensional torus:* $X \cong \mathbb{C}/\Lambda \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$.

Here $\Lambda \subset \mathbb{C}$ is a lattice, that is, a free additive subgroup $\Lambda = \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C}$ of rank 2 over $\mathbb{Z}$ ($\tau \notin \mathbb{R}$).

Proof. [31, pp. 414–416] We will sketch the proof. It requires some classical theory of complex functions.

Definition. The function $\wp(z) = \frac{1}{z^2} + \sum\limits_{\omega \in \Lambda \setminus \{0\}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$ of the complex argument z is called *Weierstrass function.*

The Weierstrass function and its derivative $\wp'(z) = -\sum_{\omega \in \Lambda} \frac{2}{(z-\omega)^3}$ are doubly periodic complex functions with periods 1 and τ, in other words Λ-periodic functions. They satisfy the equation $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$ where coefficients $g_2 = 60 \sum\limits_{\omega \in \Lambda \setminus \{0\}} \omega^{-4}$ and $g_3 = 140 \sum\limits_{\omega \in \Lambda \setminus \{0\}} \omega^{-6}$, and the discriminant $\Delta = g_2^3 - 27g_3^2 \neq 0$.

It follows from these properties that if the lattice Λ is given, then the mapping $\mathbb{C} \to \mathbb{P}^2(\mathbb{C})$ defined with $z \mapsto (\wp(z), \wp'(z))$ factors through homomorphism $\mathbb{C} \to \mathbb{C}/\Lambda$ and induces a bijection of the torus $\mathbb{C}/L$ and the cubic $y^2 = 4x^3 - g_2x - g_3$. Conversely, if the cubic is given, that is, two numbers g_2 and g_3 satisfying $\Delta = g_2^3 - 27g_3^2 \neq 0$, then one could show the existence of the lattice Λ such that its Weierstrass function satisfies the given equation.

One could obtain also the connection between j-invariant of the curve and its coefficients: $J = g_2^3/\Delta$ or $j(X) = 1728g_2^3/\Delta$.

Any lattice Λ or a complex number $\tau \notin \mathbb{R}$ defines an elliptic curve. Obviously, different values of τ could define isomorphic curves, exactly when their j-invariants coincide. The following theorem describes when this takes place.

Theorem. [31, p. 416] $J(\tau) = J(\tau') \Leftrightarrow \tau' = \frac{a\tau+b}{c\tau+d}$ *for some regular integer matrix* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$

In the sequel we shall show the connection between elliptic curves and number theory.

Let X be an elliptic curve with fixed origin O and corresponding group structure. For any $n \in \mathbb{N}$ one has the mapping $\varphi_n : X \to X$, $P \mapsto nP$ with $\varphi_n(O) = O$. One could show that this is a regular (polynomial) morphism and homomorphism of the group structure.

Definition. *Endomorphism* of the elliptic curve with fixed origin (X, O) is algebraic morphism $f : X \to X$ which maps the point O again in O.

If f and g are two endomorphisms, define their sum in a usual way, pointwise $(f+g)(P) = f(P) + g(P)$, and their product as composition $(f \cdot g)(P) = f(g(P))$. The zero-element will be the constant function $O(P) = O$, the neutral element - the identity $1(P) = P$.

Lemma. *Endomorphism of elliptic curve is a homomorphism of its group structure. The set* $\mathrm{End}(X,O)$ *of all endomorphisms is a ring.*

Theorem. [31, p. 417], [15, p. 18] *There exists a bijection between endomorphisms of the elliptic curve* (X,O) *and complex numbers* $\alpha \in \mathbb{C}$ *which leave the lattice invariant* $\alpha\Lambda \subset \Lambda$. *In such way, an embedding is defined.*

Proof. From the Serre's theorem on isomorphism of algebraic and analytical structures on complex algebraic varieties [27], algebraic morphisms $f : X \to X$ correspond to holomorphic morphisms $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$. Each such mapping extends to the mapping $\bar{f} : \mathbb{C} \to \mathbb{C}$, $\bar{f}(\Lambda) \subset \Lambda$. It is a holomorphic homomorphism in the neighborhood of 0, so $\bar{f}(z) = a_0 + a_1 z + a_2 z^2 + \cdots$ and $\bar{f}(z_1 + z_2) = \bar{f}(z_1) + \bar{f}(z_2)$. Comparing the coefficients in the equality $a_0 + a_1(z_1 + z_2) + a_2(z_1 + z_2)^2 + \cdots = (a_0 + a_1 z_1 + a_2 z_1^2 + \cdots) + (a_0 + a_1 z_2 + a_2 z_2^2 + \cdots)$ one obtains $a_0 = a_2 = a_3 = \cdots = 0$ and $\bar{f}(z) = a_1 z$.

So, $\mathrm{End}(X,O) = R = \{\alpha \in \mathbb{C} | \alpha\Lambda \subset \Lambda\}$ is a ring, $\mathbb{Z} \subset R \subset \mathbb{C}$.

Let us now analyze more closely rings of the form $R = \{\alpha \in \mathbb{C} | \alpha\Lambda \subset \Lambda\}$ where $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ ($\tau \notin \mathbb{R}$) is a given lattice. Note that $R \subset \Lambda$, $R\Lambda \subset \Lambda$, that is, the lattice Λ is a R-module.

Lemma. *Each* $\alpha \in R$ *is integral algebraic number, and* R *is a subring of the ring of integral algebraic numbers* $\mathbb{O}$.

Proof. $\alpha\Lambda \subset \Lambda \Leftrightarrow \alpha \cdot 1 = a + b\tau$, $\alpha \cdot \tau = c + d\tau$ where a, b, c, d are integers. Therefore, $(a - \alpha)(d - \alpha) - bc = 0$ and $\alpha^2 - (a + d)\alpha + (ad - bc) = 0$.

Clearly, integers do leave any lattice invariant, or $\mathbb{Z} \subset R$. When does the lattice admit nontrivial endomorphisms?

Lemma. *The ring* R *is strictly greater than the ring of integers* $\mathbb{Z} \Leftrightarrow \tau$ *is algebraic number of degree* 2 *over* $\mathbb{Q}$.

Proof. One has: $\exists \alpha \in R, \alpha \notin \mathbb{Z}, \alpha\Lambda \subset \Lambda \Leftrightarrow \exists a, b, c, d \in \mathbb{Z}, b \neq 0$ such that $\alpha \cdot 1 = a + b\tau$, $\alpha \cdot \tau = c + d\tau$, and by elimination of α one obtains $b\tau^2 + (a - d)\tau - c = 0$. Conversely, if $\tau \in \mathbb{Q}(\sqrt{-D}) = \mathbb{Q}[\sqrt{-D}]$ for some $D \in \mathbb{Z}$, $D > 0$, $\tau = r + s\sqrt{-D}$, then

$$\begin{aligned} R &= \{\alpha = a + b\tau \mid \alpha\tau = a\tau + b\tau^2 \in L\} = \{a + b\tau \in L \mid b\tau^2 \in L\} \\ &= \{a + b\tau \mid a, b, 2br, b(r^2 + Ds^2) \in Z\} \end{aligned}$$

since $b\tau^2 = -b(r^2 + Ds^2) + 2br\tau$. It is clear that R is strictly greater than $\mathbb{Z}$.

One has $R \subset O = \mathbb{O} \cap K$ where the field $K = \mathbb{Q}(\tau) = \mathbb{Q}[\tau] = \mathbb{Q}[\sqrt{-D}]$, and O is its ring of integers. Note that the lattice Λ is a projective R-module, since $R \otimes \mathbb{Q} = L \otimes \mathbb{Q} = \mathbb{Q}[\tau]$. One has $\mathrm{rank}_{\mathbf{Z}} R = \dim_{\mathbf{Q}} R \otimes \mathbb{Q} = \mathrm{rank}_{\mathbf{Z}} O = 2$. This means that for some $\rho \in O$, $O = \mathbb{Z} + \mathbb{Z}\rho$. Then $R \cap \mathbb{Z}\rho$ is a subgroup in $\mathbb{Z}\rho$, necessary of the form $R \cap \mathbb{Z}\rho = c \cdot \mathbb{Z}\rho$ for some positive integer $c \in \mathbb{N}$.

Lemma. *(& definition)* $R = \mathbb{Z} + c \cdot \mathbb{Z}\rho$. *The number* c *is called the conductor of the ring* R.

Proof. If $x = a + b\rho \in R$, then $b\rho = x - a \in R \cap \mathbb{Z}\rho = c \cdot \mathbb{Z}\rho$. In other words, $c \mid b$ and $x = a + c \cdot b'\rho$.

Example. Let $D = 1$, $K = \mathbb{Q}(i) = \mathbb{Q}[i]$ and $O = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$.

1. If $t = i$, then $R = O = \mathbb{Z}[i]$, $c = 1$ and $R = \mathbb{Z} + \mathbb{Z}i$.

2. If $t = 2i$, then $R = \mathbb{Z}[2i] \subsetneq O$, $c = 2$ and $R = \mathbb{Z} + 2\mathbb{Z}i = \{a + 2bi \mid a, b \in \mathbb{Z}\}$.

Let us return to elliptic curves. Integers correspond to "trivial" endomorphisms $\varphi_n : X \to X$, $P \mapsto nP$. Is it possible to describe all elliptic curves which allow also nontrivial endomorphisms? The answer is given by a wonderful theorem of number theory.

Definition. The elliptic curve $X = \mathbb{C}/\Lambda$ is a curve with *complex multiplication*, if $\mathrm{End}(X, O) \neq \mathbb{Z}$.

Theorem. *(Weber, Füter, Serre) If the curve X has complex multiplication, $R = \mathrm{End}(X, O)$ its ring of endomorphisms and $K = \mathbb{Q}[\sqrt{-D}]$ corresponding field of algebraic numbers, then*

(1) the invariant $j = j(X)$ is an integral algebraic number;

(2) Galois' group $\mathrm{Gal}(K(j)/K)$ is Abelian, of order $|\mathrm{Pic}(R)| = |\mathrm{Cl}(R)|$;

(3) number j is rational $\Leftrightarrow K(j) = K \Leftrightarrow |\mathrm{Cl}(R)| = 1 \Leftrightarrow$ ring O is factorial,

and there are exactly 13 such values for j:

D (discriminant)	c (conductor)	j (invariant)
1	1	$2^6 3^3$
2		$2^6 5^3$
3		0
7		$-3^3 5^3$
11		-2^{15}
19		$-2^{15} 3^3$
43		$-2^{18} 3^3 5^3$
67		$-2^{15} 3^3 5^3 11^3$
163		$-2^{18} 3^3 5^3 23^3 29^3$
1	2	$2^3 3^3 11^3$
3		$2^4 3^3 5^3$
7		$3^3 5^3 17^3$
3	3	$-2^{15} 3 \cdot 5^3$

The groups $\mathrm{Cl}(R)$ and $Pic(R)$ which appear in the theorem are the class group of fractional ideals of the ring R, and the class group of projective R-modules of rank 1.

The question how many factorial rings O exist, has been answered only recently. From classical theoretical considerations it followed that there are at most

ten, and the calculated tables for small values of D contained only nine such rings (the above table with conductor 1). It was a long-standing open problem whether there is tenth ring (the so called *problem of the tenth discriminant*). In 1967 Stark [29] answered negatively and showed that there is no such ring (see [12, p. 438], [3, p. 253]).

12. Cartier divisors and group of points of singular cubic

The notion of Weil divisor was introduced only for varieties that are nonsingular in codimension 1. In the case of curves, these are the nonsingular projective curves. But what about singular varieties? It would be possible to define divisors for arbitrary varieties as formal finite combinations $D = \sum n_i C_i$ of irreducible subvarieties of codimension 1. However, already the notion of principal divisor (and the divisor class group) does not work: the multiplicity of a rational function can not be always consistently defined along subvariety of codimension 1, since it may contain singular points. In this case one uses a different definition of divisor, suggested by connection between divisors and functions in projective space.

The notion of divisor occurs as the answer to a classical question: is there a rational function that has zeros ($n_i > 0$) and poles ($n_i < 0$) of given multiplicity n_i on given hypersurfaces C_i. If $D = \sum_i n_i C_i$ is a divisor on $\mathbb{P}^n$, each irreducible subvariety C_i of codimension 1 is globally defined by one polynomial homogeneous irreducible equation $g_i = 0$ and the solution of the problem is the rational function $f = \prod g_i^{n_i}$. This is a global rational function on $\mathbb{P}^n$ only if the degree of the divisor equals 0, that is, if $\sum_i n_i = 0$. However, in any affine chart $U_j = \{x_j \neq 0\}$ it defines a proper rational function $f_j = f/x_j^{(\Sigma n_i)}$. In addition, the family $\{U_j,\ f_j\}$ $(j = 0, \ldots, n)$ has the property that functions f_j/f_k have neither zeros nor poles on intersections $U_j \cap U_k$, since corresponding factors cancellate.

For arbitrary nonsingular variety X, in an analogous way, each Weil divisor $D = \sum n_i C_i$ on X defines a family $\{U_j,\ f_j\}$ consisting of covering U_j of X and of rational functions $f_j \in K(U_j)^*$ on each element of the covering, such that function f_j on U_j cuts out the principal divisor $(f_j) = D \cap U_j$, and rational functions f_j/f_k have neither zeros nor poles on intersections $U_j \cap U_k$. One needs nonsingularity in order to describe each C_i locally by one equation $g_i = 0$. Such a family $\{U_j,\ f_j\}$ is called *coherent system of functions*. Conversely, coherent system of functions $\{U_j,\ f_j\}$ on X defines a divisor $D = \sum n_i C_i$ on X: note that $K(U_j)$ is the field of fractions of the factorial domain $K[U_j]$ and represent f_j in the form $f_j = \prod g_{ij}^{n_{ij}}$. The coherency conditions uniquely determine subvarieties C_i and multiplicities n_i. Two coherent systems of functions $\{U_j,\ f_j\}$ and $\{V_k,\ g_k\}$ define the same divisor if and only if corresponding principal divisors coincide: $(f_j) = (g_k)$ on intersections $U_j \cap V_k$, that is, if rational functions f_j/g_k have neither zeros nor poles on $U_j \cap V_k$. This defines equivalence on the family of coherent systems of functions. Corresponding equivalence classes are called *locally principal* (or *Cartier divisors*. A Weil divisor corresponds to each Cartier divisor and vice versa, and this is a bijection.

I63

The good property of Cartier divisors is that they can be defined for arbitrary variety X, even when Weil divisors can not. The product of two Cartier divisors $\{U_j,\ f_j\}$ and $\{V_k,\ g_k\}$ is a Cartier divisor $\{U_j \cap V_k,\ f_j g_k\}$, and this defines a group structure on the set $\mathrm{Ca\,Div}(X)$ of Cartier divisors. Analogously to Weil divisors, this operation is written additively and called the sum. Every global rational function f on X defines a principal Cartier divisor $\{X,\ f\}$. This defines a homomorphism $K(X)^* \to \mathrm{Ca\,Div}(X)$. The quotient group of $\mathrm{Ca\,Div}(X)$ by the subgroup of principal divisors is the group of Cartier divisor classes $\mathrm{Ca\,Cl}(X)$.

If the variety X is nonsingular in codimension 1, then there exist both Weil and Cartier divisors. The construction of Weil divisor, corresponding to Cartier one, defines a homomorphism $\mathrm{Ca\,Cl}(X) \to \mathrm{Cl}(X)$. The construction of Cartier divisor shows that this is an inclusion. However, it does not have to be a surjection, as the example of the simple cone shows. In this case, the group $\mathrm{Cl}(X) = \mathbb{Z}_2$ is generated by the class of the directrisse L of the cone. This directrisse can not be defined by one equation in any neighborhood of cone's vertex, since any function which should describe L as a set of points, cuts out the divisor $2L$. Therefore, L is not locally principal, every locally principal divisor is principal, and $\mathrm{Ca\,Cl}(X) = 0$.

Let us now calculate the Cartier divisor class group of the singular cubic $X = V(y^2z - x^3) \subset \mathbb{P}^2$ (the "cusp"-curve). That will introduce group structure on its set of nonsingular points, exactly as in the case of nonsingular cubic. Our construction follows that of [31, p. 187]. First prove an important lemma.

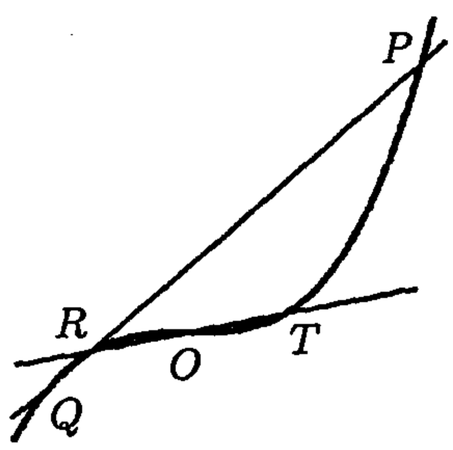
Lemma. ("removing the point from divisor's support"; (generalization see in [33, t. 1, p. 193]). *If X is a plane projective curve, $P \in X$ its point and $D \in \mathrm{Ca\,Div}(X)$ Cartier divisor on X, then there is a divisor $D' \sim D$ whose support does not contain the given point.*

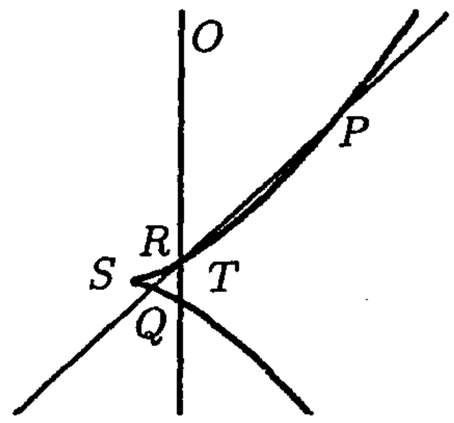
Proof. Let U be a neighborhood of P and f rational function defining locally principal divisor D in that neighborhood. Suppose that the support of the divisor contains the given point. This means that P is a zero or a pole of the function f, of some multiplicity n. Take a global rational function $g \in K(X)$ which in the point P has zero or pole of multiplicity n. The divisor $D' = D - (g)$ has the required property, since the function fg^{-1} is regular in some neighborhood of P.

Let now $X = V(y^2z - x^3) \subset \mathbb{P}^2$ with singular point $S = (0:0:1)$ and let $Y = X \setminus S$ be the nonsingular subvariety. Each Cartier divisor $D \in \mathrm{Ca\,Div}(X)$ is equivalent to divisor D' whose support does not contain the point S, that is, whose local equation does not have a pole in that point. Therefore, D' is a Weil divisor on Y. If D is principal, D' is such. The divisor D' has not to be uniquely determined, but its degree is. In such way, one defines the degree of divisor D, that is, a homomorphism $\mathrm{Ca\,Cl}(X) \to \mathbb{Z}$. Consider its subgroup $\mathrm{Ca\,Cl}(X)^0$ of divisor classes of degree 0 and, as in the case of nonsingular cubic, define a mapping $\varphi : Y \to \mathrm{Ca\,Cl}(X)^0$, $P \mapsto D_P = P - O$, where $O = (0:1:0)$ is a chosen point (point at infinity of the y-axis). One could also prove, by construction similar to nonsingular cubic case, that φ is a bijection. One should only note that if in the equality $P + Q = R + O$ points P and Q belong to Y, then the same holds for R.

The group operation on $\mathrm{Ca}\,\mathrm{Cl}(X)^0$ is therefore carried to Y. The construction of the point $P+Q$ is as before: if R is the third intersection point of the line through P and Q with the curve Y and T the third intersection point of line through R and O with the curve, then $P+Q=T$.

Note that $Y = X \setminus S \cong \mathbb{A}^1$ since the curve X is rational. The corresponding isomorphism is given by the formula $(x:y:z) \mapsto x/y$ and its inverse $t \mapsto (t:1:t^3)$. However, $\mathbb{A}^1$ has its usual structure of (additive) group, which is carried by this isomorphism to Y, and this is exactly the described group structure: if $P=(u:1:u^3)$ and $Q=(v:1:v^3)$, then $T=((u+v):1:(u+v)^3)$. Namely, if one switches to the chart $y \neq 0$, intersection of the curve $Y : z = x^3$ and the line $z = \alpha x + \beta$ are the points P, Q and R whose x-coordinates are the roots of the equation $x^3 - \alpha x - \beta = 0$, that is, u, v and $-(u+v)$ respectively (Viet's rule!). The point T is symmetric to R with respect to the origin. Therefore, its x-coordinate equals $u+v$, which proves the assertion (see the figures).





13. Sheaves and Czech cohomology

In the past 40 years homology became an indispensable tool in algebraic geometry. In the context of algebraic varieties these concepts are easily introduced via sheaf theory. Sheaves represent one of the most important contemporary techniques in algebraic geometry, and also in other geometrical theories, everywhere where one has local constructions and needs global invariants. Sheaves are the most important tool for globalization in modern geometry. In this short review it is not possible to develop the sheaf theory in its full extent. However, we will try to give some motivation, main definitions and examples.

In the definition of fundamental geometrical objects such as topological and differential manifolds, complex analytical and algebraic varieties, the same general method is used. First, one introduces and studies objects which play the role of local models. For example, local models of differential manifolds are open domains in $\mathbb{R}^n$. Then one builds global object from local models by procedure of gluing (identification).

Example. [20, p. 47] Two copies of the real line $\mathbb{R}^1$ can be glued along its open subsets $U = \mathbb{R}^1 \setminus \{0\}$ in different ways, with two different identification

functions $f : U \to U$. Using the function $f(x) = x$ one obtains the line with doubled origin 0, and using the function $f(x) = 1/x$ one obtains the circle—sphere S^1.

In the process of gluing one should take care of corresponding local structure. The local structure of a geometrical object is described by the set of permissible functions on that object. Continuous functions, differentiable functions, analytical functions, rational functions—all these are the classes of permissible functions for corresponding geometrical objects. By gluing of two local objects, identifying their parts, one must take care that on these common parts gluing takes permissible functions to permissible functions. One should know what permissible functions are, not only on the whole object, but also on its local parts. In such way one comes to a new type of structure, built by permissible functions. Let us explain it on the example of topological spaces, where the permissible functions are continuous functions. For any open subset $U \subset X$ one has a set $C(U)$ of all real continuous functions on U. It is a ring with respect to usual addition and multiplication of functions. If $V \subset U$, one has a homomorphism of rings $\rho_V^U : C(U) \to C(V)$ defined by restriction of functions $\rho_V^U(f) = f|_V$. Composition of restrictions is again a restriction: if $W \subset V \subset U$, then $\rho_W^V \circ \rho_V^U = \rho_W^U$. This provides us with the motivation for the following definition.

Definition. *Presheaf* of objects of a given category $\mathcal{C}$ (of sets, rings, Abelian groups,...) on a topological space X is a contravariant functor $\mathcal{F} : \mathrm{top}\, X \to \mathcal{C}$ from partially ordered structure of open sets in X (viewed as a category) to category $\mathcal{C}$. In other words, for each open subset $U \subset X$ there is an object $\mathcal{F}(U) \in \mathrm{Ob}\,\mathcal{C}$ of corresponding type (a set, a ring, an Abelian group,...), and for any inclusion of open sets $V \subset U$ there is a corresponding homomorphism $\rho_V^U : \mathcal{F}(U) \to \mathcal{F}(V)$, $\rho_V^U \in \mathrm{Mor}\,\mathcal{C}$, with the following properties:

1) $\rho_U^U = id$; 2) if $W \subset V \subset U$, then $\rho_W^V \circ \rho_V^U = \rho_W^U$.

One uses the term "restriction" and the notation $\rho_V^U(f) = f|_V$ also in the general case, although objects $\mathcal{F}(U)$ are not necessarily sets of functions, and homomorphisms ρ_V^U-restrictions of functions. Elements of the set $\mathcal{F}(U)$ are called sections of the sheaf $\mathcal{F}$ over the open set U. Sections over whole X are called global sections. In the sequel, all objects $\mathcal{F}(U)$ will have at least the structure of Abelian group, and therefore one could speak about their subobjects, quotient objects, kernels and images of homomorphisms etc.

Let us return to the presheaf of real continuous functions on topological space X. It has one specific property, concerning families of functions on coverings of X. Namely, if $\{U_\alpha\}$ is an open covering of X, then each continuous function f on X is uniquely determined by its restrictions $f|_{U_\alpha}$ on U_α. Conversely, a given family of functions f_α on U_α determines a global function on whole X if and only if functions f_α are coherent on intersections i.e., if for any two indexes and, $f_\alpha|_{U_\alpha \cap U_\beta} = f_\beta|_{U_\alpha \cap U_\beta}$. This property could be formalized in the following manner.

Definition. Presheaf $\mathcal{F}$ on a topological space X is a *sheaf* if for any open subset U and its open cover $\{U_\alpha\}$ the following sequence of homomorphisms is

exact:

$$0 \to \mathcal{F}(U) \xrightarrow{\varphi} \prod_{\alpha} \mathcal{F}(U_\alpha) \xrightarrow{\psi} \prod_{\alpha,\beta} \mathcal{F}(U_\alpha \cap U_\beta)$$

where $\varphi : f \mapsto \{f|_{U_\alpha}\}$, $\psi : \{f_\alpha\} \mapsto \{f_\alpha|_{U_\alpha \cap U_\beta} - f_\beta|_{U_\alpha \cap U_\beta}\}$. In other words, $\operatorname{Ker}\varphi = 0$, that is, if the families of restrictions of two sections coincide then these two sections itself also coincide; and $\operatorname{Ker}\psi = \operatorname{Im}\varphi$, that is, any family of sections which coincide on intersections originates from some global section.

All important presheaves which we have already mentioned, are in fact sheaves. Such are: the sheaf of differentiable functions on a smooth manifold, the sheaf of analytical functions on a complex-analytic variety etc. In the case of sheaves, one could give the interpretation of sections and restrictions as proper functions and corresponding restrictions, by technique of étalé spaces. Even when a presheaf is not a sheaf, one could associate a sheaf to it, called *associated sheaf*, which is locally equal to given presheaf.

Example. If the space X has two connected components and $\mathcal{F} = \mathcal{Z}$ is a presheaf of constant functions with integer values (that is, for any open subset U, $\mathcal{F}(U) = \mathbb{Z}$) then it is not a sheaf: a family of two functions, one on each component, which take two different values (say 0 and 1), agrees on intersections (they are all empty), but does not originate from a global section.

Let $\mathcal{F}$ be a (pre)sheaf on X, $x \in X$ a point, U and V its open neighborhoods. One says that two sections $f \in \mathcal{F}(U)$ and $g \in \mathcal{F}(V)$ (over different neighborhoods) are equivalent if their restrictions coincide in some common neighborhood $W \subset U \cap V$. The quotient of the disjoint union $\coprod_{U:x\in U} \mathcal{F}(U)$ of all sections over all neighborhoods of a given point is called *germ* of a (pre)sheaf $\mathcal{F}$ at the point x and denoted $\mathcal{F}_x$. For example, an element of germ of sheaf of continuous functions at the point x is a function continuous in some neighborhood of that point, and two such functions are identified if they coincide in some (maybe smaller) neighborhood of x. The associated sheaf may be defined in the following way. Consider the disjoint union $\coprod_{x\in X} \mathcal{F}_x = E$ and the corresponding projection $\omega : E \to X$, $\mathcal{F}_x \to x$. Let E be topologized by the smallest (coarsest) topology in which ω is still continuous. One obtains the *étalé space* of the presheaf $\mathcal{F}$. For any open $U \subset X$, define $\mathcal{F}^+(U) = \Gamma(U, \mathcal{F})$ as a set of all continuous functions $s : U \to E$ such that $i = \omega \circ s : U \to E \to X$ is the identity on U. In this way one obtains a sheaf $\mathcal{F}^+$, the *associated sheaf* of the presheaf $\mathcal{F}$. What is the direct connection between and $\mathcal{F}(U)$? An element $s \in \mathcal{F}^+(U)$ can be interpreted as a family of sections $s_\alpha \in \mathcal{F}(U_\alpha)$, coherent on intersections $U_\alpha \cap U_{\alpha'}$, where $\mathcal{U} = \{U_\alpha\}$ is an open cover of U. Two such families of sections in two different coverings $\mathcal{U}$ and $\mathcal{V}$ are identified if they agree on cross-intersections $U_\alpha \cap V_\beta$. Presheaf $\mathcal{F}$ and associated sheaf $\mathcal{F}^+$ have equal germs $\mathcal{F}_x = \mathcal{F}^+_x$.

Example. Associated sheaf $\mathcal{F}^+$ of the presheaf $\mathcal{F}$ of constant functions on a topological space X is the sheaf of locally constant functions. Their germs coincide in each point (these are the functions, constant in some neighborhood of given point). Even their sections on each connected component of the space coincide. However, if the space has more than one component, then $\mathcal{F}^+ \neq \mathcal{F}$.

Morphism of sheaves is introduced in a standard categorical way: it is a natural transformation of functors. More precisely, morphism $\alpha : \mathcal{F} \to \mathcal{G}$ consists of a family of homomorphisms $\alpha_U : \mathcal{F}(U) \to \mathcal{G}(U)$ commuting with restrictions: $\alpha_V \circ \rho^U_{V,F} = \rho^U_{V,G} \circ \alpha_U$. If all homomorphisms $\alpha_U : \mathcal{F}(U) \subset \mathcal{G}(U)$ are inclusions, we say that $\mathcal{F} \subset \mathcal{G}$ is a subsheaf. The definition of quotient sheaf is more complicated. Namely, if $\mathcal{F} \subset \mathcal{G}$ is a subsheaf, quotient groups $\mathcal{G}(U)/\mathcal{F}(U)$ form only a presheaf. By definition, a *quotient sheaf* $\mathcal{G}/\mathcal{F}$ is the corresponding associated sheaf. One could write $(\mathcal{G}/\mathcal{F})(U) = [\mathcal{G}(U)/\mathcal{F}(U)]^+$. Due to this construction, sections of the exact sequence of sheaves need not build an exact sequence. In other words, functor of sections is not right exact: if the sequence $0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{G}/\mathcal{F} \to 0$ is exact, only the sequence $0 \to \mathcal{F}(U) \to \mathcal{G}(U) \to (\mathcal{G}/\mathcal{F})(U)$ will be exact, and the last homomorphism need not be epimorphism. To the contrary, the functor of germs is exact: if the sequence $0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{G}/\mathcal{F} \to 0$ is exact, then for all x sequence $0 \to \mathcal{F}_x \to \mathcal{G}_x \to (\mathcal{G}/\mathcal{F})_x \to 0$ is also exact (and vice versa).

Examples. 1. [20, p. 51] Let $X = S^1$. Consider the sheaf $\mathcal{C}$ of continuous functions on X, its subsheaf $\mathcal{Z}$ of all constant functions and presheaf $\mathcal{F}(U) = \mathcal{C}(U)/\mathcal{Z}(U)$. Cover X with two open sets: two half-circles overlapping at both ends, $X = U_1 \cup U_2$, $U_1 \cap U_2 = V_1 \cup V_2$. Let $f = 0$ be the zero-function on X, g a continuous function on X which equals 0 on V_1 and 1 on V_2 and let $f_1 = f|_{U_1}$, $f_2 = g|_{U_2}$. Then, obviously $f_1|_{V_1} - f_2|_{V_1} = 0$, $f_1|_{V_2} - f_2|_{V_2} = 1$. The pair $\{f_1, f_2\}$ defines a section of the sheaf $\mathcal{F}^+ = \mathcal{C}/\mathcal{Z}$ over U which does not originate from $\mathcal{F}(U) = \mathcal{C}(U)/\mathcal{Z}(U)$.

2. [7, p. 134] If $X = \mathbb{C}$, $\mathcal{O}$ the sheaf of holomorphic functions on X and $\mathcal{O}^*$ the sheaf of (multiplicative groups of) holomorphic functions which are everywhere different from 0, the morphism $\exp : \mathcal{O} \to \mathcal{O}^*$, locally defined by $f \mapsto \exp(f)$ is an epimorphism of sheaves, since it is epi on germs: any holomorphic function different from 0 at the point x may in some neighborhood of that point be written as $\exp(f)$ for some holomorphic function f. However, if U is the open ring around 0, then $\exp_U : \mathcal{O}(U) \to \mathcal{O}^*(U)$ is not surjective.

Let us return to algebraic varieties. If X is an algebraic variety over algebraically closed field K, then generally there is no natural topology on the set X. The only topology which we could use is the Zariski topology. Which are the permissible functions? If $U \subset X$ is an open subset, let $\mathcal{O}(U)$ be the ring of regular functions on U. One obtains a sheaf $\mathcal{O}$ of rings on X, the *structure sheaf* of regular functions on X. If instead of regular, one takes rational functions and lets $\mathcal{K}(U)$ be the field of rational functions on U, one gets the sheaf $\mathcal{K}$ of fields of rational functions on X. This is a constant sheaf if X is irreducible.

Let us mention an important short exact sequence of sheaves (of multiplicative groups): $0 \to \mathcal{O}^* \to \mathcal{K}^* \to \mathcal{K}^*/\mathcal{O}^* \to 0$. If one compares the definition of Cartier divisor and the definition of quotient sheaf $\mathcal{K}^*/\mathcal{O}^*$, one sees that Cartier divisor on X is the same as global section of the sheaf $\mathcal{K}^*/\mathcal{O}^*$, that is, an element of the group $(\mathcal{K}^*/\mathcal{O}^*)(X) = \Gamma(X, \mathcal{K}^*/\mathcal{O}^*)$. How to describe principal Cartier divisors? These are the classes of those coherent systems of functions $\{U_\alpha, f_\alpha\}$ for which there is a global function f such that $f_\alpha = f|_{U_\alpha}$. In other words, this is the image of the last

morphism in the sequence of global sections $0 \to \mathcal{O}^*(X) \to \mathcal{K}^*(X) \to (\mathcal{K}^*/\mathcal{O}^*)(X)$ which needs not to be a surjection. Note one fact. Let $\{U_\alpha, f_\alpha\}$ be coherent system of (rational) functions. This means that on all $U_\alpha \cap U_\beta$, functions $g_{\alpha\beta} = f_\alpha/f_\beta$ are regular and different from 0, that is, $g_{\alpha\beta} \in \mathcal{O}^*(U_\alpha \cap U_\beta)$. However, the system $\{g_{\alpha\beta}\}$ is not arbitrary - it satisfies some special coherency conditions. For any index triple (α, β, γ) one should have $g_{\alpha\beta}g_{\beta\gamma} = f_\alpha/f_\beta \cdot f_\beta/f_\gamma = f_\alpha/f_\gamma = g_{\alpha\gamma}$ on the intersection $U_\alpha \cap U_\beta \cap U_\gamma$. These conditions could be written in the form $g_{\beta\gamma}g_{\alpha\gamma}^{-1}g_{\alpha\beta} = 1$ and called the cocycle conditions. This homological terminology has its explanation, as we will shortly see.

The exact sequence in the definition of sheaf extends naturally into a complex, *Czech complex* of the sheaf, determined by the given covering. Let $\mathcal{F}$ be a sheaf on a topological space X and $\mathcal{U} = \{U_\alpha\}$ an open covering of X. Introduce the notation $U_{\alpha_0\alpha_1\ldots\alpha_k} = U_{\alpha_0} \cap U_{\alpha_1} \cap \ldots \cap U_{\alpha_k}$ and define the cochain group $C^k(\mathcal{U}, \mathcal{F}) = \prod_{(\alpha_0,\alpha_1,\ldots,\alpha_k)} \mathcal{F}(U_{\alpha_0\alpha_1\ldots\alpha_k})$ for any $k \geq 0$ and also differentials $d = d^k : C^k(\mathcal{U}, \mathcal{F}) \to C^{k+1}(\mathcal{U}, \mathcal{F})$ with

$$d(\{s_{\alpha_0\alpha_1\ldots\alpha_{k+1}}\}) = \Big\{ \sum_{0\leq i\leq k+1} (-1)^i s_{\alpha_0\alpha_1\ldots\hat{\alpha}_i\ldots\alpha_{k+1}}|_{U_{\alpha_0\alpha_1\ldots\alpha_{k+1}}} \Big\}$$

Therefore, $d^0 : \{s_\alpha\} \mapsto \{(s_\beta - s_\alpha)|_{U_{\alpha\beta}}\}$, $d^1 : \{s_{\alpha\beta}\} \mapsto \{(s_{\beta\gamma} - s_{\alpha\gamma} + s_{\alpha\beta})|_{U_{\alpha\beta\gamma}}\}$ etc. Direct calculation shows that this is a proper differential, that is, $d^2 = 0$. One obtains Czech complex $C^0(\mathcal{U}, \mathcal{F}) \xrightarrow{d^0} C^1(\mathcal{U}, \mathcal{F}) \xrightarrow{d^1} C^2(\mathcal{U}, \mathcal{F}) \to \cdots$. Its cohomology groups $H^i(\mathcal{U}, \mathcal{F}) = \operatorname{Ker} d^i / \operatorname{Im} d^{i-1}$ $(i > 0)$, $H^0(U, \mathcal{F}) = \operatorname{Ker} d^0$ are called *Czech cohomology groups* of the sheaf $\mathcal{F}$ on the space X corresponding to covering $\mathcal{U}$. If one orders the set of indexes (for example, if the covering is finite) and leaves in the definition of C_k only all increasing k-tuples $\alpha_0 < \alpha_1 < \ldots < \alpha_k$, that is, if we eliminate all terms of the product which differ only by the sequence of open sets, one could check that cohomology will not change. In the same manner, if the covering has finite dimension, that is, if there exists an integer d such that the intersection of any $d+1$ elements of the covering is empty, then the cochains C_i for $i > d$ are trivial, Czech complex is finite and corresponding cohomologies are trivial starting from the position $d+1$. All this simplifies the explicit calculation.

The sheaf condition for $\mathcal{F}$ could be written also as $H^0(\mathcal{U}, \mathcal{F}) = \Gamma(X, \mathcal{F}) = \mathcal{F}(X)$. Let us note that this does not depend on the covering $\mathcal{U}$, thus justifying the notation $H^0(\mathcal{U}, \mathcal{F}) = H^0(X, \mathcal{F})$. This may not be so for higher cohomologies. In the general case, relation of refinement of coverings gives us the connection between cohomology groups of the same sheaf over two different coverings, and one takes the direct limit by all coverings. This theory has been developed by Cartan, Leray and Serre. Soon afterwards, Grothendieck has founded cohomological theory for sheaves in a more general context, using resolvents and derived functors. A very nice exposition of this theory may be found in [31]. We shall not discuss the general cohomological theories in this short report. For us it will do, that there exist cohomological groups $H^i(X, \mathcal{F})$ which do not depend on the covering and which satisfy all usual theorems of homology theory, and also that the calculation

of Czech cohomology, described above, gives good results for some "well chosen" coverings. One of the most important results in homological algebra is the so-called long cohomological sequence: if $0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to 0$ is a short exact sequence of sheaves, then there exists a long exact sequence of cohomology

$$\begin{array}{l} 0 \to H^0(X,\mathcal{F}) \to H^0(X,\mathcal{G}) \to H^0(X,\mathcal{H}) \\ \qquad\qquad\qquad\qquad\qquad\qquad \swarrow \\ \qquad\qquad\qquad H^1(X,\mathcal{F}) \to H^1(X,\mathcal{G}) \to H^1(X,\mathcal{H}) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \swarrow \\ \qquad\qquad\qquad\qquad\qquad H^2(X,\mathcal{F}) \to H^2(X,\mathcal{G}) \to \cdots \end{array}$$

The beginning of the sequence is just the left exact sequence of global sections.

Examples. 1. [31, p. 284] Let $X = S^1$ be the one-dimensional sphere with the (already introduced) covering by two overlapping half-circles $\mathcal{U} = \{U_1, U_2\}$, $X = U_1 \cup U_2$, $U_1 \cap U_2 = V_1 \cup V_2$ and let $\mathcal{F} = \mathcal{Z}$ be the constant sheaf. One has $C^0(\mathcal{U},\mathcal{F}) = \mathcal{F}(U) \times \mathcal{F}(V) = \mathbb{Z} \times \mathbb{Z}$, $C^1(U,\mathcal{F}) = \mathcal{F}(U \cap V) = \mathbb{Z} \times \mathbb{Z}$ and the corresponding differential in the Czech complex $0 \to C^0(\mathcal{U},\mathcal{F}) \xrightarrow{d} C^1(\mathcal{U},\mathcal{F}) \to 0 \to \cdots$ is $d : (a,b) \mapsto (b-a, b-a)$. Cohomology groups are $H^0(\mathcal{U},\mathcal{F}) = \operatorname{Ker} d = \mathbb{Z}$ and $H^1(\mathcal{U},\mathcal{F}) = \operatorname{Coker} d = C^1(\mathcal{U},\mathcal{F})/\operatorname{Im} d = \mathbb{Z}$.

2. [6, p. 61] Let $X = \mathbb{P}^1$ be the complex projective line with homogeneous coordinates u, v and usual affine covering $\mathcal{U} = \{U, V\}$, $U = \{v \neq 0\}$, $V = \{u \neq 0\}$, $U \cap V = \mathbb{C}^*$ and $\mathcal{F} = \mathcal{O}$ the sheaf of holomorphic functions. One has $C^0(\mathcal{U},\mathcal{O}) = \mathcal{O}(U) \times \mathcal{O}(V)$, $C^1(\mathcal{U},\mathcal{O}) = \mathcal{O}(U \cap V)$ and the differential $d : (f,g) \mapsto g - f$ where $f = \sum_{n\geq 0} a_n u^n \in \mathcal{O}(U)$, $g = \sum_{n\geq 0} b_n v^n \in \mathcal{O}(V)$. On the intersection $U \cap V$ one has $v = u^{-1}$ and

$$g - f = 0 \Leftrightarrow \sum_{n\geq 0} b_n u^{-n} - \sum_{n\geq 0} a_n u^n = 0 \Leftrightarrow a_0 = b_0,\ a_n = b_n = 0\ (n > 0)$$

Therefore, $H^0(\mathcal{U},\mathcal{O}) = \mathbb{C}$, that is, global holomorphic functions on X are only constants. For H^1 one gets

$$H^1(\mathcal{U},\mathcal{O}) = C^1(\mathcal{U},\mathcal{O})/\operatorname{Im} d = C[u,u^{-1}]\Big/\Big(\sum a_i u^i - \sum b_i u^{-i}\Big) = 0.$$

3. [9, p. 34] Let us calculate the cohomology groups of the structure sheaf on nonprojective quasiprojective algebraic variety. Let $X = \mathbb{A}^2 \setminus \{(0,0)\}$ be the plane without the origin, with coordinates u, v and covering $\mathcal{U} = \{U, V\}$, $U = \{v \neq 0\} = D(v)$, $V = \{u \neq 0\} = D(u)$ and let $\mathcal{O}$ be the sheaf of regular functions on X. One has $\mathcal{O}(U) = \mathcal{O}(D(v)) = K[u,v]_{(v)} = K[u,v,v^{-1}]$, $C^0(\mathcal{U},\mathcal{O}) = K[u,v,u^{-1}] \times K[u,v,v^{-1}]$ and $C^1(\mathcal{U},\mathcal{O}) = \mathcal{O}(U \cap V) = K[u,v,u^{-1},v^{-1}]$, and also $d : (f,g) \mapsto g - f$. One gets $H^0(\mathcal{U},\mathcal{O}) = \operatorname{Ker} d = K[u,v] = H^0(\mathbb{A}^2,\mathcal{O})$, that is, regular functions on X can be extended to the whole plane $\mathbb{A}^2$. Let us calculate now $H^1(\mathcal{U},\mathcal{O}) =$

$K[u, v, u^{-1}, v^{-1}]/\operatorname{Im} d = K[\{u^{-m}, v^{-n} | m, n > 0\}]$, therefore $\dim_K H^1(\mathcal{U}, \mathcal{O}) = \infty$. The dimension of cohomology groups is not necessarily finite.

4. [31, p. 284] Let us calculate cohomology groups of the sheaf of regular differential forms on the projective line. Let again $X = \mathbb{P}^1$ with usual coordinates and affine covering, and let Ω be the sheaf of regular differential forms [31, p. 224]. One has $C^0(\mathcal{U}, \Omega) = \Omega(U) \times \Omega(V) = K[u]du \times K[v]dv$, $C^1(\mathcal{U}, \Omega) = \Omega(U \cap V) = K[u, u^{-1}]du$ and $d : u \mapsto u$, $v \mapsto u^{-1}$, $dv \mapsto -u^{-2}du$. Now, $\operatorname{Ker} d = \{(f(u)du, g(v)dv) \mid f(u) + u^{-2}g(u^{-1}) = 0\} = 0$ (where f and g are polynomials), and $H^0(\mathcal{U}, \Omega) = 0$. Further,

$$\operatorname{Im} d = \{(f(u) + u^{-2}g(u^{-1}))\, du\} = \operatorname{Span}_K \{u^n du \mid n \in \mathbb{Z} \setminus \{-1\}\} \subset K[u, u^{-1}]du$$

so $H^1(\mathcal{U}, \Omega) = K \cdot u^{-1}du$ and $\dim_K H^1(\mathcal{U}, \Omega) = 1$.

14. Genus of algebraic variety

14.1. Topological genus of projective algebraic curve. Plane projective algebraic nonsingular curve (over the field of complex numbers) is a 2-dimensional compact smooth orientable manifold in $\mathbb{C}^2 = \mathbb{R}^4$. As it is known, such manifolds are uniquely classified by one integer parameter—topological genus g (this is the number of "handles" on X). This number is called *topological genus* of the corresponding nonsingular curve.

14.2. Arithmetical genus of projective variety. Theorem. (Hilbert's syzygy theorem) *Let $A = \mathbb{C}[x_0, \dots, x_n]$ and M finitely generated graded A-module ($M = \bigoplus_{k \geq 0} M_k$ as an Abelian group, and for any homogeneous polynomial f of degree d, $f \cdot M_k \subset M_{k+d}$). Then there exists a polynomial $P_M(t) \in \mathbb{Q}_n[t]$ with rational coefficients, of degree at most n, such that $\dim_{\mathbb{C}} M_k = p_M(k)$ for $k \gg 0$.*

Proof. Induction on n. 1. For $n = -1$, $A = \mathbb{C}$, M is a finite-dimensional $\mathbb{C}$-vector space, $M_k = 0$ for $k \gg 0$ and $P_M = 0$.

2. The inductive step. Multiplication homomorphism $\varphi : M_k \xrightarrow{\cdot x_n} M_{k+1}$ has kernel $\operatorname{Ker} \varphi = N' = \{m \in M : x_n m = 0\}$ and cokernel $\operatorname{Coker} \varphi = N'' = M/x_n M$, so one has an exact sequence of vector spaces

$$0 \to N'_k \to M_k \xrightarrow{\varphi} M_{k+1} \to N''_{k+1} \to 0$$

from which one has

$$\dim M_{k+1} - \dim M_k = \dim N''_{k+1} - \dim N'_k$$

Since multiplication with x_n annulates N' and N'', one can view it as finitely generated $\mathbb{C}[x_1, \dots, x_{n-1}]$-modules. By the induction hypothesis, $\dim N'_k = P'(k)$, $\dim N''_{k+1} = P''(k+1)$. We will use the following elementary lemma on polynomials.

Lemma. For any rational polynomial $f \in \mathbb{Q}[t]$ of degree d there exists a polynomial $g \in \mathbb{Q}[t]$ of degree $d+1$ such that $f(t) = g(t+1) - g(t)$.

Proof. Since $(t+1)^d - t^d = d \cdot t^{d-1} + \cdots$, the lemma follows by induction on degree of f.

From the lemma, $P''(k+1) - P'(k) = Q(k+1) - Q(k)$ for some polynomial Q, and

$$\dim M_{k+1} - \dim M_k = \dim N''_{k+1} - \dim N'_k = P''(k+1) - P'(k) = Q(k+1) - Q(k)$$

Therefore, $\dim M_k = Q(k) +$ const for $k \gg 0$. This proves the theorem.

Definition. If $X \subset \mathbb{P}^n$ is a projective algebraic variety and $M = \mathbb{C}[X] = \mathbb{C}[x_0, \ldots, x_n]/I(X)$ its homogeneous coordinate ring, viewed as $\mathbb{C}[x_0, \ldots, x_n]$-module, polynomial $P_X(t) := P_M(t)$ is called *Hilbert polynomial* of X.

Examples. 1) Projective n-dimensional space: $M = A = \mathbb{C}[x_0, \ldots, x_n]$, $M_k = \{$homogeneous forms of degree k with $n+1$ indeterminates$\}$, $\dim M_k = \binom{k+n}{n}$ and $P_M(t) = \binom{t+n}{n} = 1 \cdot t^n/n!$.

2) Projective hypersurface of degree d: $M = A/(f)$, where f is homogeneous of degree d. From the exact sequence $0 \to A_{k-d} \xrightarrow{\cdot f} A_k \to [A/(f)]_k \to 0$ one has $\dim[A/(f)]_k = \binom{k+n}{n} - \binom{k-d+n}{n}$ and $P_M(t) = \binom{t+n}{n} - \binom{t+n-d}{n} = d \cdot \frac{t^{n-1}}{(n-1)!} + \cdots$.

3) Particularly, for $n = 2$, that is, for plane projective algebraic curves of degree d one has $P_M(t) = \binom{t+2}{2} - \binom{t+2-d}{2} = d \cdot t + (1 - \frac{(d-1)(d-2)}{2})$.

Note that if $f \in \mathbb{Q}[t]$ is a rational polynomial of degree n such that in $n+1$ consequent integer points $k, k+1, \ldots, k+n \in \mathbb{Z}$ it has integer values, then it can be written in the form $P(t) = a_n\binom{t}{n} + a_{n-1}\binom{t}{n-1} + \cdots + a_0$ with integer coefficients. Therefore, the highest order coefficient of the Hilbert polynomial has the form $d/n!$ ($d \in \mathbb{Z}$), which can be guessed from previous examples. Examples also show that the degree of Hilbert polynomial equals the dimension of projective variety X. This is really so. One can show that not only the degree, but also the whole polynomial (all its coefficients) is an invariant of the variety, independent from the embedding $X \subset \mathbb{P}^n$. Some of the coefficients (the first and the last) have a special meaning and geometrical interpretation.

Definition. Let $P_X(t) = d \cdot \frac{t^r}{r!} + \cdots + P_X(0)$. The coefficient d is called *degree* of projective variety X. The integer $p_a(X) := (-1)^r[P_X(0) - 1]$ is called *arithmetical genus* of the variety X.

Example. Arithmetical genus of the plane algebraic nonsingular curve of degree d equals $(d-1)(d-2)/2$.

One can see that the definition of arithmetical genus really does not depend on the embedding $X \subset \mathbb{P}^n$ when it is expressed in terms of structure sheaf of the variety. Namely, if $\mathfrak{F}$ is a sheaf on X, its Euler characteristic is defined by $\chi(\mathfrak{F}) = \dim H^0(X, \mathfrak{F}) - \dim H^1(X, \mathfrak{F}) + \cdots$. One could prove that Euler characteristic of the structure sheaf $\mathcal{O}$ of regular functions on a variety X equals $\chi(\mathcal{O}) = P_X(0)$. Therefore, the arithmetic genus of nonsingular projective variety $X \subset \mathbb{P}^n$ equals $p_a(X) = (-1)^r[\chi(\mathcal{O}) - 1]$ where $r = \dim X$. For curves this is reduced to equality $p_a(X) = \dim H^1(X, \mathcal{O}) = h^1(X, \mathcal{O})$.

14.3. Geometrical genus of projective variety. The notion of geometrical genus appears for the first time in the works of Riemann, connected with maximal number of linearly independent global differential forms on a Riemann surface. On the language of sheaves this can be expressed in the following way. Let Ω be the sheaf of regular differential forms on projective nonsingular variety X of dimension r. The canonical sheaf of the variety X is the sheaf $\omega_X = \wedge^r \Omega$, and the dimension of the space of its global sections — geometrical genus.

Definition. $p_g(X) = \dim H^0(X, \omega_X)$.

Example. Let $X = \mathbb{P}^1$ be the complex projective line and $X = U \cup V$ its standard affine covering. Then $\omega = \Omega$ and its restriction on $U = \mathbb{A}^1$ is a free $\mathcal{O}$-module of rank 1, generated by the differential of the local coordinate du. Now,

$C^0(X, \omega) = \Omega(U) \times \Omega(V) = K[u]du \times K[v]dv$,
$C^1(X, \omega) = \Omega(U \cap V) = K[u, 1/u]du$,
$d : u \mapsto u,\ v \mapsto \frac{1}{u},\ dv \mapsto -\frac{1}{u^2}du$,
$\operatorname{Ker} d = \left\{(f(u)du, g(v)dv) \mid f(u) + \frac{1}{7}u^2 g(\frac{1}{u}) = 0\right\} = 0$,
$\operatorname{Coker} d = C^1 / \operatorname{Im} d$, $\operatorname{Im} d = \{[f(u) + u^{-2}g(1/u)]du\} = \operatorname{Span}\{u^n du, n \neq -1\}$,
$H^0(X, \omega) = 0$, $H^1(X, \omega) = K \cdot 1/u \cdot du \cong K$, $h^0 = 0$, $h^1 = 1$.

Therefore, the geometrical genus equals $p_g(\mathbb{P}^1) = 0$. We have also calculated $H^1(\mathbb{P}^1, \omega)$.

14.4. Equality of topological, algebraic and geometrical genus for nonsingular projective curves. The most important types of geometrical theorems are probably the duality theorems, connecting complementary homological objects (homology and cohomology, homology of complementary dimension etc.). These are the key theorems of geometry and topology. Such is the Serre's duality theorem for projective nonsingular varieties, which expresses sheaf cohomology in terms of higher derived functors of the functor $\operatorname{Hom}(-, \omega)$ of complementary dimension. Due to our space restrictions, we shall only state the theorem and the corollary, in which we are now interested.

Theorem. *$H^{r-i}(X, \mathcal{F})^* \cong \operatorname{Ext}^i(\mathcal{F}, \omega)$ for all $0 \leq i \leq r$ ($r = \dim X$).*

Corollary. Particularly, for $i = 0$ and $\mathcal{F} = \mathcal{O}$ (structure sheaf of regular functions) one obtains $H^0(X, \omega) = \operatorname{Hom}(\mathcal{O}, \omega) \cong H^r(X, \mathcal{O})^*$. Therefore, the geometrical genus equals $p_g(X) = h^0(X, \omega) = h^r(X, \mathcal{O})$. For curves, $r = 1$ and this leads to equality $p_g(X) = p_a(X)$. This equality is valid only for curves. For surfaces a new component appears, so-called *irregularity*. Its existence was known already in the Italian geometrical school. In this case $r = 2$ and

$$p_a(X) = (-1)^2[\chi(\mathcal{O}) - 1] = h^0(X, \mathcal{O}) - h^1(X, \mathcal{O}) + h^2(X, \mathcal{O}) - 1$$
$$= h^2(X, \mathcal{O}) - h^1(X, \mathcal{O}) = p_g(X) - \operatorname{irr}(X)$$

The equality of arithmetical and topological genus for curves can be proved by complex-analytic means, naturally only when the main field is the field of complex

numbers, that is, when the topological genus is defined. Note that both arithmetical and geometrical genera can be defined for varieties over any algebraically closed field, not only the field of complex numbers.

15. Vector space, associated to a divisor

Let $\infty \in \mathbb{P}^1$ be the point at infinity of the projective line. The polynomial $f \in K[\mathbb{P}^1 \setminus \infty]$ of degree n has in ∞ a pole of order n and does not have other poles. Vice versa, a rational function $f \in K(\mathbb{P}^1)$ which has only one pole at ∞, is a polynomial. One has

$$\deg f \leq n \Leftrightarrow (f) + n \cdot \infty \geq 0$$

The vector space of all polynomials of degree at most n (as a subset of the field of rational functions) could be described by this condition.

More generally, let X be a projective variety and $D \in \operatorname{Div} X$.

Definition. $L(D) = \{f \in K(X) \mid (f) + D \geq 0\} \subset K(X)$. This is a vector space over the ground field K, of dimension $\dim_K L(D) = l(D)$, the space of all rational functions whose zeros' and poles' divisor is bounded below by the divisor $-D$.

Remarks. 1. If $\deg D \leq 0$, then $l(D) = 0$. Global rational functions on a projective variety X have degree 0.

2. Spaces of equivalent divisors are isomorphic, that is, if $D_1 \sim D_2$, then $L(D_1) \cong L(D_2)$ and $l(D_1) = l(D_2)$. Namely, if $D_1 - D_2 = (g)$ where $g \in K(X)$ is a rational function, then the multiplication with g produces isomorphism of corresponding vector spaces, since

$$f \in L(D_1) \Rightarrow (f) + D_1 \geq 0 \Rightarrow (fg) + D_2 = (f) + (g) + D_2 = (f) + D_1 \geq 0$$
$$\Rightarrow fg \in L(D_2)$$

Therefore, $L(D)$ and $l(D)$ are well defined for classes of equivalent divisors.

A priori, the space $L(D)$ has not to be finitely dimensional. However, this is the case. We shall prove it for projective curves.

Theorem. *If X is a nonsingular projective curve and D divisor on X, then the number $l(D)$ is finite.*

Proof. Let $D = P_1 + \cdots + P_n - Q_1 - \cdots - Q_m$ $(n \geq m)$ with possible repetitions. Since $L(D) \subset L(P_1 + \cdots + P_n)$, one could consider $m = 0$. There is a sequence of vector subspaces $L(0) \subset L(P_1) \subset \cdots \subset L(P_1 + \cdots + P_n)$, and one sees that it suffices to prove $\dim L(D)/L(D-P) < \infty$. Let m be the multiplicity of P in the divisor D and let u be the local parameter in P. Now $f \in L(D) \Rightarrow (f) + D \geq 0$ $\Rightarrow \operatorname{ord}_P f \geq -m \Rightarrow (u^m f)(P) \in \mathbb{C}$. One has a linear mapping $L(D) \to \mathbb{C}$, $f \mapsto (u^m f)(P)$ whose kernel equals $\{f \in L(D) \mid (u^m f)(P) = 0\} = L(D - P)$. It follows that $\dim L(D)/L(D - P) \leq 1$.

The proof even provides an upper bound of the dimension $l(D) \leq \deg D + 1$. Attempting to calculate this dimension, Riemann obtained a lower bound, which was later named after him.

Theorem. (Riemann's inequality) *If g is the genus of the curve, then $l(D) \geq \deg D + 1 - g$.*

Riemann's student Roch made this inequality a precise equality, by calculating the additional term. In this way he arrived to very important theorem, named later after Riemann and Roch.

Theorem. (The Riemann–Roch theorem for curves) $l(D) - l(K - D) = \deg D + 1 - g$ *where K is the so called canonical divisor of the curve X.*

This theorem will be stated and proved later in a different context, using sheaves.

16. Linear systems

Vector space of rational functions associated to a given divisor is a very important object. In what follows, we will describe its connection to classical notion of linear system.

It is known that through each five points of the projective plane in the general position passes exactly one curve of second order. Less known is perhaps such fact: if the curve of third order passes through eight of nine intersection points built by three pairs of lines in the plane, then it passes also through the ninth point. These and similar geometrical theorems were very important in the classical geometry of the last century. They were often proved using linear systems. The simplest linear system is mentioned even today in courses of analytical geometry. This is the bundle of lines in the plane - a set of all lines in the plane passing through a given point. The condition of passing through point can be written as a linear condition on (general) coefficients of line's equation. When, instead of a line, one takes an arbitrary plane algebraic curve of a given order, besides the condition of passing through a point (which is a linear condition on coefficients of curve's equation), one prescribes also the highest multiplicity of this point on the curve (surprisingly, this is also a linear condition on the coefficients!) and finally if, instead of one point, one takes a finite set of points with prescribed multiplicities (that is, an effective divisor), then one obtains a linear system of equations on curve's coefficients, or linear system for short. This notion can be defined more precisely in a different way.

Let X be a projective nonsingular variety, $D \in \mathrm{Div}(X)$ a divisor on X and $L(D)$ the corresponding associated vector space.

Definition. *Complete linear system* on X, defined by the divisor D is a set of divisors $|D| = \{D' \in \mathrm{Div}^+ X \mid D' \sim D\} = \{(f) + D \mid f \in L(D)\}$.

Note that $(f) + D = (g) + D \Leftrightarrow (f) = (g) \Leftrightarrow f = \alpha g$, $\alpha \in K^*$ and therefore $|D| = \mathbb{P}(L(D)) = \mathrm{Gr}(L(D), 1)$ is a projective space of dimension $\dim |D| = l(D) - 1$, the projectivization of the vector space $L(D)$.

Definition. *Linear system* on X is a projective subspace of some complete linear system $|D|$.

Suppose that $L \subset |D|$ is a given linear system of dimension m. Since it is a projective subspace, it allows a coordinatization $L \cong \mathbb{P}^m$. Instead of identifying divisors of L with points of projective space, let us use the projective duality principle and identify them with linear forms on that space. In such way, one obtains coordinate isomorphism $\varphi : L \to (\mathbb{P}^m)^*$. Let $x_i \in (\mathbb{P}^m)^*$ be coordinate functions on $\mathbb{P}^m$ and $f_i = \varphi^{-1}(x_i) \in L(D)$ corresponding rational functions $(i = 0, \dots, m)$. Then a rational mapping $\Phi : X \to \mathbb{P}^m$, $\Phi(x) = (f_0(x), \dots, f_m(x))$ is defined. Show that conversely, any rational mapping of X in a projective space defines a linear system with chosen coordinatization. Let $\Phi : X \to \mathbb{P}^m$ be rational mapping and $- \circ \Phi : K(\mathbb{P}^m) \to K(X)$ the corresponding homomorphism of fields of rational functions. If $l \in (\mathbb{P}^m)^*$ is a linear form on $\mathbb{P}^m$ and $H \subset \mathbb{P}^m$ a hyperplane it defines, then $\Phi^{-1}(H) \subset X$ is the zeros' divisor of the regular function $l \circ \Phi \in K[X]$. Set of all such divisors when $l \in (\mathbb{P}^m)^*$ is a linear system L with coordinatization $(\mathbb{P}^m)^* \to L$, $H \mapsto \Phi^{-1}(H)$.

Examples. Consider the case $X = \mathbb{P}^n$ more closely. The class divisor group here is $\mathrm{Cl}(X) = \mathbb{Z}$, the given effective divisor $D \in \mathrm{Div}^+(X)$ is equivalent to a divisor (f) where f is a homogeneous polynomial of degree $d = \deg f = \deg D$. Vector space $L(D)$ is isomorphic to vector space V of all homogeneous polynomials of degree d and its dimension is $\binom{n+d}{d}$, and full linear system $|D| = L_d$ is its projectivization, of dimension $N = \binom{n+d}{d} - 1$. Linear system of dimension m is a projective subspace of that space, with basis consisting of $m+1$ homogeneous polynomials of degree d. If these are $f_0(x), \dots, f_m(x) \in V \subset K[x_0, \dots, x_n]$, the corresponding rational mapping is $\Phi : \mathbb{P}^n \to \mathbb{P}^m$, $(x_0 : \dots : x_n) = x \mapsto (f_0(x) : \dots : f_m(x))$. Conversely, any rational mapping is defined by such polynomials, which for their part define linear system i.e., vector subspace of dimension $m+1$ in vector space V of all homogeneous polynomials of corresponding degree.

1) $n = 1$, $d = 2$. Complete linear system

$$L_2 = \{(f) \mid f = a_{20}x_0^2 + a_{11}x_0x_1 + a_{02}x_1^2\}$$

defines a rational mapping $\Phi : \mathbb{P}^1 \to \mathbb{P}^2$, $\Phi(x_0 : x_1) = (x_0^2 : x_0x_1 : x_1^2)$ and $\Phi(\mathbb{P}^1)$ is a conic.

2) $n = 2$, $d = 2$. Complete linear system L_2 has projective dimension 5 and defines familiar Veronese rational mapping $\Phi : \mathbb{P}^2 \to \mathbb{P}^5$, $\Phi(x_0 : x_1 : x_2) = (x_0^2 : x_0x_1 : x_0x_2 : x_1^2 : x_1x_2 : x_2^2)$ and $\Phi(\mathbb{P}^2) = \mathbb{P}^1 \times \mathbb{P}^1$.

3) Rational mapping $T : (x_0 : x_1 : x_2) \mapsto (\frac{1}{x_0} : \frac{1}{x_1} : \frac{1}{x_2}) = (x_1x_2 : x_2x_0 : x_0x_1)$ is known as Cremona transformation of projective plane $T : \mathbb{P}^2 \to \mathbb{P}^2$. What is the corresponding linear system? One has $L = \{(f) \mid f \in V'\}$ where $V' = \{a_0x_1x_2 + a_1x_2x_0 + a_2x_0x_1\} \subset V$ is a 3-dimensional subspace of 6-dimensional vector space of all homogeneous polynomials of degree 2 in 3 indeterminates. Each equation in V is the equation of a quadric passing through three points $P = (1:0:0)$, $Q = (0:1:0)$, $R = (0:0:1)$. Conversely, any quadric passing through

these three points should have equation of that form. Therefore, L is the linear system of all quadrics passing through points P, Q, R. Its projective dimension is 2 i.e., it is a two-parameter family of quadrics passing through three given points. Such points are called basic points of a linear system. What is their connection to starting rational mapping? The points in which the mapping Φ is not regular are the solutions of the system $x_1x_2 = x_2x_0 = x_0x_1 = 0$ and these are exactly the three basic points. This is a general fact, not simply a coincidence.

17. Sheaf, associated to a divisor

Let X be a nonsingular projective variety and D a divisor on X. If $\mathcal{O} \subset \mathcal{K}$ are sheaves of regular and rational functions on X, then the vector space $L(D)$ associated to divisor D appears on the level of global sections $L(D) \subset \mathcal{K}(X)$, and for $D = 0$, $L(0) = \mathcal{O}(X) = K$ (the only global regular functions on a projective variety are constants). We want to define a sheaf, whose sections over open U would play a role of the vector space $L(D \cap U)$. The given divisor D on X is locally principal, which means that any point has a neighborhood U such that $C_i \cap U = (f_i)$ or $D \cap U = \sum n_i(f_i) = (g)$, where $f_i \in K[U]$ are regular on U and $g = \prod f_i^{n_i}$. The condition $(f) + D \geq 0$ for $f \in L(D)$ locally on U is $(f) + \sum n_i(f_i) = (f) + (g) = (fg) \geq 0$ i.e., on each component $C_i \cap U$ of divisor D one has $\operatorname{ord} f \geq -n_i$, or $f \cdot g \in K[U] = \mathcal{O}(U)$ or equivalently $f \in 1/g \cdot \mathcal{O}(U)$. One sees that the role of the space $L(D \cap U)$ is played by the submodule of the field of rational functions in which the local equation g of the divisor D becomes invertible: $\mathcal{O}(U) \subset 1/g \cdot \mathcal{O}(U) \subset \mathcal{K}(U) = \mathcal{K}(X)$. This enables us to define the space associated to a divisor D in more general setting of Cartier divisors.

Definition. If $D \in \operatorname{CaDiv} X$ is a Cartier divisor on a variety X, $D = \{(U_i, f_i)\}$, the sheaf associated to D is the sheaf of submodules $\mathcal{O}(D) \subset \mathcal{K}$ of the sheaf of rational functions, generated by $1/f_i$ on U_i.

Obviously, $L(D) = H^0(X, \mathcal{O}(D))$ is the space of global sections of this sheaf, and $l(D) = \dim H^0(X, \mathcal{O}(D)) = h^0(\mathcal{O}(D))$ its dimension. Higher cohomology groups of the sheaf $\mathcal{O}(D)$ provide new integer invariants, and their alternating sum - Euler characteristic of the sheaf $\Im$: $\chi(\Im) = h^0(\Im) - h^1(\Im) + \cdots + (-1)^n h^n(\Im)$ where $h^i(\Im) = \dim H^i(X, \Im)$ and $n = \dim X$. The Riemann–Roch theorem could now be formulated in the following way. We will also give the sketch of its proof [31, p. 376]. Although it is not possible to explain all technical details in a short review, this proof illustrates the power of the technique of sheaves and their cohomology in modern geometry.

Theorem. (Riemann–Roch theorem for curves). *If X is a nonsingular projective curve, $\mathcal{O}$ its structure sheaf and D a divisor on X, then*

$$\chi(\mathcal{O}(D)) = \deg D + \chi(\mathcal{O})$$

Proof. Induction on degree of divisor. 1) If $D = 0$, then $\mathcal{O}(D) = \mathcal{O}$ and the statement is obvious.

2) Let the formula hold for divisor D and let $P \in X$. Consider P as a subvariety in X. Its structure sheaf is the "skyscraper"-sheaf $K = \mathcal{K}_P$ concentrated in the point P and zero outside it. Its sheaf of ideals is the sheaf $\mathcal{O}(-P)$. One has the short exact sequence of sheaves

$$0 \to \mathcal{O}(-P) \to \mathcal{O} \to \mathcal{K}_P \to 0$$

which, after tensoring with locally free sheaf $\mathcal{O}(D+P)$ of rank 1, gives the exact sequence

$$0 \to \mathcal{O}(-P) \otimes \mathcal{O}(D+P) \to \mathcal{O} \otimes \mathcal{O}(D+P) \to \mathcal{K}_P \otimes \mathcal{O}(D+P) \to 0$$

or

$$0 \to \mathcal{O}(D) \to \mathcal{O}(D+P) \to \mathcal{K}_P \to 0$$

Since the Euler characteristic is additive on exact sequences, and $\chi(\mathcal{K}_P) = 1$, one obtains $\chi(\mathcal{O}(D+P)) = \chi(\mathcal{O}(D)) + 1$ which proves the inductive step.

How to deduce the previous statement of the Riemann–Roch theorem from this one? Since it is a curve case, the Euler characteristic contains only two terms

$$\chi(\mathcal{O}) = h^0(\mathcal{O}) - h^1(\mathcal{O}) = \dim H^0(X, \mathcal{O}) - \dim H^1(X, \mathcal{O}) = 1 - p_a(X) = 1 - g$$
$$\chi(\mathcal{O}(D)) = h^0(\mathcal{O}(D)) - h^1(\mathcal{O}(D)) = l(D) - \dim H^1(\mathcal{O}(D))$$

The last term, introduced by Roch, could be interpreted in the following way. From Serre's duality theorem, one has

$$\begin{aligned} H^1(X, \mathcal{O}(D)) &\cong \mathrm{Hom}(\mathcal{O}(D), \omega) \cong \mathrm{Hom}(\mathcal{O}, \omega \otimes \mathcal{O}(D)^*) \\ &= H^0(X, \omega \otimes \mathcal{O}(D)^*) = H^0(X, \mathcal{O}(K - D)) \end{aligned}$$

where K is the canonical divisor, which corresponds to the canonical sheaf of differential forms ω. Now $h^1(\mathcal{O}(D)) = h^0(\mathcal{O}(K-D)) = l(K-D)$ and the Riemann–Roch formula for curves takes its previous form:

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

18. Applications of Riemann–Roch theorem for curves

From the Riemann–Roch theorem on nonsingular projective curves one could directly derive important corollaries on degree of canonical divisor, curves of genus 0 and 1, and other.

Application 1. Put $D = K$, then $l(K) - l(0) = \deg K - g + 1$. Since, according to definition of canonical divisor, $l(K) = g$, and since $l(0) = 1$ one obtains that the degree of the canonical divisor is $\deg K = 2g - 2$.

Application 2. If divisor D has a sufficiently high degree, or more precisely if $\deg D > 2g - 2 = \deg K$, then $\deg(K - D) < 0$ and $l(K - D) = 0$. Therefore, $l(D) = \deg D + 1 - g$.

Application 3. Let X be a projective curve of genus 0 and $D = P \in X$ one point. Then

$$l(D) = \deg D + 1 - g + l(K - D) = 2 + l(K - D) \geq 2$$

This means that the vector space $L(D)$ contains a nonconstant rational function f with a pole of multiplicity 1 in the point P, that is, $(f)_\infty = P$. This function defines a rational mapping $f : X \to \mathbb{P}^1$ of degree 1. From this one could show that f is an isomorphism, that is, all curves of genus 0 are rational.

Application 4. Let X be a nonsingular projective curve of genus 1, $P \in X$ its point and $D = nP$. Then $\deg K = 0$ and for all $n > 0$ one has $\deg(K - nP) < 0$ and $h^0(K - nP) = 0$. Therefore $h^0(nP) = \deg nP - g + 1 = n$. There is a sequence of vector spaces $H^0(\mathcal{O}(P)) \subset H^0(\mathcal{O}(2P)) \subset \ldots \subset H^0(\mathcal{O}(nP)) \subset \ldots$ of strictly increasing dimension $1 < 2 < 3 < \cdots < n < \cdots$ Rational functions in $H^0(\mathcal{O}(nP))$ do have a pole in P of multiplicity at most n. Particularly, for $n = 2$ one has $\dim H^0(\mathcal{O}(2P)) = 2$ and this vector space has a basis $\{1, x\}$. Complete it to the basis $\{1, x, y\}$ of $H^0(\mathcal{O}(3P))$. The seven functions 1, x, y, x^2, xy, x^3, y^2 must be linearly dependent in the six-dimensional space $H^0(\mathcal{O}(6P))$. Each of them has only one pole in P, of multiplicity at most 0, 2, 3, 4, 5, 6, 6 respectively. One concludes that the coefficients in y^2 and x^3 should be different from zero. By homothety with respect to x and y one could transform these coefficients to get 1, so the linear combination has the form $y^2 + a_1xy + a_2y = x^3 + b_1x^2 + b_2x + b_3$. At last, by change $y + \frac{1}{2}(a_1x + a_2) \mapsto y$ (adding to a complete square) it could be transformed to the canonical form

$$y^2 = x^3 + c_1x^2 + c_2x + c_3$$

We obtained the canonical equation of nonsingular projective curve of genus 1. As we already know, X is nonsingular $\Leftrightarrow$ the right-hand-side polynomial has only simple roots. We conclude that every nonsingular projective algebraic curve of genus 1 is a plane curve defined by such equation in $\mathbb{P}^2$.

References

1 Atiyah M.F., Macdonald I.G.: *Introduction to commutative algebra*, Addison-Wesley, Reading, Massachusets, 1969 (Russian: Атья М., Макдональд И., *Введение в коммутативную алгебру*, Мир, Москва, 1972)

2 Арнольд В.И., Варченко А.Н., Гусейн-Заде С.М.: *Особенности дифференцируемых отображений*, Наука, Москва, 1982

3 Боревич З.И., Шафаревич И.Р.: *Теория чисел*, Наука, Москва, 1985

4 Brieskorn E., Knörrer H.: *Plane Algebraic Curves*, Birkhäuser, Basel–Boston–Stuttgart, 1986 (German: Brieskorn E., Knörrer H., *Ebene algebraische Kurven*, Birkhäuser, Basel–Boston–Stuttgart, 1981)

5 Griffiths P.A.: *Introduction to Algebraic Curves*, Translations of Mathematical Monographs 76, American Mathematical Society, Providence, 1989

6 Гриффитс Ф., Харрис Дж.: *Принципы алгебраической геометрии. В 2-х томах*, Мир, Москва, 1982 (English: Griffiths P., Harris J., *Principles of algebraic geometry*, Wiley-Interscience, New York–Chichester–Brisbane–Toronto, 1978)

7 Godement R.: *Topologie algébrique et theorie des faisceaux*, Hermann, Paris, 1958 (Russian: Годеман Р., *Алгебраическая топология и теория пучков*, Мир, Москва, 1972)

8 Данилов В.И.: *Алгебраические многообразия и схемы*, Современные проблемы математики — фундаментальные направления, том 23 (Алгебраическая геометрия 1), ВИНИТИ, Москва, 1988, 172–302

9 Данилов В.И.: *Когомологии алгебраических многообразий*, Современные проблемы математики - фундаментальные направления, том 35 (Алгебраическая геометрия 2), ВИНИТИ, Москва, 1989, 5–130

10 Исковских В.А., Шафаревич И.Р.: *Алгебраические поверхности*, Современные проблемы математики — фундаментальные направления, том 35 (Алгебраическая геометрия 2), ВИНИТИ, Москва, 1989, 131–263

11 Jordan C.: *Traite des substitutions des équations algébriques*, Gauthier-Villars, Paris, 1870

12 Касселс Дж., Фрелих А.: *Алгебраическая теория чисел*, Мир, Москва, 1969 (English: Cassels J.W.S., Fröhlich A. (ed.), *Algebraic number theory*, Thompson, Washington DC, 1967)

13 Kendig K.: *Elementary algebraic geometry*. GTM, Springer-Verlag, New York, Heidelberg, Berlin, 1977

14 Kunz E.: *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, Basel–Boston–Stuttgart, 1985.

15 Lang S.: *Elliptic Functions*, Addison-Wesley, Reading, Massachusets 1973 (Russian: С. Ланг, *Эллиптические функции*, Наука, Москва, 1984)

16 Legendre A.-M.: *Traite des fonctions elliptiques et des integrales euleriennes*, 1827–1832

17 Lipkovski A.: *Newton polyhedra and irreducibility*, Math. Z. 199, 119-127, 1988

18 Lipkovski A.: *On Serret curves*, Preprint, Faculty of Mathematics, Belgrade, 1995

19 Мамфорд Д.: *Алгебраическая геометрия. 1. Комплексные проективные многообразия*, Мир, Москва, 1979 (English: Mumford D., *Algebraic Geometry. I Complex Projective Varieties*, Grundlehren Bd. 221, Springer-Verlag, Berlin, Heidelberg, New York, 1976)

20 Манин Ю.И.: *Лекции по алгебраической геометрии 1966–1968*. Мех-мат МГУ и Московское математическое общество, Москва, 1968

21 Манин Ю.И.: *Кубические формы. Алгебра, геометрия, арифметика*, Наука, Москва, 1972

22 Newton I.: *The correspondence of Isaak Newton. Vol. 2 (1676–1687)*, Cambridge Univ. Press, Cambridge, 1960, (Newton to Oldenburg, 1676, pp. 20–42, pp. 110–163)

23 Прасолов В.В., Соловьев Ю.П.: *Эллиптические функции. Специальный курс*, Математический колледж НМУ, Москва, 1993

24 Прасолов В.В., Соловьев Ю.П.: *Алгебраические уравнения и тета-функции. Специальный курс*, Математический колледж НМУ, Москва, 1994

25 Рид М.: *Алгебраическая геометрия для всех*, Мир, Москва, 1991 (English: Reid M., *Undergraduate Algebraic Geometry*, London Mathematical Society Student Texts 12, Cambridge Univ. Press, Cambridge, 1988)

26 Савелов А.А.: *Плоские кривые*, Гос. изд. физ.-мат. лит., Москва, 1960

27 Serre J.-P.: *Geometrie algebrique et geometrie analytique*, Ann. Inst. Fourier 6(1956), 1–42

28 Serret J.-A.: *Lehrbuch der Differential- und Integralrechnung. Band 2*, Teubner, Leipzig, 1899, 228–232 (French: Serret J.-A.: , Paris,)

29 Stark H.M.: *There is no tenth complex quadratic field with class-number one.* Proc. Nat. Acad. Sci. USA 57(1967), 216–221

30 Фихтенгольц Г.М.: *Курс дифференциального и интегрального ищисления, том II*, 7 изд., Наука, Москва, 1969

31 Хартшорн Р.: *Алгебраическая геометрия*, Мир, Москва, 1981 (English: Hartshorne R., *Algebraic Geometry*, Graduate Texts in Mathematics 52, Springer-Verlag, New York, Heidelberg, Berlin, 1977)

32 Herzog J.: *Generators and relations of abelian semigroups and semigroup rings*, Manuscripta Math. 3(1970), 153–193

33 Шафаревич И.Р.: *Основы алгебраической геометрии*, Москва, Наука, 1988 (2 изд.) (1st ed., English: Shafarevich I.R., *Basic algebraic geometry* (Grundlehren Bd. 213), Springer-Verlag, Berlin, Heidelberg, New York, 1974)

34 Шокуров В.В.: *Римановы поверхности и алгебраические кривые (с введением И.Р. Шафаревича)*, Современные проблемы математики — фундаментальные направления, том 23 (Алгебраическая геометрия 1), ВИНИТИ, Москва, 1988, 5–171

35 van der Waerden: *A history of algebra (from al-Khwarizmi to Emmy Noether)*, Springer-Verlag, 1985

36 Walker R.: *Algebraic curves*, Princeton Univ. Press, Princeton, 1950 (Russian: Уокер Р., *Алгебраические кривые*, ИЛ, Москва, 1952)