Chapter 1 - Affine Varieties

1.1 Algebraic sets and the Zariski topology

Affine n-space $\mathbb{A}^n = \{(a_1, \dots, a_n) : a_i \in k\}$

$$k[x_1, \dots, x_n] = \{\text{polynomials in the } x_i\}$$
$$= \Big\{ \sum_I a_I x^I : a_I \in k \Big\}$$

$I = (i_1, \dots, i_n) \quad i_j \geq 0 \ \forall j$

For $S \subseteq k[x_1, \dots, x_n]$:
$$Z(S) = \{P \in \mathbb{A}^n : f(P) = 0 \ \forall f \in S\}$$

"zero set"

Any such $Z(S)$ is an algebraic set. or affine alg. variety

First Examples

① $\mathbb{A}^n = Z(0)$

② $\phi = Z(1)$

③ $(a_1, \dots, a_n) = Z(x_1 - a_1, \dots, x_n - a_n)$

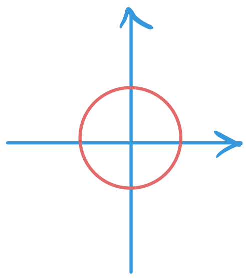
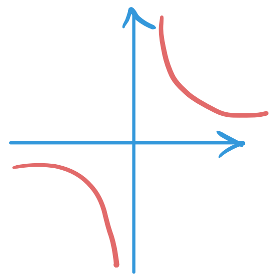
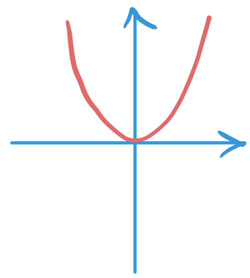
④ Linear subspaces

More Examples

⑤ Conics in the plane: $Z(f)$

$$f(x,y) = ax^2 + bxy + cy^2 + dx + ey + f$$

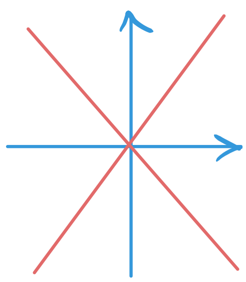
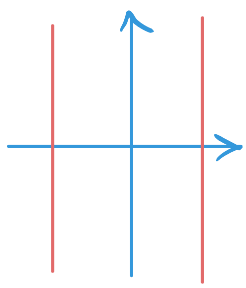
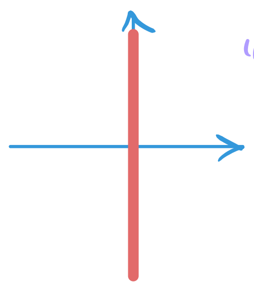
e.g. $x^2 - y^2 - 1$ $\quad$ $xy - 1$ $\quad$ $y - x^2$

actually connected in $\mathbb{C}^2$
(why?)

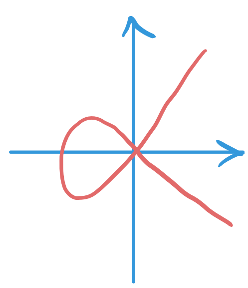
& some degenerate examples

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

"double line"

⑥ Nodal cubic



⑦ Fermat curve $Z(x^n+y^n-z^n)$

$k=\mathbb{C}$ easy, $k=\mathbb{Q}$ hard!

⑧ Algebraic groups, e.g. $SL_n(k)=Z(\det -1)$

⑨ Degree d hypersurfaces in $\mathbb{A}^n$: $Z(f)$, $\deg f = d$.

Non-examples

① Fact. Every affine variety is closed in Euclidean topology

$\Rightarrow \{z : |z|<1\}$ is not an affine variety.

② Fact. The interior of any (proper) algebraic set is empty

Pf. A holomorphic fn is determined by its restriction to any open set.

$\Rightarrow \{z : |z| \le 1\}$ is not an affine variety

③ Fact. Any subvariety of $\mathbb{A}^1$ is finite.

Pf. Fund. thm. alg.

$\Rightarrow \mathbb{Z}$ is not an affine variety.

HILBERT BASIS THM

Thm. Every alg. set is defined by finitely many polynomials.

Recall for R a ring, an ideal $I \subseteq R$ is a subgp with "absorption"

e.g. $\{ f \in k[x] : \text{const. term} = 0 \} \subseteq k[x]$

The ideal generated by $S \subseteq R$ is

$$(S) = \{ s_1 r_1 + \cdots + s_m r_m : s_i \in S, r_i \in R \}$$

or smallest ideal containing S.

Exercise. $Z(S) = Z((S))$.

Lemma/Defn. R a ring. TFAE

1. Every ideal in R is finitely generated
2. R satisfies the ascending chain condition: every infinite ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ is eventually stationary.

Say R is Noetherian.

Fact. Fields are Noetherian (only ideals are 0 & k)

Pf. ① $\Rightarrow$ ② Let $I_1 \subseteq I_2 \subseteq \cdots$

$\rightsquigarrow I = \bigcup I_i$ is an ideal. ① $\Rightarrow$ f.g.

$\Rightarrow$ some $I_j =$

② $\Rightarrow$ ① If I not fin. gen, can choose in I

$(f_1) \subset (f_1, f_2) \subset (f_1, f_2, f_3) \subset \cdots$ $\square$

Prop. R Noetherian $\Rightarrow$ $R[x_1, \dots, x_n]$ Noetherian.

Pf. First for $R[x]$. General case follows by induction.

Say $I \subseteq R[x]$ not fin. gen.

Let f_0 = non-0 elt of I of min. deg.

f_{i+1} = non-0 elt of $I \setminus (f_1, \dots, f_i)$ J_i

Note: $\deg f_i \leq \deg f_{i+1}$

a_i = leading coeff. of f_i.

$I_i = (a_0, \dots, a_i) \subseteq R$

Noetherian $\Rightarrow$ $I_0 \subseteq I_1 \subseteq \cdots$ event. stationary

$\Rightarrow \exists\, m$ s.t. $a_{m+1} \in (a_0, \dots, a_m)$

$\Rightarrow a_{m+1} = \sum r_i a_i \quad r_i \in R$

Write $f = f_{m+1} - \sum_{i=0}^{m} x^{\deg f_{m+1} - \deg f_i} r_i f_i$

f is cooked up so $\deg f < \deg f_{m+1}$

$\Rightarrow f \in J_m \Rightarrow f_{m+1} \in J_m$ (by above equality)

Contradiction. $\square$

Pf. of Thm.

Consider a $Z(S)$.

By Exercise can assume $S = I =$ ideal.

By Exercise suffices to show I f.g.

Apply Prop. and Fact. $\square$

THE ZARISKI TOPOLOGY

Goal: Define a topology on varieties.

A topology on a space X is a collection of subsets, called open sets.
A closed set is the complement of an open set.
With a topology, can define limits, continuous maps.

The closed sets must satisfy:
(i) $\emptyset, X$ closed
(ii) Finite unions of closed sets are closed.
(iii) Arbitrary intersections of closed sets are closed.

Defn. The Zariski topology on $\mathbb{A}^n$ is the one whose closed sets are the $Z(S)$.

Prop. This really is a topology.

Pf. (i) ✓

(ii) $\bigcup_{i=1}^{n} Z(S_i) = Z(\prod S_i)$

(iii) $\bigcap_{A} Z(S_\alpha) = Z(\bigcup S_\alpha)$ $\square$

For $Y \subseteq X$ the subspace topology on Y has a closed set $C \cap Y$ for each closed $C \subseteq X$.
So: points are close in Y iff close in X.

$\rightsquigarrow$ Zariski topology on any $Z(S)$.

Fact. The closed sets in $Z(S)$ are the $Z(S')$ with $Z(S') \subseteq Z(S)$.

The Zariski topology is messed up:

(i) all proper closed subsets of $\mathbb{A}^n$ have empty interior

(ii) proper closed subsets of $\mathbb{A}^1$ are the finite sets

(iii) no two Zariski open sets are disjoint.

(i) $\Rightarrow$ every Zariski open set is dense in Eucl. top.
Also: every Zariski open set is dense in Zar. top.

(ii) $\Rightarrow$ all bijections $\mathbb{A}^1 \to \mathbb{A}^1$ are continuous.
(so we don't want to define morphisms to be all continuous maps!)

(ii) $\Rightarrow$ (n) converges to every pt in $\mathbb{A}^1$.

(iii) $\Rightarrow$ Zariski top. is not Hausdorff.

Fact. compact $\not\Rightarrow$ closed   Smith says this. Example?

Example The proper Z-closed subsets of $Z(y-x^2)$ are the finite sets   or any irred. plane curve

Why? Consider $Z(f(x,y)) \cap Z(y-x^2)$
$$= Z(f(x,y),\, y-x^2)$$
$$\longleftrightarrow Z(f(x,x^2)) \subseteq \mathbb{A}^1.$$

The closure of $A \subseteq X$ is the smallest closed set in X containing A. Write $\bar{A}$

Fact. The Zariski closure of $Y \subseteq \mathbb{A}^n$ is $Z(\{f : f(Y)=0\})$ easy

Example. $Y \subseteq \mathbb{A}^1$ infinite $\Rightarrow \bar{Y} = \mathbb{A}^1$.

Fact. Zariski closure = Euclidean closure for Zariski open sets.   exercise

Example. $X = Z(xy) \subseteq \mathbb{C}^2$
$U = \mathbb{C}^2 \setminus Z(x)$
$X \cap U$ = Zariski open in X.

A set in X is <u>dense</u> if all open sets intersect it.

Equivalently, the closure of the set is X.

<u>Example.</u> $\{\mathbb{Q}\text{-points}\}$ is dense in $\mathbb{A}^n$

$\mathbb{Z}$ dense in $\mathbb{A}^1$

Exercise. Are $\mathbb{Z}$-pts dense in $\mathbb{A}^n$?

<u>Fact.</u> Say $f \in k[x_1, \dots, x_n]$, $f|_A \equiv 0$ where A is Zariski dense in $\mathbb{A}^n$. Then $f \equiv 0$.

This is in some sense the point of the Z-topology.

<u>Pf.</u> $Z(f)$ is a closed set containing A

$\Rightarrow Z(f) = \mathbb{A}^n$. $\square$

See also Milne Prop 2.26:

- Every ascending chain of open subsets of V is eventually constant ($\Longleftrightarrow$ every descending chain of closed subsets is eventually constant).
- Closed $\Rightarrow$ compact

Hilbert's Nullstullensatz

Already have: $\{\text{ideals in } k[x_1,\dots,x_n]\} \longrightarrow$ affine alg. var.'s

$$I \longmapsto Z(I)$$

Also have: affine alg var.'s $\longrightarrow \{\text{ideals in } k[x_1,\dots,x_n]\}$

$$V \longrightarrow I(V) = \{f : f|_V = 0\}$$

To what extent are these inverses?
The first map is not injective: $Z(x_1) = Z(x_1^2)$.
This is essentially the only problem.

Weak Nullstullensatz. Let k be alg. closed. Every maximal ideal in $k[x_1,\dots,x_n]$ is of the form $(x_1-a_1,\dots,x_n-a_n)$.

Strong Nullstullensatz. Let k be alg. closed, $I \subseteq k[x_1,\dots,x_n]$ an ideal. Then

$$I(Z(I)) = \sqrt{I}$$

$\{f : f \text{ has a power in } I\}$

Hilbert 1900

The WN implies other natural statements:

- Every proper ideal in $k[x_1,\dots,x_n]$ has a common zero.
- Conversely: a family of polynomials with no common zeros generates the unit ideal.

The SN is a mult-dim version of fund. thm. alg.

First note: • $\mathbb{C}[z]$ is a P.I.D. (follows from our pf of Hilbert basis thm)

• $(f) \in \mathbb{C}[z]$ radical $\iff$ f has no repeated roots.

To see the latter, note $(f) = \{f \cdot p\}$

• FTA has equivalent formulations:

(i) each $f \in \mathbb{C}[z]$ of $\deg \geq 1$ has a root

(ii) each $f \in \mathbb{C}[z]$ of $\deg \geq 1$ factors into linears

First observe: $I(Z(f)) = \sqrt{(f)} \implies f$ has a root.

Indeed $Z(f) = \phi \implies I(Z(f)) = \mathbb{C}[z] \neq \sqrt{(f)}$ (to see the $\neq$, note $1^k \notin (f)$ $\forall k$.

Now observe: f factors into linears $\implies I(Z(f)) = \sqrt{(f)}$

Clear for f with no repeated roots. If f is, say, $f(z) = (x-1)(x-3)^2$ then

$$I(Z(f)) = I(\{1,3\}) = ((z-1)(z-3)) = \sqrt{(f)}.$$

Note FTA is not a consequence of SN since SN assumes k is alg. closed.

SN gives an order-reversing bijection:

$$\boxed{\left\{\begin{matrix}\text{Affine alg.}\\ \text{vars in } \mathbb{A}^n\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{radical ideals}\\ \text{in } k[x_1,\dots,x_n]\end{matrix}\right\}.}$$

Some of the inclusions are easy:

(i) $X \subseteq Z(I(X))$ is obvious

(ii) $\sqrt{I} \subseteq I(Z(I))$ is obvious

(iii) To see $Z(I(X)) \subseteq X$ note $X = Z(I)$ some I

$\rightsquigarrow Z(I(X)) = Z(I(Z(I)))$

(ii) $\Rightarrow I \subseteq \sqrt{I} \subseteq I(Z(I))$

$\Rightarrow Z(I(Z(I))) \subseteq Z(I) = X$ ✓

(iv) is SN.

Despite the names, we have WN $\Leftrightarrow$ SN. *More to the point*, we can derive either one from the other.

Both results fail for k not alg. closed.

e.g. (x^2+1) is radical in $\mathbb{R}[x]$ since $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ and $\mathbb{C}$ has no 0-divisors.

But $I(Z(x^2+1)) = I(\emptyset) = \mathbb{R}[x]$

SN $\Rightarrow$ if $g \in I(Z(I))$ then $g^N \in I$. What is N?

Kollár 1988: if $I = (f_1,\dots,f_r)$ f_i homogeneous, $\deg f_i > 2$ then $N \leq \prod \deg f_i$. If $r < n$, this is sharp.

Zariski's Proof, Following Allcock

Thm. k = field, K = extension
If K is fin. gen. as a k-algebra then
K is algebraic over k.

For A a k-alg, we say $X \subseteq A$ is a gen. set if
each elt of A is a polynomial in X with coeffs in k.

We say K is algebraic over k if each elt of K is
a root of a polynomial with coeffs in k.
e.g. $\mathbb{C}$ is algebraic over $\mathbb{R}$
$\mathbb{R}$ is not algebraic over $\mathbb{Q}$.

Pf of WN. Say m = max ideal in $R = k[x_1, \ldots, x_n]$
$\Rightarrow R/m$ a field, fin. gen as a k-alg (since R is).
Have $k \cap m = \{0\}$ (else $m = R$)
$\Rightarrow$ image $\bar{k}$ of k is isomorphic to k.
Thm $\Rightarrow R/m$ = alg. ext. of $\bar{k}$
k alg closed $\Rightarrow R/m = \bar{k}$
image of a_i
Under $R \to R/m$, each $x_i \mapsto \bar{a}_i \in \bar{k}$.
$\Rightarrow m \supseteq (x_1 - a_1, \ldots, x_n - a_n) \leftarrow$ call this m'
But m' is maximal* $\Rightarrow m' = m$ $\square$

* Proof that m' is maximal: The maps

$$R/m' \longrightarrow k \qquad\qquad k \longrightarrow R/m'$$
$$f \longmapsto f(a_1,\dots,a_n) \qquad\qquad 1 \longmapsto 1$$

are (well-defined) inverse ring homs.
k a field $\Rightarrow$ m' maximal. $\square$

Pf of SN. The "trick of Rabinowitz," due to George Yuri Rainich (né Rabinowitsch) 1929
Wikipedia: It was part of the Rainich folklore that he could read anything published in Europe.

Restatement: Say $g \in I(Z(f_1,\dots,f_m))$.
So a common zero of the f_i is a zero of g.
Thus $f_1,\dots,f_m,\ x_{n+1}g-1$ have no common zeros in $\mathbb{A}^{n+1}$
WN $\Rightarrow$ can write
$$1 = p_1f_1 + \cdots + p_mf_m + p_{m+1}(x_{n+1}g-1)$$
where $p_i \in k[x_1,\dots,x_{n+1}]$
Apply the map $k[x_1,\dots,x_{n+1}] \longrightarrow k(x_1,\dots,x_n)$
$$x_{n+1} \longmapsto 1/g$$
$\rightsquigarrow$ $1 = p_1(x_1,\dots,x_n,\tfrac{1}{g})f_1 + \cdots + p_m(x_1,\dots,x_n,\tfrac{1}{g})f_m$
Clear denominators. $\square$

Pf of Thm (special case). Say k infinite, K is the simple transcendental extension $K = k(x)$.
Let $f_1, \dots, f_m \in K$, $A = k$-alg gen by f_i.
WTS $A \subsetneq K$.
Choose $c \in k$ away from the poles of the f_i.
No elt of A has a pole at c.
$\Rightarrow \frac{1}{x-c} \notin A$ $\square$

Pf of Thm. Assume K transcendental (not algebraic) over k.

Assume first K has transc. deg. 1, that is K contains a field (isomorphic to) $k(x)$ & K is alg. over $k(x)$.
Let $1 = f_0, f_1, \dots, f_m \in K$, $A = k$-alg. gen by the f_i. Want $A \subsetneq K$.
Finite generation of K as a k-alg $\Rightarrow$ K is a fin. dim vector space over $k(x)$*.
Let $e_1, \dots, e_n$ be a basis.
Write the mult. table for K:

$$e_i e_j = \sum_\ell \frac{a_{ij\ell}}{b_{ij\ell}} e_\ell \qquad a\text{'s}, b\text{'s} \in k[x]$$

Also write: $$f_i = \sum_j \frac{c_{ij}}{d_{ij}} e_j \qquad c\text{'s}, d\text{'s} \in k[x]$$

Any $a \in A$ is a k-linear combo of products of f_i.

Expand using the above formulas for f_i & $e_i e_j$

$\rightsquigarrow$ a is a k-linear combo of the e_i where each denominator is a product of b's & d's.

$\rightsquigarrow$ irreducible factors among the denominators are among the irred. factors of the b's & d's.

Choose some irred. poly p not among those factors.**

Then $1/p$ is not in A.

Now assume the transcendence deg is > 1.

Choose*** a subextension k' s.t. trans. deg of K over k' is 1.

Previous case: K is not fin. gen. as a k'-alg.

$\Rightarrow$ K is not fin. gen as a k-alg. $\square$

Finer points:

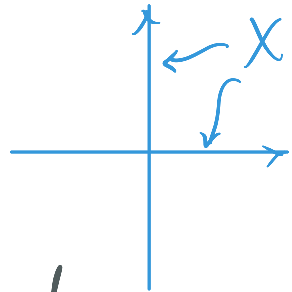
* $\exists\, a_1, \ldots, a_n$ s.t. each elt of K is a poly. in the a_i with coeffs in k. If the deg of a_i over k is d_i then only $a_i^1, \ldots, a_i^{d_i - 1}$ need in the polynomials...

** For k infinite, can use the ∞-many linears: $x - c$. Otherwise, mimic the proof of infinitude of primes.

*** A construction of k': choose k-alg gens $a_1, \ldots, a_n$ for K, let $k' = k(x_1, \ldots, x_{\ell-1})$ where x_ℓ is last x_i that is transcendental over the previous.

IRREDUCIBILITY

Basic example: $Z(x_1x_2) \subseteq \mathbb{A}^2$
$= Z(x_1) \cup Z(x_2)$



but $Z(x_i)$ cannot be further decomposed.

Defn. A top. space is <u>reducible</u> if it is the union of nonempty, proper closed subsets.

Defn. A top. space is <u>disconnected</u> if it is the union of nonempty, disjoint closed subsets

Note: disconnected $\Rightarrow$ reducible, or
irreducible $\Rightarrow$ connected.

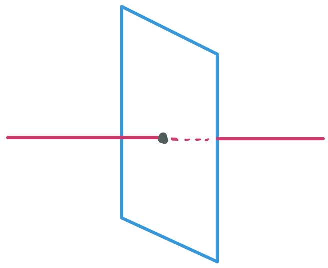
Disconnected means what you think it does.
Reducibility makes little sense for most spaces.

Fact. Hausdorff $\Rightarrow$ reducible

The maximal irreducible closed subsets of a space are the <u>irreducible components</u>. Will prove below that any $Z(I)$ decomposes into finitely many.

Examples. ① $Z(x_1x_2) \subseteq \mathbb{A}^2$ is reducible, connected.

② $Z(x_1x_2, x_1x_3) \subseteq \mathbb{A}^3$ is red, conn.



$= Z(x_1) \cup Z(x_2, x_3)$

③ $Z(x_1^2-1)$ is disconnected:

$= Z(x_1-1) \cup Z(x_1+1)$

④ A finite set in $\mathbb{A}^1$ is connected iff it has fewer than 2 elts.

⑤ $p \in \mathbb{A}^n$ is irreducible.

⑥ What about $\mathbb{A}^n$ itself?

Prop. $X = Z(I) \subseteq \mathbb{A}^n$ is irreducible iff $I(X)$ is prime.

Pf. ($\Leftarrow$) Say $I(X)$ prime & suppose $X = X_1 \cup X_2$

Then $I(X) = I(X_1) \cap I(X_2)$.

$\boxed{\text{If } P = I \cap J \text{ then } IJ \subseteq I \cap J \subseteq P \text{ so } I = P \text{ or } J = P}$

$I(X)$ prime $\Longrightarrow I(X) = I(X_1)$

Prime $\Longrightarrow$ radical and so SN $\Longrightarrow X = X_1$

($\Rightarrow$) Say X irred & $fg \in I(X)$.

Then $X \subseteq Z(fg) = Z(f) \cap Z(g)$

$\Longrightarrow X = (Z(f) \cap X) \cup (Z(g) \cap X)$

$\Longrightarrow X = Z(f) \cap X \Longrightarrow X \subseteq Z(f) \Longrightarrow f \in I(X)$ $\square$

Summary. radical ideals $\leftrightarrow$ affine alg. vars

prime ideals $\leftrightarrow$ irreducible aff. alg. vars.

maximal ideals $\leftrightarrow$ one-point sets

This is a geometric version of:

maximal $\Rightarrow$ prime $\Rightarrow$ radical

More examples ① $\mathbb{A}^n$ is irreducible

since $I(\mathbb{A}^n) = (0)$ is prime.

② $f \in k[x_1, \dots, x_n]$ irreducible

$\Rightarrow Z(f)$ irreducible

since $k[x_1, \dots, x_n]$ is a UFD.

③ If $f = \prod f_i^{m_i}$ f_i irreducible

$\Rightarrow Z(f_i)$ are irred. components of $Z(f)$

Defn. A top. space is Noetherian if every descending chain of closed subsets is eventually stationary.

Note. $k[x_1, \dots, x_n]$ Noetherian $\Rightarrow$ aff. alg. vars are Noeth.

Note. A Hausdorff space is Noetherian iff it is finite.

Prop. A Noetherian top. space X can be written as a finite union of irred. closed subsets $X_1 \cup \cdots \cup X_r$.
If $X_i \not\subset X_j$ $\forall\, i \neq j$ the X_i are unique. In this case they are called the irred. components.

Pf. Existence. Let X be a minimal counterexample.
(this exists by the Noetherian condition).
Then X must be reducible: $X = X_1 \cup X_2$.
X minimal $\Rightarrow X_1, X_2$ can be decomposed into irred. closed subsets. Contradiction.
Uniqueness. Similarly straightforward. $\square$

Cor. Let $I \subseteq k[x_1, \ldots, x_n]$ radical. Then I is a finite intersection of prime ideals $p_1 \cap \cdots \cap p_m$.
If there are no inclusions $p_i \subseteq p_j$, the p_i are uniquely determined (they are the minimal prime ideals containing I).

Pf. Write $Z(I) = \bigcup^n X_i \leftarrow$ irred. Let $p_i = I(X_i)$
Have $Z(I) = \bigcup Z(p_i) = Z(\bigcap p_i)$
$I, \bigcap p_i$ both radical, so SN $\Rightarrow I = \bigcap p_i$.
Uniqueness follows from the Prop. $\square$

Remark. $X = Z(I) \subseteq \mathbb{A}^n$ is disconn iff $\exists$ ideals I, J s.t.
$I \cap J = I(X)$ & $I + J = k[x_1, \dots, x_n]$

In this case:

$$X = Z(I \cap J) = Z(I) \cup Z(J)$$
$$\emptyset = Z(I + J) = Z(I) \cap Z(J).$$