MAT4210—Algebraic geometry I: Notes 4

Projective varieties

21st February 2018

Hot themes in Notes 4: Projective spaces—homogeneous coordinates closed projective sets—homogenous ideals and closed projective sets—projective Nullstellensatz—distinguished open sets—Zariski topology and regular functions—projective varities—global regular functions on projective varities—projective coordinate shifts—linear subvarieties—conics and the Veronese surface.

Super-Preliminary version 0.2 as of 21st February 2018 at 9:05pm—Well, still not really a version at all, but better. Improvements will follow!

Geir Ellingsrud — ellingsr@math.uio.no

The projective varities

Projective geometry arose in the wake of the discovery of the perspective by italian renaissance painters like for instance *Filippo Brunellesch* . In a perspective on considers bundles of rays of light emanating from or meeting at a point (the observers eye) or meeting at an apparent point at infinity, the so-called vanishing point, when rays are parallel. Figures are perceived the same if one is the projection of the other.

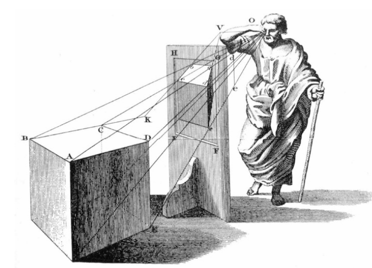


Figure 1: The discovery of perspective i art.

In the beginning projective geometry was purely a synthetic geometry (no coordinates, no function, merely points and lines). The properties of different figures that where studied were the properties invariant under projection from a point. Subsequently, an analytic theory developed and eventually became the basis for the projective geometry as we know it in algebraic geometry today.

The synthetic theory still persists, especially since some finite projective planes are important combinatorial structures[1]. The simplest being the *Fano plane* with seven points and seven lines!

[1] The axiomatics of the synthetic projective plane geometry is exceedingly simple. There are to sets of objects, points and lines, and there are two axioms: Through any pair of points there goes a unique line, and any two lines intersect in a unique point.

The projective spaces and the projective varieties are in some sense the algebro-geometric counterparts to compact spaces, and they share many the nice properties.

Non-compact spaces are notoriously difficult to handle; if you discard a bunch of points in an arbitrary manner from a compact space (for instance, a sphere) it is not much you can say about the result unless you know the way the discarded points were chosen, and moreover, functions can tend to infinity near the missing points. Compact spaces and projective varieties are in some sense complete, they do not suffer from the deficiencies of these "punctured" spaces—hence their importance and popularity!

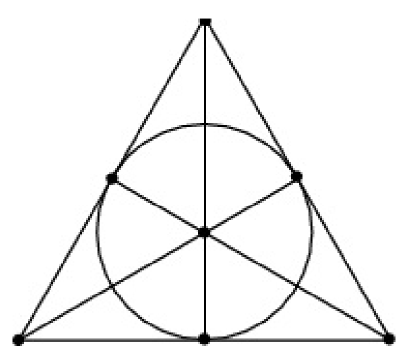


Figure 2: The Fano plane; the projective plane over the field with two elements $\mathbb{P}^2(\mathbb{F}_2)$.

The projective spaces $\mathbb{P}^n$

ProSpace

The projective spaces $\mathbb{P}^n$

Let n be a non-negative integer. The underlying set of *the projective space* $\mathbb{P}^n$ over k is the set of lines through the origin in $\mathbb{A}^{n+1}$—or in other words, the set of one dimensional vector subspaces. Since any point, apart from the origin, lies on a unique line in $\mathbb{A}^{n+1}$ passing by 0, there is map

$$\pi\colon \mathbb{A}^{n+1} \setminus \{0\} \to \mathbb{P}^n,$$

sending a point to the line on which it lies. It will be convenient to denote by $[x]$ the line joining x to the origin; that is, $[x] = \pi(x)$.

One may as well consider $\mathbb{P}^n$ as the set of equivalence classes in $\mathbb{A}^{n+1} \setminus \{0\}$ under the equivalence relation for which two points x and y are equivalent when $y = tx$ for some $t \in k^*$.

EXAMPLE 4.1 There is merely one line through the origin in $\mathbb{A}^1$, so $\mathbb{P}^0$ is just one point. ☆

We begin with getting more acquainted with the projective spaces, and subsequently we shall put a variety structure on $\mathbb{P}^n$—that is, we shall endow it with a topology (which naturally will be called the Zariski topology) and tell what functions on $\mathbb{P}^n$ are regular; that is, define the sheaf $\mathcal{O}_{\mathbb{P}^n}$ of regular functions. Finally, we introduce the larger class of *projective varieties*. They will be the closed irreducible subsets of $\mathbb{P}^n$ with topology induced from the Zariski topology on $\mathbb{P}^n$ and equipped with a sheaf of rings of regular functions.

COORDINATES ARE OFTEN USEFUL, but there are no *global* coordinates on $\mathbb{P}^n$. However, there is a very good substitute. if $[x] \in \mathbb{P}^n$ corresponds to the line through the point $x = (x_0, \ldots, x_n)$, we say that $(x_0; \ldots; x_n)$ are *homogeneous coordinates* of the point $[x]$—notice the use of semi-colons to distinguish them from the usual coordinates in $\mathbb{A}^{n+1}$. The homogeneous coordinates of x depend on the choice of a point in the line $[x]$ and are not unique; they are only defined up to a scalar multiple, so that $(x_0; \ldots; x_n) = (tx_0; \ldots; tx_n)$ for all elements $t \in k^*$. Be aware that $(0; \ldots; 0)$ is forbidden; it does not corresponds to any line through the origin and is not the coordinates of a point in $\mathbb{P}^n$.

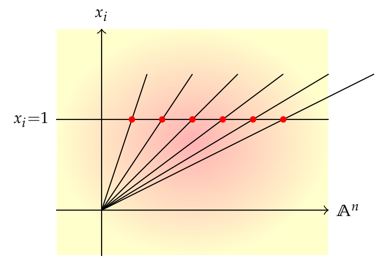
Homogeneous coordinates

VISUALIZING projective spaces are challenging, but the following is one way of thinking about them. This description of $\mathbb{P}^n$ will also be important in the subsequent theoretical development, and it is a invaluable tool when working with projective spaces.

Fix one of the coordinates, say x_i, and let $D_+(x_i)$ denote the set of lines $[x] = (x_0; \ldots; x_n)$ for which $x_i \neq 0$. These sets are called *basic open subsets* of $\mathbb{P}^n$. Every line $[x]$ with $x_i \neq 0$ intersects the subva-

The basic open subsets $D_+(x_i)$

riety A_i of $\mathbb{A}^{n+1}$ where $x_i = 1$ in precisely one point, namely the point $(x_0x_i^{-1}, \ldots, x_nx_i^{-1})$. Thus there is a natural one-to-one correspondence between the subsets $D_+(x_i)$ of $\mathbb{P}^n$ and A_i of $\mathbb{A}^{n+1}$. Now, obviously the subvariety A_i is isomorphic to affine n-space $\mathbb{A}^n$ (the projection that forgets the i-th coordinate is an isomorphism); hence $D_+(x_i)$ is in a natural bijective correspondence (later on we shall see it is an isomorphism) with $\mathbb{A}^n$.



To avoid unnecessary confusion, let us denote the coordinates on A_i by t_j where j runs from 0 to n but stays different from i. Then the map $D_+(x_i)$ to A_i is given be the relations $t_j = x_jx_i^{-1}$

The complement of the basic open suset $D_+(x_i)$ consists of the lines lying in the subvariety of $\mathbb{A}^{n+1}$ where $x_i = 0$; that is, $Z(x_i)$. This is an affine n-space with coordinates[2] $x_0, \ldots, \hat{x}_i, \ldots, x_n$ and so the complement $\mathbb{P}^n \setminus D_+(x_i)$ is equal to the projective space $\mathbb{P}^{n-1}$ of lines in that affine space. It is called the *hyperplane at infinity*.

[2] A hat indicates that a variable is missing.

Hyperplane at infinity

Be aware that the "hyperplane at infinity" is a *relative* notion; it depends on the choice of the coordinate x_i. In fact, given any linear functional $\lambda(x)$ in the x_i's, one may chose coordinates so that the hyperplane $\lambda(x) = 0$ is the hyperplane at infinity.

EXAMPLE 4.2 When $n = 1$ we have the *projective line* $\mathbb{P}^1$. It consists of a "big" subset isomorphic to $\mathbb{A}^1$ to which one has added a point at infinity. Every point can be made the point at infinity by an appropriate coordinate shift.

The projective line over the complex numbers, endowed with the strong topology, is the good old *Riemann sphere* we became acquainted with during courses in complex function theory. Indeed, let $(x_0; x_1)$ be the homogeneous coordinates on $\mathbb{P}^1$. In the set $D_+(x_0)$—which is isomorphic to $\mathbb{A}^1$, that is to $\mathbb{C}$—one uses $z = x_1/x_0$ as coordinate, where as in $\mathbb{D}_+(x_1)$ the coordinate is $z^{-1} = x_0/x_1$; and this exactly the patching used to construct the Riemann sphere.

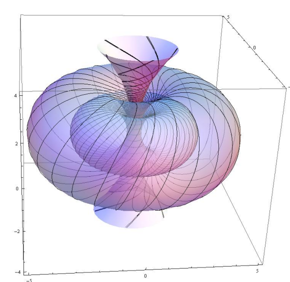
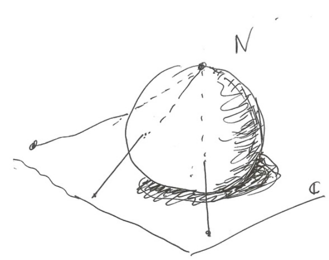


Figure 3: Te Hopf fibration

The projection map $\pi\colon \mathbb{C}^2 \setminus \{0\} \to \mathbb{C}\mathbb{P}^1$ is interesting. Restricting it to unit sphere S^3 in $\mathbb{C}^2$ one obtains a map $S^3 \to S^2$ which is very famous and goes under the name of *the Hopf fibration*. It is easy to see that its fibres are circles, so that π is a fibration of the three sphere S^3 over S^2 in circles.

The projective line over the reals $\mathbb{R}$ is just a circle, but notice there is merely one point at infinity. One uses lines and not rays through the origin and does not distinguish ∞ and $-\infty$. ☆



EXAMPLE 4.3 The variety $\mathbb{P}^2$ is called *the projective plane*. It has a "big" $\mathbb{A}^2 = D_+(x_i)$ with a projective line at infinity "wrapped" around it.

The projective plane contains many subsets that are in a natural one-to-one correspondence with the projective line $\mathbb{P}^1$. The set of one dimensional subspaces contained in a fixed two dimensional vector subspace of $\mathbb{A}^3$, is such a $\mathbb{P}^1$, and of course any two dimensional subspace will do. These subsets are called *lines* in $\mathbb{P}^2$.

By linear algebra two different two dimensional vector subspaces of $\mathbb{A}^3$ intersect along a line through the origin, hence the fundamental observation that the two corresponding lines in $\mathbb{P}^2$ intersect in a *unique* point. Two lines do not meet in the "finite part"; that is, in the affine 2-space $\mathbb{A}^2$ where $x_i \neq 0$, if and only they have a common intersection with the line at infinity; one says that the two lines meet at infinity. And naturally, when they do not meet in the finite part, they are experienced to be parallel there; hence "parallel" lines meet at a common point at infinity.

The projective plane over the reals, is a subtle creature. After having picked one of the coordinates x_i, we find a big cell of shape $D_+(x_i)$ in $\mathbb{P}^2$, which is bijective to $\mathbb{R}^2$, enclosed by the line at infinity—a circle bordering the affine world like a Midgard Serpent. Again, be aware that in constructing $\mathbb{P}^2$ one uses lines through the origin and not rays emanating from the origin. This causes $\mathbb{P}^2$ to be non-orientable—tubular neighbourhoods of the lines are in fact Möbius bands.

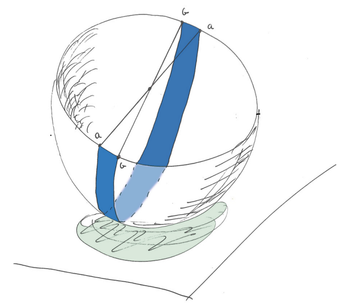


Figure 4: A Möbius band in the real projective plane.

☆

The Zariski topology and projective varieties

One may use the projection map $\pi\colon \mathbb{A}^{n+1} \setminus \{0\} \to \mathbb{P}^n$ to equip $\mathbb{P}^n$ with a topology, and we declare a subset in $X \subseteq \mathbb{P}^n$ to be closed if and only if the inverse image $\pi^{-1}X$ is closed in $\mathbb{A}^{n+1} \setminus \{0\}$. Since the operation of forming inverse images behaves well with respect to intersections and unions (*i.e.,* commutes with them), these sets are easily seen to fulfill the axioms for the closed sets of a topology. Naturally, this topology is called the *Zariski topology* on $\mathbb{P}^n$.

Zariski topology

POLYNOMIALS on $\mathbb{A}^{n+1}$ do not descend to functions on $\mathbb{P}^n$ unless they are constant, since a non-constant polynomial is not constant on lines through the origin. However, if F is a *homogeneous* polynomial it holds true that $F(tx) = t^d F(x)$ where d is the degree of F, so if F vanishes at a point x, it vanishes along the entire line joining x to the origin. Hence it is lawful to say that F is *zero* at a point $[x] \in \mathbb{P}^n$; and it is meaningful to talk about the zero locus in $\mathbb{P}^n$ of a set of homogeneous polynomials. A homogeneous ideal $\mathfrak{a}$ in $k[x_0, \ldots, x_n]$ is generated by homogeneous polynomials, and we can hence speak about the *zero locus* $Z_+(\mathfrak{a})$ in $\mathbb{P}^n$.

The zero locus of a homogeneous ideal

In the same spirit as one defined the basic open sets $D_+(x_i)$, one defines the *distinguish open subset* $D_+(F) = \{ [x] \in \mathbb{P}^n \mid F(x) \neq 0 \}$ for any homogeneous polynomial F. All these sets are open in $\mathbb{P}^n$, their complements being the closed sets $Z_+(F)$.

Distinguished open subsets

PROBLEM 4.1 Let $\mathfrak{a} \subseteq k[x_0, \ldots, x_n]$ be an ideal. Show that $\mathfrak{a}$ is homogeneous if and only if it satisfies either the following two equivalent properties:

a) A polynomial $f(x)$ belongs to $\mathfrak{a}$ precisely when $f(tx)$ lies there for all scalars $t \in k$.

b) The zero set $Z(\mathfrak{a})$ in $\mathbb{A}^{n+1}$ is a cone. ★

A HOMOGENEOUS IDEAL $\mathfrak{a}$ also has a zero set $Z(\mathfrak{a})$ in the affine space $\mathbb{A}^{n+1}$, and since homogeneous polynomials vanish along lines through $\{0\}$, it clearly holds that $\pi^{-1}Z_+(\mathfrak{a}) = Z(\mathfrak{a}) \cap \mathbb{A}^{n+1} \setminus \{0\}$. Thus the closed sets of the Zariski topology on $\mathbb{P}^n$ are the subsets of type $Z_+(\mathfrak{a})$ with $\mathfrak{a}$ being a homogeneous ideals in $k[x_0, \ldots, x_n]$. Such a subset X is called a *closed projective subset* and topology induces from the Zariski topology on $\mathbb{P}^n$ is called the Zariski topology on X. If additionally X is an *irreducible* space, it is said to be a *projective variety.*

Projective varieties

The *affine cone* $C(X)$ over a projective variety X is defined as the closed subset $C(X) = \pi^{-1}X \cup \{0\}$. It is a cone in the sense that i contains the line joining any one its points to the origin; or phrased differently, if $x \in C(X)$ then $tx \in C(X)$ for all scalars $t \in k$. The inverse image $\pi^{-1}X$ will now and then be called the *punctured cone* over X and denoted by $C_0(X)$; so that $C_0(X) = C(X) \cap (\mathbb{A}^{n+1} \setminus \{0\})$.

The affine cone over a projective variety

The punctured cone

In this story there is one ticklish point. The maximal ideal $\mathfrak{m}_+ = (x_0, \ldots, x_n)$ vanishes only at the origin in $\mathbb{A}^{n+1}$, and so it defines the *empty set* in $\mathbb{P}^n$; indeed, for no point in $\mathbb{P}^n$ do all the coordinates x_i vanish. Hence $\mathfrak{m}_+$ goes under the name of *the irrelevant ideal*.

The irrelevant ideal

PROBLEM 4.2 Show that if $\mathfrak{a}$ and $\mathfrak{b}$ are two homogeneous ideals, then $\mathfrak{a} \cdot \mathfrak{b}$ and $\mathfrak{a} + \mathfrak{b}$ are homogeneous, and it holds true that $Z_+(\mathfrak{a} \cdot \mathfrak{b}) = Z_+(\mathfrak{a}) \cup Z_+(\mathfrak{b})$ and $Z_+(\mathfrak{a} + \mathfrak{b}) = Z_+(\mathfrak{a}) \cap Z_+(\mathfrak{b})$. ★

SINCE π OBVIOUSLY is continuous, the Zariski topology makes the projective spaces irreducible. It also clear that the "big" affine subsets $D_+(x_i)$ where $x_i \neq 0$ are open subsets, their complements—the hyperplanes at infinity—being the closed sets $Z_+(x_i)$.

AiHomeoDPlus

Proposition 4.1 *The restriction $\pi|_{A_i}$ of π to the subset A_i where $x_i = 1$ is a homeomorphism.*

The proof of this needs the process of *homogenization* of a polynomial which, when the variable x_i is fixed, is a systematic way of

Homogenization of polynomials

producing a homogeneous polynomial f^h from a polynomial f. If d is the degree of f, one puts

$$f^h(x_0,\ldots,x_n) = x_i^d f(x_0x_i^{-1},\ldots,x_nx_i^{-1}). \tag{1}$$

HomProc

For example, if $f = x_1x_2^3 + x_3x_0 + x_0$, one finds that

$$f^h(x_0,x_1,x_2) = x_0^4\big(x_1x_0^{-1}(x_2x_0^{-1})^3 + x_3x_0^{-1} + 1\big) = x_1x_2^3 + x_3x_0^3 + x_0^4.$$

The net effect of the homogenization process is that all the monomial terms are filled up with the chosen variable so they become homogeneous. To verify that f^h in (1) is homogeneous of degree d, let t be any scalar. Each fraction $x_jx_i^{-1}$ is invariant when the variables are scaled, and the front factor x_i^d changes by the multiple t^d. The important relation $f|_{A_i} = f^h|_{A_i}$, which is easy to establish, just put $x_i = 1$, holds true as well.

Proof of Proposition 4.1: Now, we come back to the proof of the proposition. The restriction $\pi|_{A_i}$ is, as already observed, continuous, so our task is to show that the inverse is continuous, or what amount to same, that $\pi|_{A_i}$ is a closed map.

Since any closed subset of A_i is the intersection of sets of the form $Z = Z(f) \cap A_i$, and π being bijective takes intersections to intersections, it suffices to demonstrate that $\pi(Z(f) \cap A_i)$ is closed in $D_+(x_i)$ for any polynomial f on A_i. But this is precisely what the homogenization f^h is constructed for. Indeed, the subset $Z(f^h)$ of $\mathbb{A}^{n+1}$ is a closed cone satisfying $Z(f^h) \cap A_i = Z(f) \cap A_i$, and this means that $\pi(Z(f) \cap A_i) = Z_+(f^h) \cap D_+(x_i)$. ❑

Problem 4.3 Let $f(x_0,x_1,x_2,x_3) = x_0^3x_2 + x_3^2x_1 + 1$. Determine f^h with respect to each of the four variables. ★

Problem 4.4 In this exercise $n = 2$ and the coordinates are x_0 and x_1. Let $f(x_0) = (x_0 - a)(x_0 - b)$. Determine f^h and make a sketch of $Z(f) \cap \mathbb{A}^1$ and the cone $Z(f^h)$ ★

The sheaf of regular functions on projective varieties.

Although polynomials on $\mathbb{A}^{n+1}$ do not descend to $\mathbb{P}^n$, certain rational functions do. To describe these, assume that a and b are two polynomials both homogeneous of the same degree, say d. Although none of them defines a function on the projective space $\mathbb{P}^n$, their fraction will, at least at points where the denominator does not vanish. Indeed, letting x and tx be two points on the same line through the origin, we find

$$\frac{a(tx)}{b(tx)} = \frac{t^d a(x)}{t^d b(x)} = \frac{a(x)}{b(x)},$$

whenever $b(x) \neq 0$. The function $a(x)/b(x)$ thus takes the same value at any point on the line $[x]$, and this common value is the value of $a(x)/b(x)$ at $[x]$.

THIS OBSERVATION leads us to define the *sheaf of regular functions* on $\mathbb{P}^n$, or more generally to the notion of regular functions on any closed projective set $X \subseteq \mathbb{P}^n$, hence to the sheaf $\mathcal{O}_X$ of regular functions on X.

OK

The sheaf of regular functions on $\mathbb{P}^n$

A functions f on an open subset U of X is said to be *regular* at a point $p \in U$ if there exist an open neighbourhood $V \subseteq U$ of p in X and homogenous polynomials a and b of the same degree such that $b(x) \neq 0$ throughout V and such that the equality

Regular functions

$$f(x) = \frac{a(x)}{b(x)}$$

holds for $x \in V$. For any open U in X, we let $\mathcal{O}_X(U)$ be set of functions regular at all points in U, and we let the restriction maps be just the restrictions. Sums and products of regular functions are regular so $\mathcal{O}_X(U)$ is a k-algebra, and the restriction maps are k-algebra homomorphisms. Moreover, a regular function in $\mathcal{O}_X(U)$ is invertible if and only if it does not vanish in U.

Obviously $\mathcal{O}_X$ is a *presheaf* on X, and the first sheaf-axiom is trivially fulfilled (it always is, when the sections are set-theoretical functions with some extra properties). Neither the second sheaf-axiom is hard to establish: Continuous functions in $\mathcal{X}$, this is functions with values in $\mathbb{A}^1$, given on members on an open covering $\{U_i\}$ that coincide on intersections, patch together considered as continuous functions into $\mathbb{A}^1$, and since being regular is a local condition, the resulting function is regular (it restricts to regular functions on the members of the open covering $\{U_i\}$). Hence $\mathcal{O}_X$ is a *sheaf* on X.

PROBLEM 4.5 Show in detail that $\mathcal{O}_X(U)$ is a k-algebra. ★

PROBLEM 4.6 Given an open $U \subseteq X$ and a continuous fucntion $f\colon U \to \mathbb{A}^1$. Let $C_0(U)$ be punctured cone over U and let $\pi\colon C_0(U) \to U$ be the (restriction of the) projection. Show that f is regular if and only if the cmposition $f \circ \pi$ is regualr on $C_0(U)$. ★

PraktKrit

EXAMPLE 4.4 If the index i is fixed, the functions x_j/x_i are regular on the basic open subset $D_+(x_i)$ of $\mathbb{P}^n$ where x_i does not vanish. ☆

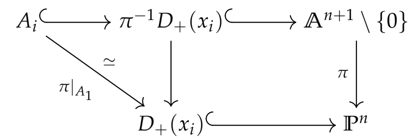
FracsAreRegFu

Assume now that $Y \subseteq X$ is a Zariski-closed subset and $U \subseteq X$ is open. The following lemma is almost tautological:

Lemma 4.1 *Restrictions of regular functions are regular: If f is a regular function in the open set $U \subseteq X$ and $Y \subseteq X$ is closed, the restriction $f|_{U\cap Y}$ is regular in $Y \cap U$. Any functions on $U \cap Y$ regular at a point $p \in Y$ extends to a regular function on some open neighbourhood V of p in X.*

Projective varieties are varieties

In the end we shall show that projective varieties are varities. There are to steps, and for the moment we contend ourself to see that they are *prevarieties*. We have equipped projective varieties with a topology and a sheaf of rings, so what is left, is to check they are locally affine. To this end, one shows that the basic open subsets $D_+(x_i)$ are isomorphic to affine n-space $\mathbb{A}^n$—more precisely the regular functions x_j/x_i will serve as affine coordinates. This resolves the matter for projective space itself, and for a closed subset $X \subseteq \mathbb{P}^n$ the sets $X \cap D_+(x_i)$ will do (closed subsets of affine space are affine).



Recall the subvariety A_i of $\mathbb{A}^{n+1}$ where the i-th coordinate x_i equals one. We already saw that $\pi|_{A_i}$ is a homeomorphism between A_i and $D_+(x_i)$, and it will turn out to be an isomorphism. There is a natural candidate for an inverse map α. If $x_i \neq 0$ we may send a point x with homogenous coordinates $(x_0; \ldots; x_n)$ to the point $(x_0 x_i^{-1}, \ldots, x_n x_i^{-1})$ which obviously has the i-th coordinate equal to one, and hence lies in A_i. One has

BaiscsAreAffine

Proposition 4.2 *The projection $\pi|_{A_i}$ is an isomorphism between A_i and $D_+(x_i)$. The inverse map is the map α above; that is, $\alpha(x_0, \ldots, x_n) = (x_0/x_i, \ldots, x_n/x_i)$.*

Notice, the last sentence says that the basic open $D_+(x_i)$ subset is an affine n-space on which the n functions $x_0/x_i, \ldots, x_n/x_i$ serve as coordinates.

PROOF: What is left, is to check is that the two maps π and α are morphisms.

That π is a morphism is almost trivial: Let f be regular at p and represent f in some open neighbourhood U of p as $f(x) = a(x)/b(x)$ with a and b homogeneous polys of the same degree and with b being non-zero through out U. One simply has $f \circ \pi|_{A_i} = ab^{-1}|_{A_i}$, which is regular on $A_i \cap \pi^{-1}U$ as b does not vanish along $\pi^{-1}U$.

To prove the other way around, let f be regular on an open set $U \subseteq A_i$ and represent f as $f = a/b$ with a and b being polynomials and b not vanishing in U. To obtain $f \circ \alpha$ one simply plugs in $x_j x_i^{-1}$ in the j-th slot (this automatically inserts a one in slot i) and one arrives at the expression

$$f \circ \alpha(x_0; \ldots; x_n) = a(x_0 x_i^{-1}, \ldots, x_n x_i^{-1})/b(x_0 x_i^{-1}, \ldots, x_n x_i^{-1}).$$

We already observed that the fractions $x_j x_i^{-1}$ are regular throughout $D_+(x_i)$, and as the regular functions form a ring with non-vanishing functions being invertible, it follows that $f \circ \alpha$ is regular in U. ❑

This was the warm up for $\mathbb{P}^n$, and the general case of a projective variety is not very much harder—in fact it follows immediately:

BasicOpnAff

Proposition 4.3 *Assume that $X \subseteq \mathbb{P}^n$ is a closed projective set. Then $V_i = D_+(x_i) \cap X$ equipped with the sheaf $\mathcal{O}_X|_{V_i}$ is affine variety.*

PROOF: Closed subsets of affine varities are affine varities. ❑

We have almost establishes the following all important theorem:

Theorem 4.1 *Irreducible, projective closed sets are varieties when endowed with the Zariski topology and the sheaf of regular functions.*

PROOF: Let the set in question by $X \subseteq \mathbb{P}^n$. The only thing that remains to be proven is that X satisfies the Hausdorff axiom. By lemma **??** on page **??** in Notes 3, if suffices to exhibit an open affine subset containing any two given points. This no big deal, given two distinct points in X, there is linear form λ on $\mathbb{A}^{n+1}$ that does not vanish at either. Hence both lie in the basic open subset $D_+(\lambda) \cap X$, which is affine by proposition 4.3 above. ❑

The following corollary is with proposition 4.2 above in mind, merely an observation

OK

DistingAreDisting

Corollary 4.1 *Let F be a homogeneous form on $\mathbb{A}^{n+1}$. The open set $D_+(F) \cap D_+(x_i)$ is affine. When the coordinates x_j/x_i on $D_+(x_i)$ are used, $D_+(F) \cap D_+(x_i)$ corresponds to the distinguish open set $D(F^d)$ of $\mathbb{A}^n$ where $F^d = F(x_0/x_i, \ldots, x_n/x_i)$.*

The projective Nullstellensatz

The correspondence between homogeneous ideal in the polynomial ring $k[x_0; \ldots; x_n]$ an closed subsets of the projective space $\mathbb{P}^n$ is like in the affine case governed by a Nullstellensatz.

There are however, some differences. In the projective case the ideals must be homogeneous, and there is a slight complications concerning the ideals with empty zero locus. Just as in the affine case if $1 \in \mathfrak{a}$, the zero locus of $\mathfrak{a}$ is empty, but neither ideals whose zero set in $\mathbb{A}^{n+1}$ is reduced to the origin (that is, $Z(\mathfrak{a}) = \{0\}$) have zeros in the projective space; the forbidden tuple $(0; \ldots; 0)$ is not the homogenous coordinates of any point. In other words, ideals $\mathfrak{a}$ whose radical equals the irrelevant ideal $\mathfrak{m}_+$, do not have zeros in $\mathbb{P}^n$.

A SIMPLE AND DOWN to earth and, not the least, a geometric way of thinking about the relation between the affine and the projective Nullstellensatz is via the affine cone $C(X) = \pi^{-1}X \cup \{0\}$ over a closed set $X \subseteq \mathbb{P}^n$ (recall the projection map $\pi\colon \mathbb{A}^{n+1} \setminus \{0\} \to \mathbb{P}^n$ that sends a point to the line joining it to the origin). This sets up one-to-one correspondence between closed non-trivial[3] cones in $\mathbb{A}^{n+1}$ and non-empty closed subsets in $\mathbb{P}^n$;

[3] Formally, a cone in $\mathbb{A}^{n+1}$ is a subset closed under homothety; that is, if $x \in C$, then $tx \in C$ for all scalars $t \in K$. Clearly the singleton $\{0\}$ comply to this definition, so $\{0\}$ is a cone. It is called the *trivial cone* or the *null cone*.

Lemma 4.2 *Associating the affine cone $C(X)$ to X gives a bijection between closed non-empty subsets of $\mathbb{P}^n$ and closed non-trivial cones in $\mathbb{A}^{n+1}$. The bijection respects inclusions, intersections and unions.*

ProjConeClosed

PROOF: Let $C \subseteq \mathbb{A}^{n+1}$ be a non-trivial cone and denote by C_0 the punctured cone; that is, the intersection $C_0 = C(X) \setminus \{0\}$ of C and $\mathbb{A}^{n+1} \setminus \{0\}$. There are two points to notice; firstly, C_0 is nonempty and if it is closed in $\mathbb{A}^{n+1} \setminus \{0\}$, its closure in $\mathbb{A}^{n+1}$ satisfies $\overline{C_0} = C$ (the origin can not be the only point on a line where a polynomial does not vanish), and secondly, $\pi^{-1}\pi(C_0) = C_0$. It follows that C is closed in $\mathbb{A}^{n+1}$ if and only if C_0 is closed in $\mathbb{A}^{n+1} \setminus \{0\}$, and by the definition of the Zariski topology, we infer that C is closed if and only if $\pi(C_0)$ is closed in $\mathbb{P}^n$. This shows that the correspondence in the lemma is surjective, and it is injective since it holds true that $\pi(\pi^{-1}C) = C$ because π is surjective.

The last statement in the lemma is a general feature of inverse images. ❏

To any closed subset $X \subseteq \mathbb{P}^n$, we let $I(X)$ be the ideal in $k[x_0, \ldots, x_n]$ generated by all homogeneous polynomials that vanish in X. It is clearly an homogeneous ideal, and one has $I(X) = I(C(X))$. Combining the bijection in lemma 4.2 above with the bijection between homogeneous radical ideals and closed cones from the affine Nullstellensatz[4], one arrives at the following version of the Nullstellensatz in a projective setting:

[4] A closed subset $C \subseteq \mathbb{A}^{n+1}$ is a cone if and only if the ideal $I(C)$ is homogeneous. Indeed, C is a cone presicely when a polynomial $f(x)$ vanishes along X if and only if $f(tx)$ does for all $t \in k$.

Proposition 4.4 (Projective Nullstellensatz) *Assume that $\mathfrak{a}$ is a homogeneous ideal in $k[x_0, \ldots, x_n]$.*

ProjNNS

- *Then $Z_+(\mathfrak{a})$ is empty if and only if $1 \in \mathfrak{a}$ or $\mathfrak{a}$ is $\mathfrak{m}_+$-primary; that is, $\mathfrak{m}_+^N \subseteq \mathfrak{a}$ for some N.*
- *If $Z_+(\mathfrak{a}) \neq \emptyset$, it holds true that $I(Z_+(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.*
- *Associaing $I(X)$ with X is a bijection bwteen closed non-empty subsets $X \in \mathbb{P}^n$ and radical homogeeous ideals I in $k[x_0, \ldots, x_n]$.*
- *The subset $Z_+(\mathfrak{a})$ is irreducible if and only if the radical $\sqrt{\mathfrak{a}}$ is a prime ideal.*

PROOF: We already argued for most of the statements; what remains is to clarify when $Z_+(\mathfrak{a})$ is empty. This is precisely when $Z_+(\mathfrak{a}) \subseteq \{0\}$. There are two cases; either $Z(\mathfrak{a}) = \emptyset$ or $Z(\mathfrak{a}) = \{0\}$; which by the Affine Nullstellensatz correspond to respectively $1\mathfrak{a}$ or $\sqrt{\mathfrak{a}} = I(\{0\}) = \mathfrak{m}_+$.

For the last statement, it is clear that X is irreducible if and only if the cone $C(X)$ over X is irreducible. ❏

Global regular functions on projective varieties

One of the fundamental theorem of affine varieties states that the space $\mathcal{O}_X(X)$ of global sections of the structure sheaf of an affine variety X —that is, the space of globally defined regular function—is equal to the coordinate ring $A(X)$. This is space is quit large and in many ways determines the structure of the variety.

For projective varieties the situation is quite different. The only globally defined regular functions are constant. True, one has the coordinate ring $S(X) = A(C(X))$ of the *cone* over X, but most elements there are not functions on X, not even the homogeneous ones.

By assumption X will be irreducible, and the same is then true for the cone $C(X)$. The ring $S(X) = A(C(X))$ is therefore an integral domain and has a fraction field which we shall denote by K. One calls $S(X)$ the *homogeneous coordinate ring* of X. It is a graded ring because the ideal $I(X)$ is homogeneous, and it has a decomposition into homogeneous parts $S(X) = \bigoplus_{i\geq 0} S(X)_i$, where $S(X)_i$ denotes the subspace of elements of degree i. The fraction field K of $S(X)$ is not graded, but the fraction of two homogeneous elements from $S(X)$ has a a degree, namely $\deg ab^{-1} = \deg a - \deg b$.

Homogeneous coodinate rings

PROBLEM 4.7 Let S be a graded ring. Show that the set T consisting of the homogeneous elements in S is a multiplicative system and that the localization S_T is a graded ring. Show S_T is an integral domain when S is, and that in that case, the part S_T^0 of elements of degree zero is a field. ★

PROBLEM 4.8 If $X \subseteq \mathbb{P}^n$ is a projective variety. Show that the rational function field $k(X)$ equals $S(X)_T^0$ (notation as in the previous exercise). ★

All regular function on open sets in $C(X)$ are elements of K, and two are equal as functions on an open if and only if they are the same element in K. The ground field k is contained in K as the constant functions on $C(X)$.

AS GENTLE BEGINNING let us consider the case of the projective space $\mathbb{P}^n$ itself. So let f be a global regular function on $\mathbb{P}^n$. Composing it with the projection $\pi\colon \mathbb{A}^{n+1} \setminus \{0\} \to \mathbb{P}^n$ we obtain a regular function $f \circ \pi$ on $\mathbb{A}^{n+1} \setminus \{0\}$. In example **??** on page **??** in Notes 3 we showed that every regular function on $\mathbb{A}^{n+1} \setminus \{0\}$ is a polynomial, hence $f \circ \pi$ is a polynomial. But $f \circ \pi$ is also constant on lines through the origin, and therefore must be constant. We thus arrive at the following:

Proposition 4.5 *It holds true that $\mathcal{O}_{\mathbb{P}^n}(\mathbb{P}^n) = k$.*

FOR A GENERAL projective variety the same is true, but considerably more difficult to prove. One has

GlobFuConst

Theorem 4.2 *The only globally defined regular functions on a projective variety $X \subseteq \mathbb{P}^n$ are the constants. In other words, it holds true that $\mathcal{O}_X(X) = k$.*

PROOF: Let f be a global regular function on X. Composed with the projection it gives a global regular function one the punctured cone $C(X) \setminus \{0\}$ which we still denote by f. It is an element in the function field K of the cone $C(X)$.

Let D_i be the distinguished open set in $C(X)$ where $x_i \neq 0$; that is, in earlier notation $D_i = C(X)_{x_i}$. We know[5] that the coordinate ring $A(D_i)$ satisfies $A(D_i) = S(X)_{x_i}$ so that for each index i the function f has a representation $f = g_i/x_i^{r_i}$ for some $g_i \in S(X)$ and some natural number r_i. The function f being constant along lines through the origin, it must be homogeneous of degree zero; in other words, g_i is homogeneous and $\deg g_i = r_i$.

[5] Lemma 3.3 one page 6 in notes 2.

So we have $x_i^{r_i} f = g_i$, and the salient point is that g_i lies in the homogeneous part $S(X)_{r_i}$. It follows that $hx_i^{r_i} f \in S(X)_{r_i+j}$ for all elements h of $S(X)$ that are homogeneous of degree j.

Now, chose an integer r so big that $r > \sum_i r_i$. Then any monomial M of degree r contains at least one of the variables, say x_i, with an exponent larger than r_i, and consequently $Mf \in S(X)_r$. In other words, multiplication by f leaves the finite dimensional vector space $S(X)_r$ invariant. It is a general fact (for instance, use the Cayley-Hamilton theorem), that f then satisfies a relation of the type

$$f^m + a_{m-1}f^{m-1} + \ldots + a_1 f + a_0 = 0$$

where the a_i are elements in the ground field k. This shows that $f \in K$ is algebraic over k, and since k is algebraically closed by assumption, f lies in k and is constant. ❑

AN IMPORTANT CONSEQUENCE of the theorem is that morphisms of projective varieties into affine ones necessarily are constant. Indeed, if $X \subseteq \mathbb{P}^n$ is projective and $Y \subseteq \mathbb{A}^m$ is affine, the component functions of a morphism $\phi\colon X \to Y \subseteq \mathbb{A}^m$ must all be constant according to the theorem we just proved. Hence we have

Corollary 4.2 *Any morphism from a projective variety to an affine one is constant.*

Another consequence is the following:

BaadeAffOgProj

Corollary 4.3 *A variety X which is both projective and affine, is reduced to a point.*

PROOF: The coordinate functions are regular functions on a subvariety $X \subseteq \mathbb{A}^n$, and according to the theorem they must be constant when X is projective. ❏

Morphisms from projective varoties

Quasi-projective varieties

A *quasi-projective variety* is a variety that is isomorphic to an open subset of a projective variety. Every affine variety is quasi-projective, and every open subset of an affine variety is quasi-projective. So the quasi-projective varieties s form a large and natural class of varieties.

Let X and Y be two quasi projective varieties and let $\phi\colon X \to Y$ be a set-theoretical map, which we want to check is a morphism. Assume that ϕ fits into a diagram

$$\begin{array}{ccc} C_0(X) & \xrightarrow{\Phi} & C_0(Y) \\ {\scriptstyle \pi_X}\downarrow & & \downarrow{\scriptstyle \pi_Y} \\ X & \xrightarrow[\phi]{} & Y \end{array}$$

where $C_0(X)$ and $C_0(Y)$ are the punctured cones and the two vertical maps are the usual projections and where Φ is a morphism.

Examples of this scenario are the cases where Φ is given as $\Phi(x) = (f_0(x), \ldots, f_m(x))$ where the f_i's hare homogeneous polynomials of the same degree and where X is the open subset of $\mathbb{P}^m$ of the points where the f_i's do not vanish simultaneously; that is, $X = \mathbb{P}^m \setminus Z_+(f_1, \ldots, f_m)$. On this set Φ descends to the map $\phi([x]) = (f_0(x); \ldots; f_m(x))$(these are legitimate homogenous coordinates, not all components being zero). Several interesting maps are of this form.

MorfismeLemma

Lemma 4.3 *With the notation as above, ϕ is a morphism*

PROOF: It suffices to see that $\phi|_{U_i}$ is a morphism for each of the basic open sets $U_i = D_+(x_i) \cap X$. Recall the natural map $\alpha_i\colon D_+(x_i) \to \mathbb{A}^{n+1} \setminus \{0\}$ which is a section of the canonical projection $\pi_{\mathbb{P}^n}$ over $D_+(x_i)$. Its basic property is being an isomorphism between $D_+(x_i)$ and A_i. Restricted to $U_i = D_+(x_i) \cap X$ the section α_i it gives a section α' of π_X which is an isomorphism $U_i \to A_i \cap C_0(X)$. It follows that

Recall that A_i is the locus in $\mathbb{A}^{n+1}$ where $x_i = 1$, and one has $\alpha_i(x_0; \ldots; x_N) = (x_0 x_i^{-1}, \ldots, x_n x_i^{-1})$.

$$\begin{array}{ccccc} A_i \cap C_0(X) & \hookrightarrow & C_0(X) & \xrightarrow{\Phi} & C_0(Y) \\ {\scriptstyle \alpha'}\uparrow & & {\scriptstyle \pi_X}\downarrow & & \downarrow{\scriptstyle \pi_Y} \\ U_i & \hookrightarrow & X & \xrightarrow[\phi]{} & Y \end{array}$$

$$\phi|_{U_i} = \phi \circ \pi_X \circ \alpha' = \pi_Y \circ \Phi$$

and since both maps to the right are morphisms, $\phi|_{U_i}$ is one as well. ❏

PROBLEM 4.9 In this exercise x, y and z are coordinates on the projective plane $\mathbb{P}^2$. Let $\phi(x, y, z) = (yz; xz; xy)$.

a) Show that ϕ defines a rational map from $\mathbb{P}^2$ to $\mathbb{P}^2$ defined on the complement of the three points $(1;0;0)$, $(0;1;0)$ and $(0;0;1)$.

b) What does ϕ do to the lines $Z_+(x)$, $Z_+(y)$ and $Z_+(z)$?

c) Let $U = D_+(xyz)$; that is, the subset where none of the coordinates vanish. Show that ϕ maps U into U and that $(\phi|_U)^2 = \mathrm{id}_U$. ★

PROBLEM 4.10 Let $Q \subseteq \mathbb{P}^3$ be the quadratic surface $xz - yw$. Let P be the point $P = (0;0;0;1)$. Define a map $\pi\colon Q \setminus \{P\} \to \mathbb{P}^2$ by $\pi(x;y;z;w) = (x;y;z)$. Let L and M be the two lines $L = Z_+(x,y)$ and $M = Z_+(z,y)$. Both lines lie on Q and the point P lies on both.

a) Show that the set $L \setminus \{P\}$ is collapsed to the point $(0;0;1)$ and the set $M \setminus \{P\}$ to $(1;0;0)$.

b) Show that the image of π is the set $D_+(y) \cup \{(0;0;1),(1;0;0)\}$

c) Show that π induces an isomorphism between $Q \setminus (L \cup M)$ and $D_+(y) = \mathbb{P}^2 \setminus Z_+(y)$. ★

EXAMPLE 4.5 — LINERA PROJECTIONS Let $\lambda_1, \ldots, \lambda_n$ be linear forms whose coomon zeros is the point $p \in \mathbb{P}^n$; for instance, if the λ_i's are just the coordinates $\lambda_i(x) = x_i$ then $p = (1;0;\ldots;0)$.

Show that $L(x) = (\lambda_1(x);\ldots;\lambda_n(x))$ is a morphism from $\mathbb{P}^n \setminus \{p\} \to \mathbb{P}^{n-1}$ called a linear projection from p. ☆

The d-uple embedding

This is a class morphisms of $\mathbb{P}^n$ into a larger projective space $\mathbb{P}^N$ given by all the monomials of a given degree d in $n+1$ variable[6]. The images are closed and the maps induce isomorphism between $\mathbb{P}^n$ and the images. More generally, morphisms between varieties having closed image and inducing isomorphism onto their image, are called *closed embeddings*; so the d-uple embeddings deserve their name; they are *closed embeddings*. We already have met some of these embeddings, the rational normal curves are of this shape with $n = 1$, and the Veronese surface is of the sort whith $n = 2$ and $d = 2$.

[6] There are $\binom{n+d}{d}$ such monomials, so the number N is given as $N = \binom{n+d}{d} - 1$.

The following lemma is almost obvious:

LiteLettLemma

Lemma 4.4 *Assume that the morphism $\mathbb{A}^n \to \mathbb{A}^{n+m}$ has a section that is a projection. Then ϕ is a closed embedding.*

PROOF: As a hint: After a coordinate change on $\mathbb{A}^{n+m}$, the map ϕ appears as the graph of a morphism $\mathbb{A}^n \to \mathbb{A}^m$. The details are left to the zealous students. ❏

To fix the notation let $\mathcal{I}$ be the set of sequence $I = (a_0, \ldots, a_n)$ of non-negative intregers such that $\sum_i a_i = d$; there are $N+1$ of them. The sequences I serve as indices for the monomials; that is, when

I run through $\mathcal{I}$, the polynomials $M_I = x_0^{a_0} \dots x_n^{a_n}$ will be all the monomials of degree d in the x_i's. We let $\{m_I\}$ for $I \in \mathcal{I}$, in some order, be homogeneous coordinates on the projective space $\mathbb{P}^N$.

The so-called d-uple embedding is the a map $\phi\colon \mathbb{P}^n \to \mathbb{P}^N$ that sends $x = (x_0; \dots, x_n)$ to the point in $\mathbb{P}^N$ whose homogeneous coordinates are given as $m_I(\phi(x)) = M_I$; that is,

$$m_I(\phi(x)) = x_0^{a_0} \cdot \ldots \cdot x_n^{a_n}$$

This is a morphism, as follows from lemma 4.3 above, but more is true:

Proposition 4.6 *The map ϕ is closed and ϕ is an isomorphism bteween $\mathbb{P}^n$ and the image $\phi(\mathbb{P}^n)$; that is, it is what is called a closed embedding.*

Proof: The are three salient points in the proof.

Firstly, the basic open subset $D_i = D_+(x_i)$, where the i-th coordinate x_i does not vanish, maps into one of the basic open subsets of $\mathbb{P}^N$, namely the one corresponding to the pure power monomial x_i^d.

To fix the notation, let m_i be the corresponding homogeneous coordinate[7] on $\mathbb{P}^N$; so that ϕ maps D_i into $D_+(m_i)$. The first one of these basic open subsets is isomorphic to $\mathbb{A}^n$, with the fractions $x_j x_i^{-1}$ as coordinates, and the second to $\mathbb{A}^N$ with $m_I m_i^{-1}$ as coordinates.

[7] That is m_i corresponds to the sequence $(0, 0, \dots, d, \dots, 0)$ with a d in slot i and zeros everywhere else.

Secondly, although the n basic open subsets $D_+(m_i)$ do not cover the entire $\mathbb{P}^N$, they cover the image $\phi(\mathbb{P}^n)$. Hence it suffices to the see that for each index i the restriction $\phi|_{D_i}$ has a closed image and is an isomorphism onto its image.

The thirds salient point is that $\phi|_{D_i}\colon \mathbb{A}^n \to A^N$ has a section that is a linear projection; once this is establishes we are through in view of the small and obvious lemma 4.4 above. To exhibit a section of $\phi|_{D_i}$, we introduce the n monomials $M_{i,j} = x_j x_i^{d-1}$ where $j \neq i$ and the corresponding homogenous coordinates $m_{i,j}$. Then $m_{i,j}(\phi(x)) m_i(\phi(x))^{-1} = x_j x_i^{-1}$. Hence the projection onto the affine space $\mathbb{A}^n$ corresponding to the coordinate $m_{i,j} m_i^{-1}$ is a section of the map $\phi|_{D_i}$, and we are through! ❑

As a corollary one has

Corollary 4.4 *Let $f(x_0, \dots, x_n)$ be a homogeneous polynomial. Then the distinguished open subset $D_+(f)$ of $\mathbb{P}^n$ is affine.*

Proof: Let d be the degree of f, and let ϕ be the d-uple embedding of $\mathbb{P}^n$ in $\mathbb{P}^M$. The homogeneous polynomial f is a linear combination $f = \sum_{I \in \mathcal{I}} \alpha_I M_I$ of the monomials M_I, and $D_+(f)$ is the intersection of the image $\phi(\mathbb{P}^n)$ with the basic open subset $D_+(L)$ of $\mathbb{P}^N$ where L is the linear form $L = \sum_{I \in \mathcal{I}} \alpha_I m_I$ corresponding to f. Now $D_+(L)$ is isomorphic to $\mathbb{A}^N$ and $\phi(D_+(f))$, which is isomorphic to $D_+(f)$, is therefore closed in $\mathbb{A}^N$, hence affine. ❑

Corollary 4.5 *Let $X \subseteq \mathbb{P}^n$ be a subvariety which is not a point, and let $f(x_0, \ldots, x_n)$ be a homogeneous polynomial. Then $Z_+(f) \cap X$ is not empty.*

PROOF: Assume that $X \cap Z_+(f) = \emptyset$. Then $X \subseteq D_+(f)$; but $D_+(f)$ is affine and therefore X being closed in $D_+(f)$ is affine. So X is both affine and projective. Corollary 4.3 on page 12 applies, and X is a point. ❑

Coordinate changes and linear subvarieties

Coordinate changes are ubiquous in mathematics and of paramount importance. Changing the homogeneous coordinates in a projective space is very similar to changing linear coordinates in an affine space $\mathbb{A}^{n+1}$, but there are a few differences due to the homogeneous coordinates merely being defined up to scalars.

The affine space $\mathbb{A}^n$ is equal to k^n and has in addition to the variety-structure we have given it, the structure of a vector space over the field k. This linear structure is to a certain extend inherited by the projective space $\mathbb{P}^n$, and manifests itself through the so called *linear subvarieties*, which we now shall to introduce.

Linear subvarieties

Linear subspaces of $\mathbb{A}^{n+1}$ project to subvarieties of $\mathbb{P}^n$ called *linear subvarieties*. To be precise, if $V \subseteq \mathbb{A}^{n+1}$ is a vector subspace, we let $\mathbb{P}(V) \subseteq \mathbb{P}^n$ be the subset $\mathbb{P}(V) = \{ [x] \mid x \in V \}$ which simply is the set of line lying in V. It is a closed subset and therefore a subvariety; indeed, linear functional are homogeneous polynomials of degree one, so the linear functionals cutting out V in $\mathbb{A}^{n+1}$ serve as equations for $\mathbb{P}(V)$ in $\mathbb{P}^n$.

Linear subvarieties

Clearly $\mathbb{P}(V)$ is isomorphic to $\mathbb{P}^m$ if $\dim_k V = m + 1$, and one says that $\mathbb{P}(V)$ is a linear subvariety of dimension m, thus anticipating the definition of the dimension of a general variety. Sometimes it is more convenient to work with the *codimension* of $\mathbb{P}(V)$ in $\mathbb{P}^n$; that is, the difference $n - \dim_k \mathbb{P}(V)$; which also equals $n + 1 - \dim_k V$.

The codimension

Two linear subvarieties $\mathbb{P}(V)$ and $\mathbb{P}(W)$ intersect along the linear subvariety $\mathbb{P}(V \cap W)$ which is the largest linear subvariety contained in both. Similarly, the smallest linear subvariety containing both is $\mathbb{P}(V + W)$. It is called the linear subvariety *spanned* by the two. When $m = 1$ we have *line*, and when $m = 2$ we called it *plane*.

Proposition 4.7 *Suppose $\mathbb{P}(V)$ and $\mathbb{P}(W)$ are linear subvarieties of $\mathbb{P}^n$ of dimension m and r respectively. Then it holds true that*

$$\dim \mathbb{P}(V) \cap \mathbb{P}(W) \geq m + r - n,$$

and equality holds if and only if $\mathbb{P}(V)$ *and* $\mathbb{P}(W)$ *span* $\mathbb{P}^n$*.*

A nice way of phrasing the proposition is the inequality

$$\operatorname{codim}\mathbb{P}(V) + \operatorname{codim}\mathbb{P}(W) \geq \operatorname{codim}(\mathbb{P}(V) \cap \mathbb{P}(W)),$$

which is an equality if and only if $\mathbb{P}(V)$ and $\mathbb{P}(W)$ span $\mathbb{P}^n$. In some sense the codimension is additive when the inresections is "good".

PROOF: The dimension formula from linear algebra states that

$$\dim_k(V + W) + \dim_k(V \cap W) = \dim_k V + \dim_k W,$$

and since $\dim_k(V + W) \leq n + 1$, one infers that

$$\dim \mathbb{P}(V) \cap \mathbb{P}(W) = \dim_k(V \cap W) - 1 \geq m + 1 + r + 1 - (n + 1) - 1 = m + r - n.$$

If equality holds, it follows that $\dim_k(V + W) = n + 1$; that is, $\mathbb{P}(V)$ and $\mathbb{P}(W)$ span $\mathbb{P}^n$. ❑

One instance of the proposition worthwhile to mention especially, is the case when the two linear subvarieties $\mathbb{P}(V)$ and $\mathbb{P}(W)$ are of *complementary dimension*; that is, when $n = m + r$. If $\mathbb{P}(V)$ and $\mathbb{P}(W)$ additionally also span the entire space $\mathbb{P}^n$, they intersect precisely in *one* point.

PROBLEM 4.11 Show that $\mathbb{P}(V)$ is isomorphic to $\mathbb{P}^m$ when $\dim_k V = m + 1$. ★

PROBLEM 4.12 Show that two different planes in $\mathbb{P}^3$ always intersect along a line. Show that two different lines in $\mathbb{P}^3$ meet if and only if they lie in common plane. ★

PROBLEM 4.13 Show that four hyperplanes in $\mathbb{P}^5$ intersect at least along a line. Show that five hyperplane in $\mathbb{P}^5$ has a non-empty intersection. Generalize. ★

JUST AS IN A VECTOR SPACE one can speak about points $p_1, \ldots, p_r$ in $\mathbb{P}^n$ being *linearly independent*. This simply means that if we represent the points p_i as $p_i = [v_i]$, the vectors v_i in $\mathbb{A}^{n+1}$ are linearly independent. And of course, the points are *linearly dependent* if they are not independent.

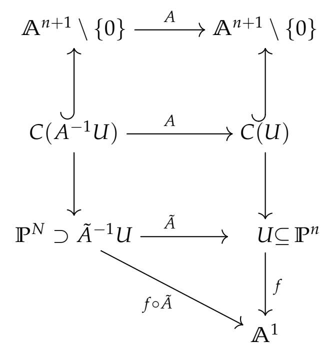
In geometric terms, the r points $\{p_i\}$ being independent means that the smallest linear subvariety containing the p_i's is of dimension $r - 1$; notice the shift in dimension compare to the affine case. For instance, two different points in $\mathbb{P}^2$ are linearly independent and lie on a line, whereas in $\mathbb{P}^3$ three points are linearly independent when they span a plane.

Changing homogeneous coordinates

Suppose that $A\colon k^{n+1} \to k^{n+1}$ is a linear map. Any line through the origin—or if you want a one dimesnional subsapce—is mapped by A eiher to a line through the origin or to zero. In former cae $[A(x)]$ is a well defined point in $\mathbb{P}^n$, and we thus obtain a map $\tilde{A}$ from the open subset $\mathbb{P}^n \setminus \mathbb{P}(\ker A)$ to $\mathbb{P}^n$.

Lemma 4.5 *The map $\tilde{A}$ is a morphism where ir is deined.*

Proof: Let $U \subseteq \mathbb{P}^n$ be open and f a regular function on U. If contemplate the diagram in the margin for a few second, you convince your self that $(f \circ \tilde{A}) \circ \pi = f \circ \pi \circ A$ (where we have skipped to indiacate restrictions) and that is regular; hence $f \circ \tilde{A}$ is regular. ❑



vector such that $A(v) \neq 0$, teh istakes lines through the origin tolines trough the origin, or if you want, one-dimesnional subsapces to one dimensional subspaces. So one suspects A to induce a map from the projective space $\mathbb{P}^n$ to itself, by the assignment $\tilde{A}[x] = [A(x)]$. If $x \in \ker A$ it holds that $A(x) = 0$ and $A(x)$ does not give a line thrpigh the origin. Hence, we only obtai a map $\tilde{A}$ from $\mathbb{P}^n \setminus \mathbb{P}(\ker A)$. Given any invertible $(n+1) \times (n+1)$-matrix $A = (a_{ij})$ with entries $a_{ij} \in k$. Then of course, $A(tx) = tA(x)$ for any $t \in k$, so A induces a well defined mapping $A\colon \mathbb{P}^n \to \mathbb{P}^n$, which easily is seen to be a morphism. It is even an isomorphism with inverse map induced by the matrix A^{-1}. Such a map is called a *linear automorphism* of $\mathbb{P}^n$.

Linear automorphisms

However, unlike in the affine case, for any non-zero scalar u, the matrix uA induces the *same* automorphism of $\mathbb{P}^n$ as A does. This leads us to introduce the group $\mathrm{PGl}(n+1, k) = \mathrm{Gl}(n+n, k)/k^*$; the group of invertible $n+1 \times n+1$-matrices modulo the normal subgroup consisting of scalar multiples of the identity matrix. This is the group of linear automorphisms of projective n-space.

Problem 4.14 Show that the induced map $A\colon \mathbb{P}^n \to \mathbb{P}^n$ is a morphism. ★

We illustrate this by the case of the projective line $\mathbb{P}^1$. Let A be the matrix

$$A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{00} \end{pmatrix}$$

In homogeneous coordinates the action of A on $\mathbb{P}^1$ is expressed as

$$A(x_0; x_1) = (a_{00}x_0 + a_{01}x_1; a_{10}x_0 + a_{11}x_1).$$

This action has much stronger homogeneity properties that in the affine case; one says that an action of a group G is *triply transitive* if two sets of three distinct points p_1, p_2, p_3 and q_1, q_2, q_3 there is group element $g \in G$ so that $g \cdot p_i = q_{ij}$.

Triply transitive actions

Proposition 4.8 *The action of* $\mathrm{PGl}(2, k)$ *on the projective line* $\mathbb{P}^1$ *is triply transitive.* TePunktHom

PROOF: Without loss generality we may assume that one of the three-point-sets consists of the points $e_1 = (1;0)$, $e_2 = (0;1)$ and $e_3 = (1,1)$. Since p_1 and p_2 are different points in $\mathbb{P}^1$, the lines in $\mathbb{A}^2$ upon which they lie are different, so if we chose a vector v_i in each, the v_i's will be linearly independent. Hence there is a matrix with $Ae_1 = p_1$ and $Ae_2 = p_2$.

The common *isotropy group* of the e_1 and e_2; that is, the matrices B such that $Be_i = e_i$ is easily seen to be the diagonal matrices

$$B = \begin{pmatrix} a_{00} & 0 \\ 0 & a_{11} \end{pmatrix}.$$

Now, such matrix a sends $(1;1)$ to $(a_{00};a_{11})$; hence as long as the the point $A^{-1}p_3$ is different from $(1;0)$ and $(1;0)$; *i.e.,* on the form $(a;b)$ with $a \cdot b \neq 0$; we can find a matrix B with $B(1;1) = A^{-1}p_3$ and $Be_i = e_i$ for $i = 1,2$. Then the composition AB sends e_i to p_i, and we are done. ❑

More one coordinate changes

There is a generalization of proposition 4.8 above to projective n-space. The action of $\mathrm{PGl}(n+1, k)$ si not $(n+2)$-transitive, since different points can be dependent, however, one has the following proposition whose proof is left as an exercise:

Proposition 4.9 *Given two sets of points* $p_1, \ldots, p_{n+2}$ *and* $q_1, \ldots, q_{n+2}$ *of projective n-space* $\mathbb{P}^n$*. Assume that no subset with* $n+1$ *elements of the two are linearly dependent. Show that there exists an* $(n+1) \times (n+1)$*-matrix* A *such that* $Ap_i = q_i$*.* HomGenLinInd

PROBLEM 4.15 Prove proposition 4.9. Show by examples that the condition about linearly independence can not be skipped. ★

PROBLEM 4.16 If A is a linear automorphism of projective n-space $\mathbb{P}^n$ that fixes $n+2$ points such that no selection of $n+1$ of them is linearly dependent, then A is a scalar matrix. ★

Example: Hypersurfaces

In the previous section we introduced the notation $\mathbb{P}(V)$ for the linear subspaces of a given projective space. They are projective spaces which are isomorphic to $\mathbb{P}^m$ with $m+1 = \dim_k V$, but the isomorphism depends heavily on a choice of coordinates. Since coordinates are man-made and usually by no means canonical, it is convenient to the extend te notation to any vector space V.

So given one, we let $\mathbb{P}(V)$ be the set of one-dimensional vector subspaces of V. To put a variety structure on V, we chose a basis for V tom obtain a linear isomorphism $V \to k^{m+1}$. This induces a bijection $\mathbb{P}(V) \to \mathbb{P}^m$ and with the help of this, we transport the Zariski topology and the structure sheaf on $\mathbb{P}^m$ to $\mathbb{P}(V)$ (details left as an exercise).

PROBLEM 4.17 Perform the transportation of structure in detail. Show that different choices of bases give identical structures on $\mathbb{P}(V)$ ★

One important instance of this construction is the projective spaces obtained from the homogeneous forms. To begin with, we introduce the notation V for the vector space of linear forms in the variables $x_0, \ldots, x_n$; that is, $V = \{ \sum_i a_i x_i \mid a_i \in k \}$. Generalizing this, for any natural number d, we let $S^d V$ be the vector space of forms of degree d in the variables $x_0, \ldots, x_n$. It is frequently called d-th *symmetric power* of V.

PROBLEM 4.18 Show that $\dim_k S^d V = \binom{n+d}{d}$. HINT: Induction on d. ★

The points in the projective space $\mathbb{P}(S^d V)$ associated with the symmetric power $S^d V$, are equivalence classes of homogeneous forms F in the variables $x_0, \ldots, x_n$, and a form F is equivalent to any of its non-zero scalar multiples $t \cdot F$.

Now, the equation of a hypersurface in $\mathbb{P}^n$ is of course only defined up to a non-zero scalar multiple, so $\mathbb{P}(S^d)$ is naturally identified with the set of hypersurfaces of degree d in $\mathbb{P}^n$—this is true at least when F has no irreducible factors of multiplicity more than one. In the latter case, points in $\mathbb{P}(S^d V)$ correspond to data consisting of the geometric set $Z_+(F)$ together with the multiplicities of the different components. That is, if $F = F_1^{d_1} \cdot \ldots \cdot F_r^{d_r}$ is the decomposition of F into irreducible factors, the point in $\mathbb{P}(S^d V)$ corresponds to the data consisting of the components $X_i = Z_+(F_i)$ of $Z_+(F)$ and the sequence of multiplicities $d_1, \ldots, d_r$.

This coupling between the algebra of homogeneous forms and geometry, it so fundamental that it merits to be formulated as a proposition:

Proposition 4.10 *There is a natural one-to-one correspondence between points in the projective space $\mathbb{P}(S^d V)$ and the set of sequences $X_1, \ldots, X_r$ and $d_1, \ldots, d_r$ of irreducible hypersurfaces X_i and natural numbers d_i so that $d = \sum_i d_i \deg X_i$.*

PROBLEM 4.19 Show that the hypersurfaces of degree d in $n + 1$

variable that pass by a given point in $\mathbb{P}^n$ constitute a hyperplane in $\mathbb{P}(S^r V)$. Show that those passing by r given points form a linear subvariety of codimension at most r. ★

PROBLEM 4.20 Given five points i $\mathbb{P}^2$, no three of which are colinear, show there is unique conic passing through them. ★

Example: Conic sections and the Veronese surface

In this section we study conic sections in the projective plane. This illustrates the strength of projective geometry, in that all irreducible conics are projectively equivalent; that is, up to coordinate change all irreducible conics are equal. Of the degenerate conics—that is, the reducible ones—there are just two types, again up change of coordinates: the union of two different lines and a "double line".

We also illustrate that geometric objects frequently come in families which are parametrized by other geometric objects, and that the study of these "secondary spaces" gives insight into the geometry of the "primary objects' and *vice versa*. The different quadratics forms in three variables, which are the equations of the conics, depend on six parameters, hence the conics are parametrized by a projective space of dimension five. The degenerate conics lie on a determinantal, cubic hypersurface and the double lines correspond to the points of the Veronese surface.

Conic sections

A conic C in $\mathbb{P}^2$ is given by a quadratic equations. If x_0, x_1 and x_2 are homogeneous coordinates on $\mathbb{P}^2$, such a quadratic equation is shaped like

$$F(x_0, x_1, x_2) = \sum_{i,j} a_{ij} x_i x_j = 0$$

where $A = (a_{ij})$ is a symmetric 3×3-matrix whose entries are from k; in other words, we have[8]

$$F(x) = xAx^t.$$

[8] Normally one prefer working with column vectors, but for obvious typographical reasons points x are represented with row vectors. Hence the occurrence of the transposed vector x^t several places.

The space of quadratic forms in three variables constitute an affine space $\mathbb{A}^6$. As the equation of a conic in $\mathbb{P}^2$ is defined only up to a non-zero scalar, and of course, it must not be identically zero, the space of conics is the corresponding projective space $\mathbb{P}^5$. One may also think about it as the space of non-zero symmetric 3×3-matrices (a_{ij}) modulo scalars; that is, the projective space space where a matrix A and the scaled matrix tA are considered equal.

Changing coordinates in $\mathbb{P}^2$ by an invertible 3×3-matrix B; that is, replacing x by xB gives the fresh equation

$$G(x) = F(xB) = xBAB^t x^t = x(BAB^t)x^t.$$

Hence the effect of the coordinate change on the symmetric matrix is to change A to BAB^t. So the action of $\mathrm{PGl}(3, k)$ on the space $\mathbb{P}^5$ of conics is to move the conic given by A to one given by BAB^t.

We saw in example **??** in Notes 2— as an application of the Gram–Schmidt procedure—that under the action of $\mathrm{PGl}(n, k)$ any symmetric matrix may be brought on a very special form D, where D is a diagonal matrix with 1's along the first part of the diagonal and 0's along the rest. In the 3×3-case there are three possible outcomes of this procedure:

$$D_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad D_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \qquad (2)$$

This means that up to projective equivalence conics are of three different shapes.

OutCome

The maximal rank of the symmetric matrix A is three, and this corresponds to the first outcome above. The conic is then irreducible, and its equation may be brought on the form

$$x_0^2 + x_1^2 + x_3^2 = 0,$$

or after another change of coordinates on the form $x_0x_1 - x_2^2$.

When the rank of A is two, the conic is reducible, and it is the union of two different lines. The equation becomes $x_0^2 + x_1^2 = 0$ after an appropriate base change, or if desired, a fresh coordinate change brings it on the form $x_0x_1 = 0$. Finally, the last case when the matrix A is of rank one, the conic is a double line, and the equation is $x_0^2 = 0$. To sum up

Proposition 4.11 *An irreducible conic in $\mathbb{P}^2$ has the equation $x_0x_1 - x_2^2$ in appropriate coordinates. If the conic is not irreducible, it is either the union of two lines or a double line with equations respectively $x_0x_1 = 0$ and $x_0^2 = 0$ in appropriate coordinates.*

Let V be the space of linear forms in x_0, x_1 and x_2. We have identified the space $\mathbb{P}(S^2V) \simeq \mathbb{P}^5$ of conics in $\mathbb{P}^2$ with the projective space of non-zero symmetric matrices up to scale. The identification is $A \mapsto F = xAx^t$.

This $\mathbb{P}^5$ is stratified by the closed subsets W_r where then rank of the symmetric matrix drops below r. In the present case of conics in $\mathbb{P}^2$ there are two strata. The larger is W_2 where the rank of A is it at most two. It is a hypersurface given by the vanishing of the determinant, which is a the cubic equation

$$\det A = 0.$$

The smaller locus is W_1 consists of rank one matrices and the corresponding conics are double lines. It is cut out by the 2×2-minors of A. There are 9 such, and each one is defines a quadratic hypersurface. The projective variety W_1 is isomorphic to $\mathbb{P}^2$ and is called the *Veronese surface*. Indeed, we just saw that the rank one quadratic forms are squares of linear forms. Indeed, one may write $A = \alpha^t \cdot \alpha$ where α is a row vector, and this implies that

$$F(x) = xAx^t = x\alpha^t \cdot \alpha x^t = L^2(x)$$

where $L(x) = x\alpha^t$. (remember, $x = (x_0, x_1, x_2)$)

Hence W_1 is the image of the map $\mathbb{P}^2 \simeq \mathbb{P}(V) \to \mathbb{P}^5$ sending the linear form $L(x_0, x_1, x_2)$ to $L(x_0, x_1, x_2)$. The factors of the a square being unique up to scale, this map is injective, and thus give s bijection with the Veronese surface.

It turns out to be an isomorphism.

Writing a linear form as $L = u_0u_0 + u_1u_1 + u_2u_2$ where the u_i are the coefficients, one finds that the consider the mapping

$$(u_0, u_1, u_2) \mapsto (u_0^2, u0u_1, u_0u_2, u_1^2, u_1u_2, u_2^2)$$

PROBLEM 4.21 Let $[A_0] \in V$ be a point in the Veronese surface. Choose coordinates so that $A_0 = D_3$ (notation as in equation (2) above).

a) Let $[A]$ be any other point in $\mathbb{P}(S^2V)$ and let t be a variable. Show that $\det(A_0 + tA)$ is a cubic polynomial in t with a double zero at $t = 0$.

b) Let $[A]$ and $[B]$ be two points on the Veronese surface. Show that line joining two points in the Veronese surface is entirely contained in the determinantal cubic.

★

PROBLEM 4.22 Show that any non-zero rank one symmetric matrix may be factored as $A = \alpha^t \cdot \alpha$ where α is a row vector unique up to scale. ★

Example: Elliptic cures and Weierstrass normal form

Among of the many gems in algebraic geometry the elliptic curves are may be the most brilliant ones; anyhow they are certainly aomg the oldest objects to be studied and in some marked the beginning of modern algebraic geomtery. The in the theory of so-called *elliptic integrals* and their inerses the *elliptic functions*; the fisrt calss of fucnftion not expressible in the elementary functions to be studied.

We shall not dive into the deep water of elliptic curves, but only approach them from the view point of cubic curves. All elliptic curves can be realised as a plane cubic curve, and even with the equeation on a verus special form called the Weierstrass normal form.

is the oldes and may be the most it has been polished through the enturies;

AN INFLECTION POINT of a plane curve C is a point where the tangent has a higher contact with the curve than tangent usually have. From calculus we know that the $y = x^3$ has an inflection point at the origin; the graf crosses the tanget at that point, or expressed analytically both te first and the second derivative vanish.

More generally, assume that the projevtive palne curve C in $\mathbb{P}^2$ is given by the homogeneous equation $f(x, y, z) = 0$. Let $p = (p_0; p_1; p_2)$ be a point on the curve and let $(x(u); y(u); z(u))$ be a linear parametrization[9] of a line L through p with the parameter value $u = 0$ corresponding to the point p. Then $f(x(u), y(u), z(u))$ is a polynomial in u of degree d, and it vanishes for $u = 0$ since the pint p lies on L. Moreover if L happens to be the tangent to C at p, it has double zero at $u = 0$ (meaning that its derivative vanishes as well), and we say p is an inflection point of C, if the polynomial $f(x(u), y(u), z(u))$ has a triple zero at $u = 0$ (that is the second derivative vanishes also).

[9] Strictly speaking, this is a local parametrization valid in an affine piece containing P. To get a global one, one needs two homogenous parameters $(t; u)$.

For a cubic curve, which is given by a cubic equation $f(x, y, z) = 0$, this means that the contact order is three, and that p is *the only* intersection point between the curve and the tangent. Indeed, the polynomial $f(x(t), y(t), z(t))$ is of degree three and has at most three zeros. In the case of P being an inflection point, it has a triple zero at the origin, and can have no other zeros.

For example, the curve

$$y^2 z = x^3 + axz^2 + bz^3 \tag{3}$$

has a flex at the point $(0 ; 1 ; 0)$. The line $z = 0$ has triple contact, since putting $z = 0$ reduces the equation to $x^3 = 0$—the line may be parametrized as $(x; 1; 0)$ with x as a parameter.

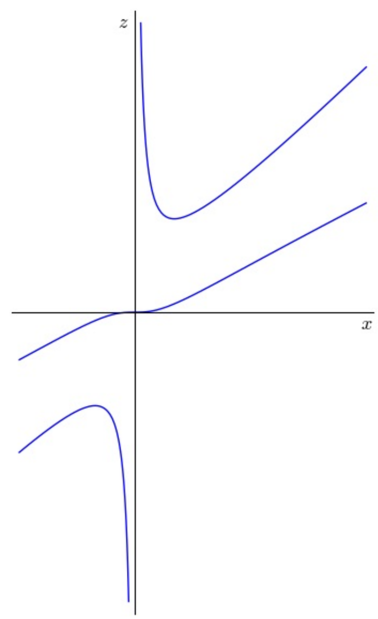


Figure 5: The curve $z = x(x - z)(x - 2z)$ has an inflection point a the origin

ExEq

BY A CLEVER CHOICE of coordinates on $\mathbb{P}^2(k)$ one may simplify the equation of an irreduicble cubic curve and bring it on a standard form. There are of course several standard forms around, their usefulness depends on what one wants to do, but the most prominent one is the one called the . This is also the one most frequently used in the arithmetic studies. In case the characteristic of k is not equal to 2 or 3, it is particularly simple.

Weierstrass normal form

The name Weierstrass normal form refers to the differential equation

$$\wp' = 4\wp^3 - g_2\wp - g_3$$

discovered by Weierstrass, and one of whose solution—the famous Weierstrass $\wp$-function—was used by him to parametrize complex elliptic curves. It seems that the Norwegian mathematician Trygve Nagell was the first[10] to show that genus one curves over $\mathbb{Q}$ with a given $\mathbb{Q}$-rational point O, can be embedded in $\mathbb{P}^2$ with the point O as a flex.

[10] This is what J. W.S. Cassels writes in his obituary of Nagell.

The idea behind the Weierstrass normal form is to place the specified inflection point at infinity—that is at the point $(0;1;0)$—and chose the z-coordinate in a manner that $z = 0$ is the inflectionally tangent.

Proposition 4.12 *Assume that E is as smooth, cubic curve defined over k with a flex at $P = (0;1;0)$. Then there is linear change of coordinates with entries in k, such that E has the affine equation*

$$y^2 + a_1xy + a_3y = g(x) \qquad \text{(WW)}$$

where a_1 and a_3 are elements in k, and $g(x)$ is a monic, cubic polynomial with coefficients in k.

GeneralWeierstrass

Proof: The first step is to choose coordinates on $\mathbb{P}^2$ such that the point $P = (0;1;0)$ is the flex and such that the tangent to E at P is the line $z = 0$. That the curve passes through $(0;1;0)$ amounts to there being no term y^3 in the equation $f(x,y,z)$, and that $z = 0$ is the inflectionally tangent amounts to there being no terms y^2x or yx^2. Indeed, in affine coordinates round P the dehomogenized polynomial defining E—that is $f(x,1,z)$—has the form

$$f(x,1,z) = z + q_2(x,z) + q_3(x,z),$$

where the $q_i(x,z)$'s are homogenous polynomials of degree i, and where the coefficient of the z-term has been absorbed in the z-coordinate. Now we exploit that $z = 0$ is the inflectionally tangent. Putting $z = 0$, we get

$$f(x,1,0) = q_2(x,0) + q_3(x,0),$$

and $f(x,1,0)$ has a triple root at the origin so $q_2(x,0)$ must vanish identically. Hence

$$f(x,1,z) = z + a_1xz + a_3z^2 + q_3(x,z)$$

with $a_1, a_3 \in k$. The homogeneous equation of the curve is thus

$$y^2z + a_1xyz + a_3yz^2 = G(x,z) \tag{4}$$

where $G(x,z) = -q_3(x,z)$. Write $G(x,z)$ as $G(x,z) = \gamma x^3 + zr(x,z)$ where $r(x,z)$ is homogenous of degree two. Since the curve is irreducible, we have $\gamma \neq 0$ and may change the coordinate z to γz. By cancelling γ throughout the equation, one can assume $\gamma = 1$, so that $g(x) = G(x,1)$ is a monic polynomial. ❑

HomogenW

There is a standard notation for the coefficients of the polynomial $g(x)$ going like this:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{WWII}$$

and there is a very good reason behind the particular choice of the numbering the coefficients which will be clarified in the following example. (See also examples **??** and **??** on page **??**).

GeneralWeierstrassII

Example 4.6 — Scaling If one replaces x by c^2x and y by c^3y in (WWII), one obtains

Skalering3

$$c^6y^2 + c^5a_1xy + c^3a_3y = c^6x^3 + c^4a_2x^2 + c^2a_4x + a_6.$$

Scaling the equation by c^{-6} one arrives at the Weierstrass equation

$$y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6,$$

where $a'_n = c^{-n}a_n$. And this certainly explains the way of indexing the coefficients. ☆

Simple Weierstrass form With some restrictions on the characteristic of k the Weierstrass equation can be further simplified. If the characteristic is different from two, one may complete the square on left the side of (4), that is, one replaces y by $y + (a_1x + a_2z)/2$. This transforms (4) into an equation of the form

$$y^2z = G(x,z)$$

where G is a homogenous polynomial of degree three (another than the G above), and after a scaling of the z-coordinate similar to the one above it will be monic in x.

In case the characteristic is not equal to three, there is a standard trick to eliminate the quadratic term of a cubic polynomial. It disappears on replacing x by $x - \alpha/3$ with α the coefficient of the quadratic term. We therefore have

WeirstrassI

Proposition 4.13 *Assume that k is a field whose characteristic is not 2 or 3. If E is a smooth, cubic curve defined over k having a k-rational inflection* *point, then there is linear change of coordinates with entries in k, such that the affine equation becomes*

$$y^2 = x^3 + ax + b \tag{W}$$

where $a, b \in k$.

Weierstrassl

The equation shows that a point (x, y) lies on the curve if and only if $(x, -y)$ lies there. Hence there is a regular map $\iota\colon E \to E$ with $\iota(x, y) = (x, -y)$. It is called . (Common usage is to call maps whose square is the identity involutions).

the canonical involution of E

Appendix: Graded rings and homogeneous polynomials.

A ring is said to be graded if there is a decomposition of S as direct sum

$$S = \bigoplus_{i \geq 0} S_i$$

a priori as abelian groups, subjected to the condition that

$$S_i \dot{S}_j \subseteq S_{i+j}.$$

for all i and j- The elements in S_i are said to be *homogeneous* of degree i. The direct sum decomposition in xxx tells us that any element s in S can be expanded a $s = \sum_i s_i$ as finite sum of homogeneous elements, and the condition xxx tells us tat $\deg s\dot{t} = \deg s + \deg t$.

PROBLEM 4.23 Let $V \subseteq \mathbb{A}^{n+1}$ be a linear subspace of dimension $m + 1$. Show that V is a cone and that the corresponding projective set $\mathbb{P}(V)$ is isomorphic to $\mathbb{P}^n$. Show that if W is another linear subspace of dimension $m' + 1$ and $m + m' \geq n$, then $\mathbb{P}(V)$ and $\mathbb{P}(W)$ has a non-empty intersection. ★

PROBLEM 4.24 Show that two different lines in $\mathbb{P}^2$ meet in exactly one point. ★

PROBLEM 4.25 Show that n hyperplanes in $\mathbb{P}^n$ always have a common point. Show that n general hyperplane meet in one point. ★

PROBLEM 4.26 Let $p_0, \ldots, p_n$ be $n + 1$ points in $\mathbb{P}^n$ and let $v_0, \ldots, v_n$ be non-zero vectors on the corresponding lines in $\mathbb{A}^{n+1}$. Show that the p_i's lie on a hyperplane if and only if the v_i's are linearly independent. ★