MAT4210—Algebraic geometry I: Notes 2

The Zariski topology and irreducible sets

26th January 2018

Hot themes in notes 2: The Zariski topology on closed algebraic subsets—irreducible topological spaces—Noetherian topological spaces—-primary decomposition and decomposition of noetherian spaces into irreducibles—polynomial maps—quadratic forms.

Preliminary version 1.1 as of 26th January 2018 at 10:27am—Prone to misprints and errors—new version will follow.
Changes from 0.1: Added a few exercises at the end. New figure to example 2.10;
Changes from 0.2: Added comments on homogeneous poly's and monomial ideals. New example 2.11 on page 13 about quadratic forms.
Changes form 1.0: Corrected a stupid error in example 2.10 on page 13 and a few misspellings. Corrected the formulation of problem 2.12

Geir Ellingsrud — ellingsr@math.uio.no

Introduction

The realm of algebraic geometry is much bigger than the corner occupied by the closed algebraic sets. There are many more geometric objects, several of which will be the principal objects of our interest. However, the closed algebraic sets are fundamental and serve as building blocks. Just like a smooth manifold locally looks like an open ball in euclidean space, our spaces will locally look like a closed algebraic set, or in a more restrictive setting, like an affine variety. Before giving the general definition, we need to know what "locally" means, and of course, this will be encoded in a topology. The topologies that are used, are particularly well adapted to algebraic geometry, and they are called *Zariski topologies* after one of the great algebraic geometers Oscar Zariski.

The Zariski topology is of course useful in several other ways as well. For instance, it leads to a general concept of irreducible topological spaces and a decomposition of spaces into irreducible components—a generalization of the primary decomposition of ideals in Noetherian rings.

Oscar Zariski (1899–1986)
Russian–American mathematician

The Zariski topology

In Notes 1 we established the tight relation between closed algebraic sets and ideals in polynomial rings, and among those relations were the following two:

- ❏ $Z(\sum_i \mathfrak{a}_i) = \bigcap_i Z(\mathfrak{a}_i)$;
- ❏ $Z(\mathfrak{a} \cap \mathfrak{b}) = Z(\mathfrak{a}) \cup Z(\mathfrak{b})$,

where $\mathfrak{a}$ and $\mathfrak{b}$ are ideals and $\{\mathfrak{a}_i\}_{i\in I}$ any collection of ideals in $k[x_1,\ldots,x_n]$. The first relation shows that the intersection of arbitrarily many closed algebraic sets is a closed algebraic set, the second that the union of two is closed algebraic (hence the union of finitely many). And of course, both the empty set and the entire affine space are closed algebraic sets (zero loci of respectively the whole polynomial ring and the zero ideal). The closed algebraic sets in $\mathbb{A}^n$ therefore fulfill the axioms for being the closed sets of a topology. This topology is called the *Zariski topology*.

The Zariski topology

Every closed algebraic set X in $\mathbb{A}^n$ has a Zariski topology as well, namely the topology induced from the Zariski topology on $\mathbb{A}^n$. The closed sets of this topology are easily seen to be those contained in X. These are the zero loci of ideals $\mathfrak{a}$ containing $I(X)$; that is, of those $\mathfrak{a}$'s with $I(X)\subseteq\mathfrak{a}$. Such ideals are in one-to-one correspondence with the ideals in the coordinate ring $A(X) = k[x_1,\ldots,x_n]/I(X)$; in other words, the Zariski closed sets in X are the zero loci of the ideals in $A(X)$. And if we confine the $\mathfrak{a}$'s to be radical ideals, the correspondence is one-to-one.

Example 2.1 The closed algebraic sets of $\mathbb{A}^1$ are apart from the empty set and $\mathbb{A}^1$ itself just the finite sets. Indeed, the polynomial ring $k[x]$ is a PID so that any ideal is shaped like $(f(x))$, and the zeros of f are finite in number. The Zariski open sets are therefore those with finite complements.

ZarTopA1

In $\mathbb{A}^2$ the closed sets are more complicated. Later on we shall show that they are finite unions of either points or subsets shaped like $Z(f(x,y))$ where f is a polynomial in $k[x,y]$. Notice that this is not the product topology on $\mathbb{A}^2$. Indeed, the closed sets in the product topology are unions of intersections of inverse images of points from the two factors, and these are easily seen to be finite unions of points or lines "parallel to one of the axes"; that is, sets of the form $Z(x-a)$ or$Z(y-a)$. But, for instance, a quadric like the hyperbola $xy=1$ is not among those. ☆

The open sets are of course the complements of the closed ones, and among the open sets there are some called *distinguished open sets* that play a special role. They are the sets where a single polynomial does not vanish. If f is any polynomial in $k[x_1,\ldots,x_n]$, we define

The distinguished open sets

$$X_f = \{\, x\in X \mid f(x)\neq 0\,\},$$

which clearly is open in X being the complement of $Z(f)\cap X$. Another common notation for X_f is $D(f)$.

Proposition 2.1 *Let X be a closed algebraic set. The distinguished open sets form a basis for the Zariski topology on X.*

PROOF: Fix an open set U. The complement U^c is closed and hence of the form $U^c = Z(\mathfrak{a})$ for some ideal $\mathfrak{a}$ in $A(X)$. If $\{f_i\}$ is a set of generators for $\mathfrak{a}$, it holds true that $Z(\mathfrak{a}) = \bigcap_i Z(f_i)$, and consequently $U = Z(\mathfrak{a})^c = \bigcup_i U_{f_i}$. ❑

WHEN THE GROUND FIELD is the field of complex numbers $\mathbb{C}$, the affine space $\mathbb{A}^n(\mathbb{C}) = \mathbb{C}^n$ has in addition to the Zariski topology the traditional metric topology, and a closed algebraic set X in $\mathbb{A}^n$ inherits a topology from this. The induced topology on X is called *the complex* or *the strong* topology.

The complex or strong topology

The Zariski topology is very different from the strong topology. Polynomials are (strongly) continuous, so any Zariski-open set is strongly open, but the converse is far from being true. For example, in contrast to the usual topology on $\mathbb{C}$, the Zariski topology on the affine line $\mathbb{A}^1(\mathbb{C})$, as we saw in example 2.1 above,is the topology of finite complements; a non-empty set is open if and only if the complement is finite.

The Zariski topology has, however, the virtue of being defined whatever the ground field is (as long as it is algebraically closed), and the field can very well be of positive characteristic.

Irreducible topological spaces

A topological space X is called *irreducible* if it is not the union of two proper non-empty closed subsets. That is, if $X = X_1 \cup X_2$ with X_1 and X_2 both being closed, either $X_1 = X$ or $X_2 = X$.

Irreducible topological spaces

If X is a closed algebraic subset of $\mathbb{A}^n$, one may translate the topological property of being irreducible into an algebraic property of the ideal $I(X)$: If $I(X) = \mathfrak{a} \cap \mathfrak{b}$ then either $\mathfrak{a} = I(X)$ or $\mathfrak{b} = I(X)$, and in commutative algebra such ideals are called *irreducible* (guess why!). Prime ideals are examples of irreducible ideals, but there are many more. However, irreducible ideals are *primary ideal*, and this observation is at the base of the theory of primary decomposition in Noetherian rings.

Taking complements, we arrive at the following characterization of irreducible spaces:

Lemma 2.1 *A topological space X is irreducible if and only if the intersection of any two non-empty open subsets is non-empty.*

PROOF: Assume first that X is irreducible and let U_1 and U_2 be two open subset. If $U_1 \cap U_2 = \emptyset$, it would follow, when taking complements, that $X = U_1^c \cup U_2^c$, and X being irreducible, we infer that

$U_i^c = X$ for either $i = 1$ or $i = 2$; whence $U_i = \emptyset$ for one of the i's. To prove the other implication, assume that X is expressed as a union $X = X_1 \cup X_2$ with the X_i's being closed. Then $X_1^c \cap X_2^c = \emptyset$; hence either $X_1^c = \emptyset$ or $X_2^c = \emptyset$, and therefore either $X_1 = X$ or $X_2 = X$. ❑

There are a few properties irreducible spaces have that follows immediately. Firstly, every open non-empty subset U of an irreducible space X is dense. Indeed, if $x \in X$ and V is any neighbourhood of x, the lemma tells us that $U \cap V \neq \emptyset$, and x belongs to the closure of U.

Secondly, every non-empty open subset U of X is irreducible. This follows trivially since any two non-empty open sets of U are open in X, hence their intersection is *a fortiori* non-empty.

Thirdly, the closure $\overline{Y}$ of an irreducible subset Y of X is irreducible. For if U_1 and U_2 are two non-empty open subsets of $\overline{Y}$, it holds true that $U_i \cap Y \neq \emptyset$, and hence $U_1 \cap U_2 \cap Y \neq \emptyset$ since Y is irreducible, and *a fortiori* the intersection $U_1 \cap U_2$ is non-empty.

Fourthly, continuous images of irreducible spaces are irreducible. If $f\colon X \to Y$ is surjective and continuous and U_i for $i = 1, 2$ are open and non-empty, it follows that $f^{-1}(U_i)$ are open and non-empty (the map f is surjective) for $i = 1, 2$. When X is irreducible, it holds that $f^{-1}(U_1 \cap U_2) = f^{-1}(U1) \cap f^{-1}(U_2) \neq \emptyset$, and so $U_1 \cap U_2$ is not empty.

Summing up for later reference, we state the following lemma:

Lemma 2.2 *Open non-empty sets of an irreducible set are irreducible and dense. Closures and continuous images of irreducible sets are irreducible.* IrredLemma

We should also mention that Zariski topologies are far from being Hausdorff; it is futile to search for disjoint neighbourhoods when all non-empty open subsets meet!

Closed algebraic sets in the affine space $\mathbb{A}^n$ are of special interest, and we have already alluded to the algebraic equivalent of being irreducible. Here is the formal statement and a proof:

Proposition 2.2 *An algebraic set $X \in \mathbb{A}^n$ is irreducible if and only if the ideal $I(X)$ of polynomials vanishing on X is prime.*

As a particular case we observe that the affine space $\mathbb{A}^n$ itself is irreducible.

Proof: Assume that X is irreducible and let f and g be polynomials such that $fg \in I(X)$, which implies that $X \subseteq Z(f) \cup Z(g)$. Since X is irreducible, it follows that either $Z(g) \cap X$ or $Z(f) \cap X$ equals X. Hence one has either $X \subseteq Z(f)$ or $X \subseteq Z(g)$, which for the ideal $I(X)$ means that either $f \in I(X)$ or $g \in I(X)$.

The other way around, assume that $I(X)$ is prime and that $X = Z(\mathfrak{a}) \cup Z(\mathfrak{b})$ with $\mathfrak{a}$ and $\mathfrak{b}$ being radical ideals. Then it holds that $I(X) = \mathfrak{a} \cap \mathfrak{b}$ and because $I(X)$ is prime, we deduce that $I(X) = \mathfrak{a}$ or $I(X) = \mathfrak{b}$. Hence $X = Z(\mathfrak{a})$ or $X = Z(\mathfrak{b})$. ❑

ALGEBRAIC SETS that are the zero locus of one single polynomial—that is, sets X such that $X = Z(f)$—are called *hypersurfaces*. They are all-important players in our story. Curves in $\mathbb{A}^2$ and surfaces in $\mathbb{A}^3$ are well known examples of this sort.

Hypersurfaces

In general hypersurfaces are somehow more manageable than general algebraic sets—even though the equation can be complicated, there is as least just one!

If f is a linear polynomial, $Z(f)$ is called a *hyperplane*—basically a hyperplane is just a linear subspace of dimension $n-1$ in $\mathbb{A}^n$.

Hyperplanes

The Nullstellensatz tells us that (f) and the radical $\sqrt{(f)}$ have the same zero locus, so every hypersurface has a polynomial f without multiple factors as defining polynomial. Moreover, we know that a polynomial f generates a prime ideal if and only it is irreducible—this is just the fact that polynomial rings are UFD. Hence a hypersurface is irreducible if and only if it can be defined by an irreducible polynomial.

Proposition 2.3 *Let f be a polynomial in $k[x_1, \ldots, x_n]$. If f is an irreducible polynomial, the hypersurface $Z(f)$ is irreducible. If the hypersurface $Z(f)$ is irreducible, then f is a power of some irreducible polynomial.*

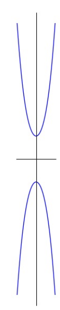


Figure 1: A hyperelliptic curve.

EXAMPLE 2.2 Polynomials shaped like $f(x) = y^2 - P(x)$ are irreducible unless $P(x)$ is a square; that is $P(x) = Q(x)^2$. Indeed; if $f = A \cdot B$ either both A and B are linear in y or one of them does not depend on y at all. In the former case $A(x,y) = y + a(x)$ and $B(x,y) = y + b(x)$ which gives

$$y^2 - P(x) = (y + a(x)) \cdot (y + b(x)) = y^2 + (a(x) + b(x)) \cdot y + a(x)b(x),$$

and it follows that $a(x) = -b(x)$. In the latter case one finds

$$y^2 - P(x) = (y^2 + a(x)) \cdot b(x)$$

which implies that $b(x) = 1$ and hence $f(x)$ is irreducible. When the polynomial $P(x)$ has merely simple zeros, the curve defined by f is called a *hyperelliptic curve*, and if $P(x)$ in addition is of the third degree, it is said to be an *elliptic curve*. In figures 1 and 2 in the margin we have depicted (the real points of) two, both with $P(x)$ of the eighth degree. Can you explain the qualitative difference between the two?

Hyperelliptic curves

We already met some elliptic curved in Notes 1, and they are omnipresent in both geometry and number theory and we shall study them closely later on. ☆

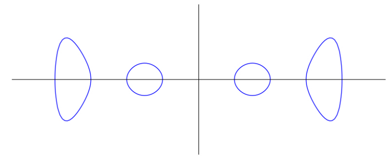


Figure 2: A hyperelliptic curve.

EXAMPLE 2.3 Our second example is a well known hypersurface, namely the determinant. It is one of many interesting algebraic sets that appear as subsets of the matrix-spaces $\mathbb{M}_{n,m} = \mathbb{A}^{nm}$ which are defined by rank conditions. The example is about the determinant $\det(x_{ij})$ of a "generic" $n \times n$-matrix; that is, one with independent variables as entries. It is a homogenous polynomial of degree n.

We shall see that it is irreducible by a specialization technic. Look a matrices like

$$A = \begin{pmatrix} t & y_1 & 0 & 0 & \dots & 0 \\ 0 & t & y_2 & 0 & \dots & 0 \\ 0 & & \ddots & & \ddots & 0 \\ 0 & \dots & 0 & t & y_{n-2} & 0 \\ 0 & \dots & 0 & 0 & t & y_{n-1} \\ y_n & \dots & 0 & 0 & 0 & t \end{pmatrix}$$

with a variable t's along the diagonal, and variables y_i's along the first "supra-diagonal" and y_n in the lower left corner; in other words the specialization consists in putting $x_{ii} = t$, $x_{i,i+1} = y_i$ for $i \leq n-1$ and $x_{n1} = y_n$, and the rest of the x_{ij}'s are put to zero.

It is not difficult to show that $\det A = t^n - (-1)^n y_1 \cdot \ldots \cdot y_n$ and that this polynomial is irreducible. A potential factorization $\det(x_{ij}) = F \cdot G$ with F and G both being of degree less than n must persist when giving the variables special values, but as $\det A$ is irreducible and of the degree of is n, we conclude that there can be no such factorization. ☆

PROBLEM 2.1 With notation as in the example, show that the determinant $\det A$ is given as $\det A = t^n - (-1)^n y_1 \cdot \ldots \cdot y_n$ and that this is an irreducible polynomial. ★

Emmy Noether (1882–1935)
German mathematician

Decomposition into irreducibles

From commutative algebra we know that ideals in Noetherian rings have a *primary decomposition*. An ideal $\mathfrak{a}$ can be expressed as an intersection $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r$ where the $\mathfrak{q}_i$'s are primary ideals. Recall that $\mathfrak{q}_i$ being primary means the radicals $\sqrt{\mathfrak{q}_i}$ are a prime ideals, and the primes $\sqrt{\mathfrak{q}_i}$ are called the *primes associated* to $\mathfrak{a}$. The decomposition is not always unique. The associated prime ideals are unique as are the components $\mathfrak{q}_i$ corresponding to minimal associated primes, but the so called embedded components[1] are not. For instance $(x^2, xy) = (x) \cap (x^2, y)$ but also $(x^2, xy) = (x) \cap (x^2, xy, y^2)$.

[1] A primary component $\mathfrak{q}_i$ is *embedded* if $\sqrt{\mathfrak{q}_i}$ contains the radical $\sqrt{\mathfrak{q}_j}$ of another component $\mathfrak{q}_j$.

A PROPERTY of ideals in the polynomial ring $k[x_1, \ldots, x_n]$ translates usually to a property of algebraic sets, so also with the primary decomposition. In geometric terms it reads as follows. Let $Y = Z(\mathfrak{a})$ for an ideal $\mathfrak{a} \subseteq k[x_1, \ldots, x_n]$ and write down the primary decomposition of $\mathfrak{a}$:

$$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r.$$

Putting $Y_i = Z(\sqrt{\mathfrak{q}_i})$ we find $Y = Y_1 \cup Y_2 \cup \ldots \cup Y_r$, where each Y_i is an irreducible closed algebraic set in $\mathbb{A}^n$. If $\sqrt{\mathfrak{q}_i}$ is not minimal among the associated primes, say $\sqrt{\mathfrak{q}_j} \subsetneq \sqrt{\mathfrak{q}_i}$, it holds that $Y_i \subseteq Y_j$ and the component Y_i contributes nothing to intersection and can be discarded.

A decomposition $Y = Y_1 \cup \ldots \cup Y_r$ of any topological space is said to be *redundant* if one can discard one or more of the Y_i's without changing the union. That a component Y_j can be discarded is equivalent to Y_j being contained in the union of rest; that is, $Y_j \subseteq \bigcup_{i \neq j} Y_i$. A decomposition that is not redundant, is said to be *irredundant*.

Irredudant decompositions

primeDekompAffine

Proposition 2.4 *Any closed algebraic set $Y \subseteq \mathbb{A}^n$ can be written as an irredundant union*

$$Y = Y_1 \cup \ldots \cup Y_r$$

where the Y_i's are irreducible closed algebraic subsets.

A DECOMPOSITION result like proposition 2.4 above holds for a much broader class of topological spaces than the closed algebraic sets. The class in question is the class of so called *Noetherian topological spaces*; they comply to the requirement that every descending chain of closed subsets is eventually stable. That is; if $\{X_i\}$ is a collection of closed subsets forming a chain

Noetherian topological spaces

$$\ldots X_{i+1} \subseteq X_i \subseteq \ldots \subseteq X_2 \subseteq X_1,$$

it holds true that for some index r one has $X_i = X_r$ for $i \geq r$. It is easy to establish, and left to the zealous students, that any subset of a Noetherian space endowed with the induced topology is Noetherian. Notice also that common usage in algebraic geometry is to call a topological space *quasi-compact* if every open covering can be reduced to a finite covering.

By common usage in mathematics a compact space is Hausdorff. The “Zariski"-like” spaces are far from being Hausdorff, therefore the notion quasi-compact.

Quasi-compact

Lemma 2.3 *Let X be a topological space. The following three conditions are equivalent:*

- *X is Noetherian;*
- *Every open subset of X is quasi-compact;*
- *Every non-empty family of closed subsets of X has a minimal member.*

The last statement leads to the technic called *Noetherian induction*—proving a statement about closed subsets, one can work with a minimal "crook"; *i.e.*, a minimal counterexample.

PROOF: Assume to begin with that X is Noetherian and let Σ be a family of closed sets without a minimal elements. We shall recursively construct a strictly descending chain that is not stationary. Assume a chain

$$X_r \subset X_{r-1} \subset \ldots \subset X_1$$

of length r has been found; to extend it just append any subset in Σ strictly contained in X_r, which does exist since Σ has no minimal member.

Next assume every Σ has a minimal member and let $\{U_i\}$ be an open covering of X. Let Σ be the family of closed sets being finite intersections of complements of members of the covering. It has a minimal element Z. If U_j is any member of the covering, it follows that $Z \cap U_j^c = Z$, hence $U_j \subseteq Z^c$, and by consequence $U = Z^c$.

Finally, suppose that every open U in X is quasi-compact and let $\{X_i\}$ be a descending chain of closed subsets. The open set $U = X \setminus \bigcap_i X_i$ is quasi-compact by assumption and covered by the ascending collection $\{X_i^c\}$, hence it is covered by finitely many of them. The collection $\{X_i^c\}$ being ascending, we can infer that $X_r^c = U$ for some r; that is, $\bigcap_i X_i = X_r$ and consequently it holds that $X_i = X_r$ for $i \geq r$. ❑

The decomposition of closes subsets in affine space as a union of irreducibles can be generalized to any Noetherian topological space:

Theorem 2.1 *Every closed subset Y of a Noetherian topological space X has an irredundant decomposition $Y = Y_1 \cup \ldots \cup Y_r$ where each is Y_i is a closed and irreducible subset of X. Furthermore, the decomposition is unique.*

Irreducible components

The Y_i's that appear in the theorem are called the *irreducible components* of Y. They are *maximal* among the closed irreducible subsets of Y.

PROOF: We shall work with the family Σ of those closed subsets of X which can not be decomposed into a finite union of irreducible closed subsets; or if you want, the set of counterexamples to the assertion in the theorem—and of course, we shall prove that it is empty!

Assuming the contrary—that Σ is non-empty—we can find a minimal element Y in Σ because X by assumption is Noetherian. The set Y can not be irreducible, so $Y = Y_1 \cup Y_2$ where both the Y_i's are proper subsets of Y and therefore do not belong to Σ. Either is thus a finite union of closed irreducible subsets, and consequently the same is true for their union Y. We have a contradiction, and Σ must be empty.

As to uniqueness, assume that we have a counterexample; that is, two irredundant decomposition such that $Y_1 \cup \ldots \cup Y_r = Z_1 \cup \ldots \cup Z_s$ and such that one of the Y_i's, say Y_1, does not equal any of the Z_k's.

Since Y_1 is irreducible and $Y_1 = \bigcup_k (Z_k \cap Y_1)$, it follows that $Y_1 \subseteq Z_k$ for some k. A similarly argument gives $Z_k = \bigcup_i (Z_k \cap Y_i)$ and Z_k being irreducible, it holds that $Z_k \subseteq Y_i$ for some i, and therefore $Y_1 \subseteq Z_k \subseteq Y_i$. By irredundancy we infer that $Y_1 = Y_i$, and hence $Y_1 = Z_k$. Contradiction. ❑

You should already have noticed the resemblance of the condition to be Noetherian for topological spaces and rings—both are chain conditions—and of course that is where the name Noetherian spaces comes from. When X is a closed algebraic set in $\mathbb{A}^n$ the one-to-one correspondence between the prime ideals in the coordinate ring $A(X)$ and the set of closed irreducible sets in X, yields that X is a Noetherian space; indeed, Hilbert's basis theorem implies that $A(X)$ is a Noetherian ring, so any ascending chain $\{I(X_i)\}$ of prime ideals corresponding to a descending chain of $\{X_i\}$ of closed irreducibles, is stationary. We have

There are examples of non-noetherian rings with just one maximal ideal, so an ascending chain condition on prime ideals does not imply that the ring is Noetherian. However, by a theorem of I.S. Cohen, a ring is Noetherian if all prime ideals are finitely generated.

Proposition 2.5 *If X is a closed algebraic subset of $\mathbb{A}^n$, then X is a Noetherian space.*

Hypersurfaces once more and some examples

It is often difficult to prove that an algebraic set X is irreducible, or equivalently that the ideal $I(X)$ is a prime ideal. This can be challenging even when X is a hypersurface.

Generally, to find the primary decomposition of an ideal a difficult. In additions to the problems of finding the minimal primes and the corresponding primary components, which frequently can be attacked by geometric methods, one has the notorious problem of embedded components. They are annoyingly well hidden from geometry

If $X = Z(f)$ is a hypersurface in $\mathbb{A}^n$, there will be no embedded components since the polynomial ring is a UFD. Indeed, one easily sees that $(f) \cap (g) = (fg)$ for polynomial without common factors. Hence one infers by induction that

$$(f) = (f_1^{a_1}) \cap \ldots \cap (f_r^{ar}),$$

where $f = f_1^{a_1} \cdot \ldots \cdot f_r^{a_r}$ is the factorization of f into irreducibles, and observes there are no inclusions among the prime ideals (f_i).

There is a vast generalization of this. A very nice class of rings are formed by the so called Cohen-Macaulay rings. If the coordinate ring $A(X)$ is Cohen Macaulay, the ideal $I(X)$ has no imbedded components. This is a part of the Macaulay's unmixed theorem—which even says that all the components of $I(X)$ have the same dimension.

Example 2.4 — Homogeneous polynomials Recall that a polynomial f is *homogenous* if all the monomials that appear (with a non-zero coefficient) in f are of the same total degree. By recollecting terms of the same total degree, one sees that any polynomial can be written as a sum $f = \sum_i f_i$ where f_i's is homogeneous of degree i; and since homogeneous polynomials of different total degrees are linearly independent, such a decomposition is unique.

Homogeneous polynomials

If a *homogeneous* polynomial f factors as a product $f = a \cdot b$, then polynomials a and b are also *homogeneous*. (Sometimes this can make life easier if you want *e.g.*, to factor f or to show that f is irreducible.) Indeed, if $a = \sum_{0 \leq i \leq d} a_i$ and $b = \sum_{0 \leq j \leq e} b_j$ with a_i's and b_j's homogeneous of degree i and j respectively and with $a_d \neq 0$ and $b_e \neq 0$, one finds

$$f = ab = \sum_{i+j<d+e} a_i b_j + a_d b_e$$

Since the decomposition of f in homogeneous parts is unique, it follows that $f = a_e b_d$. ☆

Example 2.5 The polynomial $f(x) = x_1^2 + x_2^2 + \ldots + x_n^2$ is irreducible when $n \geq 3$ and the characteristic of k is not equals to two. To check this, we can assume $n = 3$. Suppose there is a factorization like

QuadraticForms

$$x_1^2 + x_2^2 + x_3^2 = (a_1x_1 + a_2x_2 + a_3x_3)(b_1x_1 + b_2x_2 + b_3x_3).$$

Observing that $a_1 \cdot b_1 = 1$ and replacing a_i by a_1/a_1 and b_i by b_i/b_1, one can assume that $a_1 = b_1 = 1$; that is the equation takes the shape

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + a_2x_2 + a_3x_3)(x_1 + b_2x_2 + b_3x_3).$$

Putting $x_3 = 0$, and using the factorization $x_1^2 + x_2^2 = (x_1 + ix_2)((x_1 - ix_2)$, one easily brings the equation on the form

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + ix_2 + a_3x_3)(x_1 - ix_2 + b_3x_3),$$

from which one obtains $a_3 = b_3$ and $a_3 = -b_3$. If the characteristic is not equal to two, this is a contradiction. ☆

Example 2.6 — Monomial ideals An ideal $\mathfrak{a}$ is said to be *monomial* if it is generated by monomials. Such that an ideal has the property that if a polynomial f belongs to $\mathfrak{a}$, all the monomials appearing in f belong to $\mathfrak{a}$ as well. One To verify this one writes f as a sum $f = \sum M_i$ of monomial terms[2] and let $\{N_j\}$ be monomial generators for $\mathfrak{a}$. Then one infers that

Monomial ideals

[2] A *monomial term* is of the form $\alpha \cdot M$ where α is a scalar and M a monomial.

$$f = \sum_i M_i = \sum_j P_j N_j = \sum_{j,k} A_{kj} N_j$$

where P_j are polynomials whose expansions in monomial terms are $P_j = \sum_k A_{kj}$. Since different monomials are linearly independent (by definition of polynomials), every term M_i is a linear combination of the monomial terms $A_{kj}N_j$ corresponding to the same monomial, and hence lies in the ideal $\mathfrak{a}$. ☆

Example 2.7 Monomial ideals are much easier to work with than general ideals. As an easy example, consider the union of the three coordinate axes in $\mathbb{A}^3$. It is given as the zero locus of the ideal $\mathfrak{a} = (xy, xz, yz)$, and one has

$$(xy, xz, yz) = (x, y) \cap (x, z) \cap (z, w)$$

Indeed, one inclusion is trivial; for the other it suffices to show that a monomial in $\mathfrak{b} = (x, y) \cap (x, z) \cap (y, z)$ belongs to (xy, xz, yz). But $x^n y^m z^l$ lies in $\mathfrak{b}$ precisely when at least two of the three integers n, m and l are non-zero, which as well is the requirement to lie in $\mathfrak{a}$. ☆

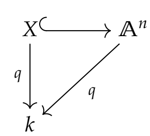
Polynomial maps between algebraic sets

The final topic we approach in these Notes2 are the so called *polynomial maps* between closed algebraic sets. This anticipates the introduction of "morphisms" between general varieties in the next section, but we still find it worth while doing. Polynomial maps between algebraic sets are conceptually much simpler than morphisms, and in concrete cases one works with polynomials. In the end, the two concepts of polynomial maps and morphisms between closed algebraic sets turn out to coincide.

The coordinate ring

Polynomial functions

Let $X \subseteq \mathbb{A}^n$ be a closed algebraic set. A *polynomial function* (later on they will also be called *regular functions*) on X is just the restriction to X of a polynomial on $\mathbb{A}^n$; that is, it is a polynomial $q \in k[x_1, \dots, x_n]$ regarded as a function on X. Two polynomials p and q restrict to the same function precisely when the difference $p - q$ vanishes on X; that is to say, the difference $p - q$ belongs to the ideal $I(X)$. We infer that the polynomial functions on X are exactly the elements in the coordinate ring $A(X) = k[x_1, \dots, x_n]/I(X)$.



Polynomial maps

Now, given another closed algebraic subset $Y \subseteq \mathbb{A}^n$ and a map $\phi\colon X \to Y$. Composing ϕ with the inclusion of Y in $\mathbb{A}^m$, we may consider ϕ as a map from X to $\mathbb{A}^m$ that takes values in Y; and as such, it has m component functions $q_1, \dots, q_m$. We say that ϕ is a *polynomial*

Polynomial maps

map if these components are polynomial functions on X. The set of polynomial maps from X to Y will be denoted by $\text{Hom}_{\mathsf{Aff}}(X, Y)$.

EXAMPLE 2.8 We have already seen several examples. For instance, the parametrization of a rational normal curve C_n is a polynomial map from $\mathbb{A}^1$ to C_n whose component functions are the powers t^i. ☆

Proposition 2.6 *Polynomial maps are Zariski continuous.*

PROOF: Assume that $\phi\colon X \to Y$ is the polynomial map. Let $Z(\mathfrak{a})$ be a closed subset of Y. Given a polynomial q form $\mathfrak{a}$. Clearly $\phi \circ q$ is a polynomial function on X, and hence $\phi^{-1}(Z(q)) = Z(\phi \circ q)$ is closed in X, and consequently for any closed set $Z(q_1, \ldots, q_m)$ we find $\phi^{-1}Z(q_1, \ldots, q_r) = \bigcap_i \phi^{-1}Z(q_i)$ is closed. ❑

Examples

We finish this lecture by a few example of diverse themes. One example to warn that images of polynomial maps can be complicated, followed by two examples to illustrate that important and interesting subsets naturally originating in linear algebra can be irreducible algebraic sets.

EXAMPLE 2.9 — DETERMINANTAL VARIETIES Determinantal varieties are as the name indicates, closed algebraic sets defined by determinants. They are much studied and play a prominent role in mathematics. In this example we study one particular instance of the species.

The space $\mathbb{M}_{2,3} = \text{Hom}_k(k^3, k^2)$ of 2×3-matrices may be consider the space $\mathbb{A}^6$ with the coordinates indexed like the entries of a matrix; that is, the points are like

$$\begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \end{pmatrix}.$$

We are interested in the subspace W of matrices of rank at most one. For a 2×3-matrix to be of rank at most one is equivalent to vanishing of the maximal minors (in the present case there are three[3] maximal minors and they all quadrics). This shows that W is a closed algebraic set.

[3] The three are $x_{11}x_{22} - x_{12}x_{21}$, $x_{11}x_{23} - x_{13}x_{21}$, $x_{12}x_{23} - x_{13}x_{22}$

To see it is irreducible we express W as the image of an affine space under a polynomial map. Indeed, any matrix of rank at most one, can be factored as

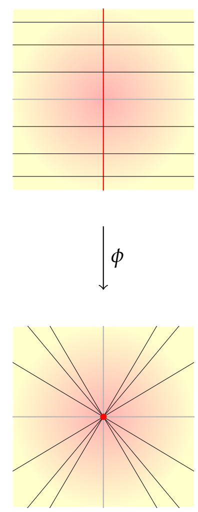
$$a = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} (b_1, b_2, b_3).$$

So W is the image of $\mathbb{A}^2 \times \mathbb{A}^3$ under the map—which clearly is polynomial—that sends the tuple $(a_1, a_2; b_1, b_2, b_3)$ to the matrix $(a_i b_j)$. ☆

PROBLEM 2.2 Show that rank one maps can be factored as in the example above. HINT: The linear map corresponding to the matrix has image of dimension one and can be factored as $k^3 \xrightarrow{\alpha} k \xrightarrow{\iota} k^2$ ★

BildetStygt

EXAMPLE 2.10 Images of polynomial maps can be complicated. In general they are neither closed nor open. For example, consider the map $\phi\colon \mathbb{A}^2 \to \mathbb{A}^2$ given as $\phi(u,v) = (u, uv)$. Pick a point (x,y) in $\mathbb{A}^2$. If $x \neq 0$, it holds that $\phi(x, x^{-1}y) = (x,y)$ so points lying off the y-axis are in the image. Among points with $x = 0$ however, only the origin belongs to the image. Hence the image is equal to the union $\mathbb{A}^2 \setminus Z(x) \cup \{(0,0)\}$. This set is neither closed (it contains an open set and is therefore dense) nor open (the complement equals $Z(x) \setminus \{(0,0)\}$ which is dense in the closed set $Z(x)$, hence not closed).



The map ϕ collapses the v-axis to the origin, and consequently lines parallel to the u-axis are map to lines through the origin; the intersection point with the v-axis is mapped to the origin. Pushing these lines out towards infinity, their images approach the v-axis. So in some sense, the "lacking line" that should have covered the v axis, is the "line at infinity". ☆

NyOppgave

PROBLEM 2.3 Let ϕ be the map in example 2.10. Show that ϕ maps lines parallel to the u-axis (that is, those with equation $v = c$) to lines through the origin. Show that lines through the origin (those having equation $v = cu$) are mapped to parabolas. ★

PROBLEM 2.4 Describe the image of the map $\phi\colon \mathbb{A}^3 \to \mathbb{A}^3$ given as $\phi(u,v,w) = (u, uv, uvw)$. ★

QuadForms

Quadratic forms

EXAMPLE 2.11 — QUADRATIC FORMS Recall that a *quadratic form* is a homogeneous polynomial of degree two. That is, one that is shaped like $P(x) = \sum_{i,j} a_{ij} x_i x_j$ where both i and j run from 1 to n. In that sum $a_{ij}x_i x_j$ and $a_{ji} x_j x_i$ appear as separate terms, but as a matter of notation, one organizes the sum so that $a_{ij} = a_{ji}$. Coalescing the terms $a_{ij}x_i x_j$ and $a_{ji}x_j x_i$, the coefficient in front of $x_i x_j$ becomes equal to $2a_{ij}$. For instance, when $n = 2$, a quadratic form is shaped like

$$P(x) = a_{11}x_1^2 + 2a_{12}x_1 x_2 + a_{22}^2 x_2^2.$$

The *coefficient matrix* of the form is the symmetric matrix $A = (a_{ij})$. Then one can express $P(x)$ as the matrix product

$$P(x) = xAx^t$$

where $x = (x_1, \ldots, x_n)$.

The set of such forms—or of such matrices—constitute a linear space which we shall denote by S_n. It has a basis x_i^2 and $2x_ix_j$ so in our language S_n is isomorphic to an affine space $\mathbb{A}^N$ whose dimension N equals the number of distinct monomials x_ix_j; that is $N = n(n+1)/2$. The coordinates with respect to the basis described above, are denoted by a_{ij}.

We are interested in the subspaces $W_r \subseteq \mathbb{A}^N$ where the rank of A is as most r. They form a descending chain; that is $W_{r-1} \subseteq W_r$; and clearly $W_n = \mathbb{A}^N$ and $W_0 = \{0\}$.

The W_r's are all closed algebraic subsets, and the aim of this example is to show they are irreducible:

Proposition 2.7 *The subsets W_r are closed irreducible algebraic subset of $\mathbb{A}^N$.*

PROOF: That the W_r's are closed, hinges on the fact that a matrix is of rank at most r if and only if all its $(r+1) \times (r+1)$-minors vanish.

To see that the W_r's are irreducible, we shall use a common technique. Every matrix in W_r can be expressed in terms of a "standard matrix" in a a continuous manner.

By the classical Gram-Schmidt process, any symmetric matrix can be diagonalized. There is a relation

$$BAB^t = D$$

where B is an invertible matrix and where D is a diagonal matrix of a special form. If the rank of A is r, the first r diagonal elements of D are 1's and the rest are 0's. Introducing $C = B^{-1}$, we obtain the relation

$$A = CDC^t.$$

Allowing C to be any $n \times n$-matrix, not merely an invertible one, one obtains in this way all matrices A of rank at most r.

Rendering the above considerations into geometry, we introduce a parametrization of the locus W_r of quadrics of rank at most r. It is not a one-to-one map as several parameter values correspond to the same point, but it is a polynomial map and serves our purpose to prove that W_r is irreducible. We define a map

$$\Phi\colon \mathbb{M}_{n,n} \to \mathbb{A}^N$$

but letting it send an $n \times n$-matrix C to CDC^t. The map Φ is a polynomial map because the entries of a product of two matrices are expressed by polynomials in the entries of the factors, and by the Gram-Schmidt process described above, its image equals W_r. Hence W_r is irreducible. ❑

Giuseppe Veronese (1854–1917)
Italian mathematician

To GET A BETTER UNDERSTANDING of how forms of rank r are shaped, one introduces new coordinates by the relations $yB = x$, which is legitimate since B and therefore B^t is invertible. Then $xAx^t = yB^tAB^ty^t = yDy^t$. So, in view of the shape of D, expressed in the new coordinates the quadratic form $P(x)$ has the form:

$$P(y) = y_1^2 + \ldots + y_r^2.$$

OF SPECIAL INTEREST are the sets W_1 of rank one quadrics. By what we just saw, these quadrics are all squares of a linear form in the variables x_i's (remember that y_1 is a linear form in the original coordinates, the x_i's); that is, one has an expression

$$P(x) = (\sum_i u_i x_i)^2 = \sum_i u_i^2 x_i^2 + \sum_{i<j} 2u_i u_j x_i x_j.$$

This gives us another parametrization of W_1, namely the one sending a linear form to its square. The linear forms constitute a vector space of dimension n (one coefficient for each variable), so "the square" is map

$$\nu\colon \mathbb{A}^n \to \mathbb{A}^N \tag{1}$$

sending $(u_1, \ldots, u_n)$ to the point whose coordinates are all different products $u_i u_j$ with $i \leq j$ (remember we use the basis for the space of quadrics made up of the squares x_i^2 and the cross terms $2x_i x_j$, in some order). When $n = 3$ we get a mapping of $\mathbb{A}^3$ into $\mathbb{A}^6$ whose image is called the *cone over the Veronese surface*.

The *Veronese surface* is famous *projective* surface living in the projective space $\mathbb{P}^5$ (we shall study these spaces closely in subsequent lectures). The real points of the Veronese surface be can realized in $\mathbb{R}^3$, at least if one allows the surface to have self intersections. The surface depicted in the margin is parametrized by three out of the six quadratic terms in the parametrization (1) above, and is the image of the unit sphere in $\mathbb{R}^3$ under the map $(x, y, z) \mapsto (xy, xz, yz)$. This specific real surface is often called the *Steiner surface* after the Swiss mathematician Jacob Steiner who was the first to describe it , but it also goes under the name the *Roman surface* since Steiner was in Rome when he discovered this surface. ☆

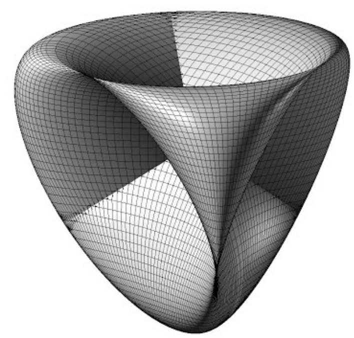


Figure 3: The Roman surface—a projection of a real Veronese surface

PROBLEM 2.5 Show that the map v above in (1) is not injective, but satisfies $\nu(-x) = \nu(x)$. Show that if $\nu(x) = \nu(y)$, then either $y = x$ or $y = -x$. ★

Vero

Problems

2.6 Show that an irreducible space is Hausdorff if and only if it is reduced to single point.

2.7 Endow the natural numbers $\mathbb{N}$ with the topology whose closed sets apart from $\mathbb{N}$ itself are the finite sets. Show that $\mathbb{N}$ with this topology is irreducible. What is the dimension?

2.8 Show that any infinite countable subset of $\mathbb{A}^1$ is Zariski-dense.

2.9 Let X be an infinite set and $Z_1, \ldots Z_r \subsetneq X$ be proper infinite subsets of X such any two of them intersect in at most a finite set. Let $\mathcal{T}$ be the set of subsets of X that are either finite, the union of some of the Z_i's and a finite set, the empty set or the entire set X. Show that $\mathcal{T}$ is the set of closed sets for a topology on X. When is it irreducible?

2.10 Let $X \subseteq \mathbb{A}^3$ be the union of the three coordinate axes. Determine the ideal $I(X)$ by giving generators. Describe the Zariski topology on X.

2.11 Let $\mathfrak{a}$ be the ideal $\mathfrak{a} = (xz, xw, zy, wy)$ in the polynomial ring $k[x, y, z, w]$. Describe geometrically the algebraic set $W = Z(\mathfrak{a})$ in $\mathbb{A}^4$, and show that the primary decomposition of $\mathfrak{a}$ is ToPlan

$$\mathfrak{a} = (x, y) \cap (z, w).$$

2.12 Continuing the previous exercise, let $\mathfrak{b}$ be the ideal $\mathfrak{b} = (w - \alpha y)$ with α a non-zero element in k, and let $X = Z(\mathfrak{b})$. Describe geometrically the intersection $W \cap X$. Show that the image $\mathfrak{c}$ of the ideal $\mathfrak{a} + \mathfrak{b}$ in $k[x, y, z]$ under the map that sends w to αy is given as ToPlan2

$$\mathfrak{c} = (xz, xy, zy, y^2),$$

and determine a primary decomposition of $\mathfrak{c}$. What happens if $\alpha = 0$?

2.13 Let two quadratic polynomials f and g in $k[x, y, z, w]$ be given as $f = xz - wy$ and $g = xw - zy$. Describe geometrically the algebraic subset $Z(f, g)$ and find a primary decomposition of the ideal (f, g).

2.14 Let $f = y^2 - x(x-1)(x-2)$ and $g = y^2 + (x-1)^2 - 1$. Show that $Z(f, g) = \{(0, 0), (2, 0)\}$. Determine the primary decomposition of (f, g).

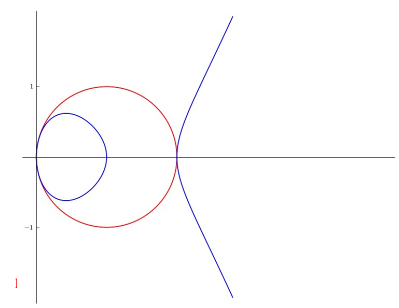


Figure 4: The curves in problem 2.14.

2.15 Let $\mathfrak{a}$ be the ideal $(wy - x^2, wz - xy)$ in $k[x, y, z, w]$. Show that the primary decomposition of $\mathfrak{a}$ is

$$\mathfrak{a} = (w, x) \cap (wz - xy, wy - x^2, y^2 - zx).$$

2.16 Let $\mathfrak{a} = (wz - xy, wy - x^2, y^2 - zx)$. Show that $Z(\mathfrak{a})$ is irreducible and determine $I(X)$.

2.17 Show that any reduced[4] algebra of finite type over k is the coordinate ring of a closed algebraic set.

RedRinsClSets

[4] Reduced means that there are no non-zero nilpotent elements.

2.18 Show that any integral domain finitely generated over k is the coordinate ring of an irreducible closed algebraic set.

2.19 Show that the multiplication map $\mathbb{M}_{n.m} \times \mathbb{M}_{m,k} \to M_{n,k}$ is a polynomial map.

2.20 Let W_r be the subset of $\mathrm{Hom}_k(k^n, k^m) = \mathbb{M}_{n,m} = \mathbb{A}^{nm}$ of maps of rank at most r. Show that W_r is irreducible.

★