初めての代数幾何学 ②

東京工業大学　渡辺澄夫

1　復習

復習1

（あ）多項式の集合 $f_1(x), f_2(x), \cdots, f_K(x)$ に対し、それらの共通零点の集合を $\mathbf{V}(f_1,f_2,\ldots,f_K)$ と書いて代数多様体という。

（い）多項式の集合 $f_1(x), f_2(x), \cdots, f_K(x)$ に対しそれらを含む最小のイデアルを $<f_1,f_2,\ldots,f_K>$ と書き, $f_1(x),f_2(x), \cdots, f_K(x)$ により生成されるイデアルという。

（う） 代数多様体 V 上で零になる多項式全体はイデアルになる。これを $\mathbf{I}(V)$ と書き、V の定義イデアルという。

（え） {V; 代数多様体} ⇔ {$\mathbf{I}(V)$;定義イデアル} は全単射。

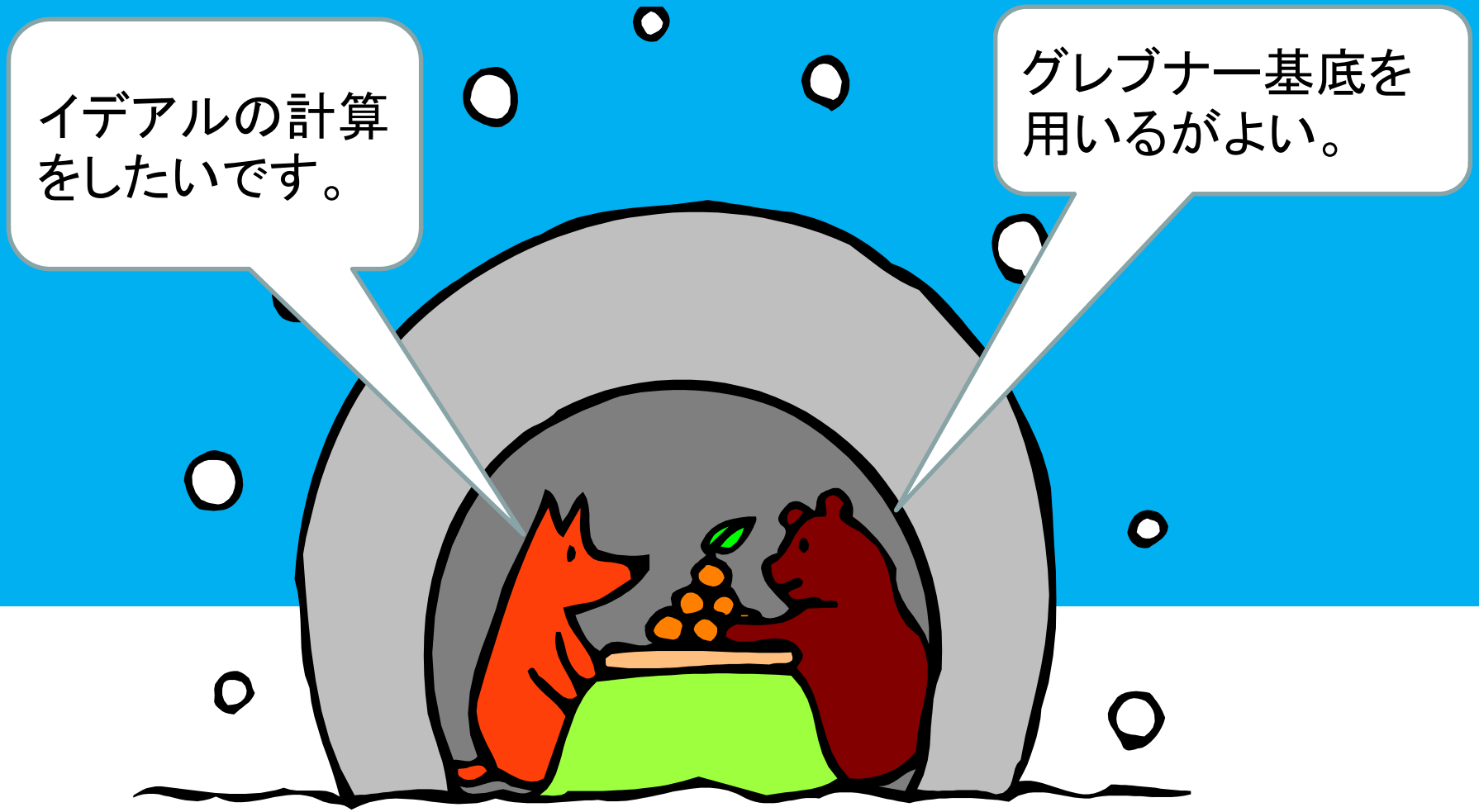
（お） 図形 V を調べるには代数 $\mathbf{I}(V)$ を調べるとよい。

復習２

パラメータ w を持つ関数 y=f(x,w) を統計学や機械学習に用いる場合、w についての特異点があると、100年前の統計学の方法はすべて使えなくなる。

深層学習や混合正規分布など現代で使われるすべてのモデルは特異点だらけである。学習の挙動は特異点により定められている。

第2回　目標



２　単項式と辞書式順序

単項式とイデアル

（あ） $\mathbf{R}[x_1,x_2,\ldots,x_n]$ の元で $a\,(x_1)^{k_1}(x_2)^{k_2}\,(x_3)^{k_3}\cdots(x_n)^{k_n}$ で
表されるものを単項式という。ここで $a\in\mathbf{R}$ で、
$k_1,k_2,\ldots,k_n$ は非負の整数。

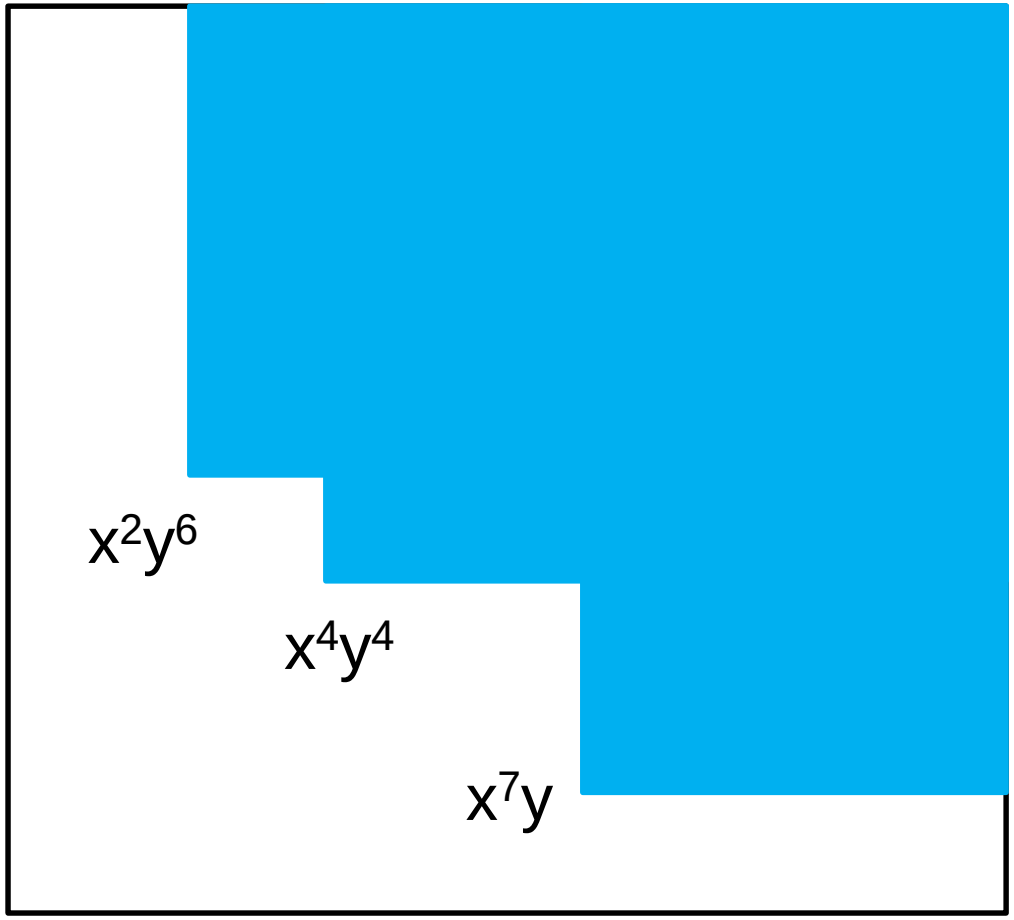
（い）単項式だけで生成されるイデアルを単項式イデアルという。
無限個の多項式から生成されていてもよい（が実は有限になる）。

例　$\mathbf{R}[x,y]$の元で x^2y^3 は単項式。$x^3y^4+x^5y^6$ は単項式でない。

$\langle x^3y^4,\ x^5y^3\rangle$ は単項式イデアルである。
$\langle x^3y^4 + xy^2 + 3\rangle$ は単項式イデアルではない
$\langle x^2 - y^3,\ x^2 + y^3\rangle$ は単項式イデアルである。

ディクソンの補題

定理　単項式イデアル I では、その中の有限個の単項式 $f_1,f_2,\ldots,f_K$ を選んで　$I=<f_1,f_2,\ldots,f_K>$ とできる。



証明。

この図を
みて証明を
述べて
みましょう。

3次元以上
のときは
次元に関する
帰納法です。

辞書式順序

たとえば $\mathbf{R}[x,y,z]$ の単項式 $x^p y^q z^r$ について

$x^p y^q z^r$ が $x^a y^b z^c$ よりも大きな項である。

$\Leftrightarrow$ 「$p>a$」 または 「$p=a$ かつ $q>b$」
または「$p=a$ かつ $q=b$ かつ $r>c$」

を辞書式順序という。変数がたくさんあるときも同様。

多項式 $f(x)$ の辞書式順序での最大項を $LT(f)$ と書く。
$LT(f)$ は単項式である。

例。$LT(x^3+y^3) = x^3$, $LT(y^4+y) = y^4$
$LT(x^3y^4+x^5y^3) = x^5y^3$, $LT(x^3y^4+x^3y^2) = x^3y^4$

多項式の割り算　例

割り算とは　：　辞書式順序での最大項を順番に消していく。
余りに繰り返し手続きをします。割る順は辞書式順序。

$f = x^3y + xy^2 + y^3$ を　x^2y-1, y^2-1 で割る。

$f = x(x^2y-1) + xy^2+x+y^3$　←あまりは(y^2-1)で割れる。

$= x(x^2y-1) + (x+y)(y^2-1) + 2x + y$

練習問題。　$f = x^5+y^5$ を x^2+y^2 と xy で割る。

多項式の割り算　例

順序を変えると余りは変わる。

(1) $x>y$ の順序では　$LT(x^3+y)=x^3$, $LT(x^2+y^2)=x^2$

$f = x^4+y^4$　を x^3+y, x^2+y^2　で割る。

$f = x(x^3+y) -xy+y^4$　←余りは x^2 で割れない。

(2) $x<y$ の順序では　$LT(x^3+y)=y$, $LT(x^2+y^2)=y^2$

$f = x^4+y^4$　を x^2+y^2, x^3+y で割る。

$f = y^2(x^2+y^2) –x^2y^2+x^4$　←余りは y で割れる。

$f = y^2(x^2+y^2) –(x^2y-x^5)\cdot(x^3+y)-x^8$ ←余りは y で割れない。

多項式の割り算　定義

多項式 f(x) の $f_1(x)$, $f_2(x)$,...,$f_K(x)$ による割り算の定義。

$LT(f_1(x))$, $LT(f_2(x))$,...,$LT(f_K(x))$ は辞書式順序について
大きいほうから並んでいるものとする。

(1) f(x) を $f_1(x)$ で割ると余りの辞書式順序は下がる。
(2) 余りを辞書式順序の大きい $f_k(x)$ の順で割っていく。
(3) 辞書式順序は下に有界なので、いずれとまる。このとき

$$f(x) = \Sigma_k\, g_k(x)\, f_k(x) + r(x)$$

で r(x) はOまたはどの $LT(f_k)$ でも割れなくなっている。

２　イデアルと単項式

イデアルと単項式

イデアル I に対して LT(I) ={ LT(f) ; f∈I } と定義する。

LT(I) は単項式の集合である。イデアルではない。

< LT(I) > は単項式イデアルである。

注意1 : 一般に <LT(I)>≠I である。

注意2 : I = $<f_1,f_2, \ldots,f_K>$ であっても

<LT(I)> = $<LT(f_1), LT(f_2), \ldots,LT(f_K)>$ とは限らない。

イデアルの単項式　例1

（注意）もしも f = g･q+ r ならば <f,g>=<g,r> である。

例　I=< x^3+y ,　x^2 >　とする。

I= < x^2, y >　なので
LT(I)={x^2, x^3, ..., y, y^2, ..., x^2y, x^3y,...}
<LT(I)>=<x^2,y>。

I=< x^2, y> かつ <LT(I)>=< LT（x^2）, LT（y） >である。
しかし <LT(I)>≠< LT（ x^3+y ）, LT（x^2） >である。

イデアルの単項式　例2

例。 $I=< x^3+y,\ x^2+y^2 >$ とする。

$I=< x^2+y^2\ ,\ xy^2-y >$ なので
$LT(I)=\{ x^2,\ldots,\ xy^2,\ldots, \}$. から $<LT(I)>=<x^2,\ xy^2>$.

このとき $I=< x^2+y^2\ ,\ xy^2-y >$ であり、かつ
$<LT(I)>=< LT(x^2+y^2),\ LT(xy^2-y) >$
が成り立っている。

注意：$<LT(I)>\neq< LT(\ x^3+y\ ),\ LT(x^2+y^2)\ >$である。
　　また $<LT(I)>\neq I$ である。

３　グレブナー基底

定理

定理　任意のイデアル I　に対して次が成り立つ。

(1) ある $f_1,f_2,\ldots,f_K \in I$ が存在して次式が成り立つ。

$$<LT(I)> = <LT(f_1), LT(f_2), \ldots, LT(f_K)>。$$

(2) (1) を成立させる $f_1,f_2,\ldots,f_K$ について

$$I = <f_1,f_2, \ldots,f_K>$$ が成り立つ。

◎ この定理はヒルベルトの基底定理を用いずに示すことができるから、この定理からヒルベルトの基底定理が証明できた。

証明

(1) $<LT(I)>$ は単項式の集合 LT(I) から生成されるイデアル
であるから、ディクソンの補題からすぐに証明される。

(2) $f_1,f_2,...,f_K \in I$ だから $<f_1,f_2, ...,f_K> \subset I$ は明らか。

$I \subset <f_1,f_2, ...,f_K>$を示せばよい。$f \in I$ とする。

ある r(x) が存在して $f(x) = \Sigma_k\, g_k(x)\, f_k(x) + r(x)$ と書けて

r(x) はOか、どの $LT(f_k)$ でも割り切れない（割り算の定義）。

$r(x) = f(x) - \Sigma_k\, g_k(x)\, f_k(x) \in I$ であるから (1) より

$LT(r) \in <LT(f_1), LT(f_2), ...,LT(f_K)>$が成り立つ。従って

r(x)=0. これより、$f \in <f_1,f_2, ...,f_K>$。 （証明終わり）

グレブナー基底

定義。 イデアル I に対して、$f_1,f_2,\ldots,f_K \in I$ が
次の両方を満たすとき

(1) $\langle LT(I)\rangle = \langle LT(f_1), LT(f_2), \ldots, LT(f_K)\rangle$

(2) $I = \langle f_1,f_2, \ldots,f_K\rangle$

I のグレブナー基底（標準基底）という。

注意1。任意のイデアルについてグレブナー基底は存在し、
(1)を満たせば(2)は自動的に満たされる。

注意2。グレブナー基底でないものについては (2) が
成り立っていても (1) が成りたたない。

グレブナー基底の作り方

I = $<f_1,f_2, \ldots,f_K>$ とする。

$f_1,f_2, \ldots,f_K$ の任意の組み合わせ (f_i,f_j) について

$LT(f_i)$ と $LT(f_j)$ が最小公倍の単項式になるように

単項式をかけて引き算し、打ち消すあうようにしたときの

余りを I に付け加えていくことを繰り返すと、新しい

LT( ) は辞書式順序で単調非増加になり、いずれ停止して、

そのときグレブナー基底が得られる。

グレブナー基底の作り方　例

$I=< x^3, yx^2+y^2 >$ とする。グレブナー基底でない。

$LT(x^3) = x^3$
$LT(yx^2+y^2) = yx^2$
であるから $y(x^3) - x(yx^2+y^2) = -xy^2$
$I=< x^3+y,\ yx^2+y^2,\ xy^2 >$ である。グレブナー基底でない。

$LT(yx^2+y^2) = x^3$
$LT(xy^2) = xy^2$
であるから $y(yx^2+y^2) - x(xy^2) = y^3$
$I=< x^3+y,\ yx^2+y^2,\ -xy^2,\ y^3 >$
どの組み合わせからも新しい LT が生まれなくなったので
グレブナー基底になった。

極小グレブナー基底

覚え方。

イデアルのグレブナー基底とは、イデアルの生成元であるだけでなく LT を作用させても足りないものがないもののことである。

I のグレブナー基底では

$$<LT(I)> = <LT(f_1), LT(f_2), \ldots, LT(f_K)>$$

が成り立つが、このうち、どれかひとつでも欠けたらこの関係が成り立たないとき極小グレブナー基底という。

４　既約な代数多様体

既約な代数多様体

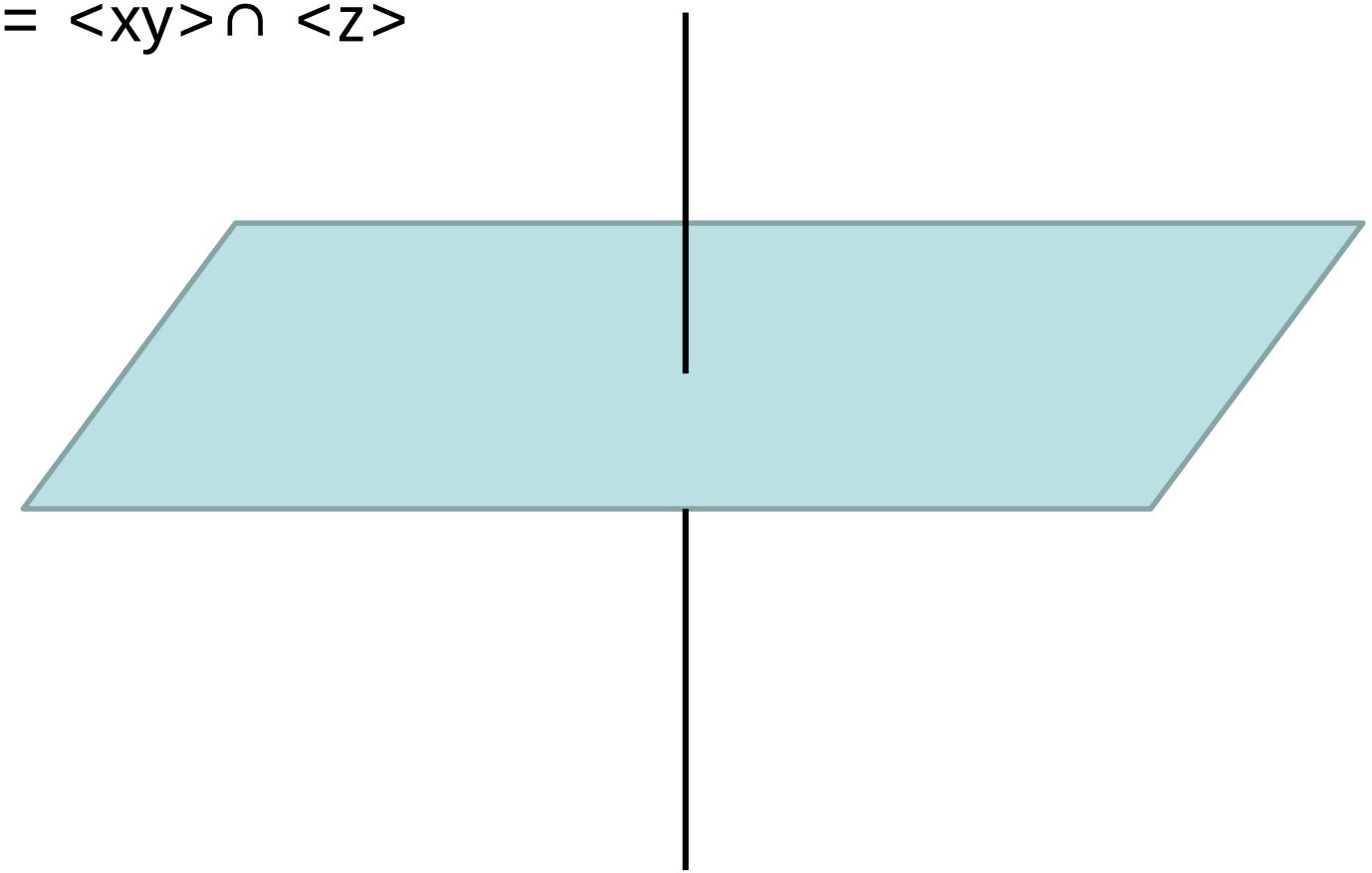
代数多様体 V が既約であるとは
$V=V_1 \cup V_2$ ならば $V=V_1$ または $V=V_2$

イデアル I が素イデアルであるとは
$f(x)g(x) \in I$ ならば $f(x) \in I$ または $g(x) \in I$

定理。代数多様体 V が既約である
$\Leftrightarrow$ 定義イデアル $\mathbf{I}(V)$ が素イデアルである

既約でない代数多様体の例

I(V)=<xy,z>
= <xy>∩ <z>



証明1

(既約⇒素イデアル)

$f(x)g(x) \in \mathbf{I}(V)$ とする。

V 上で $f(x) = 0$ または $g(x)=0$

$V=(V \cap \mathbf{V}(f)) \cup (V \cap \mathbf{V}(g))$

Vが既約であると仮定したから
$\mathbf{V}(f) \supset V$ または $\mathbf{V}(g) \supset V$

従って $f \in \mathbf{I}(V)$ または $g \in \mathbf{I}(V)$。

証明2

(素イデアル⇒既約)

$V=V_1 \cup V_2$とする。「$\mathbf{I}(V)=\mathbf{I}(V_1)$ または $\mathbf{I}(V)=\mathbf{I}(V_2)$ 」を示せばよい。

$\mathbf{I}(V_1) \cap \mathbf{I}(V)^c$ と $\mathbf{I}(V_2) \cap \mathbf{I}(V)^c$ のどちらかが空集合であることが示せればよい。

背理法:どちらも空でないとすると

$f \in \mathbf{I}(V_1) \cap \mathbf{I}(V)^c$

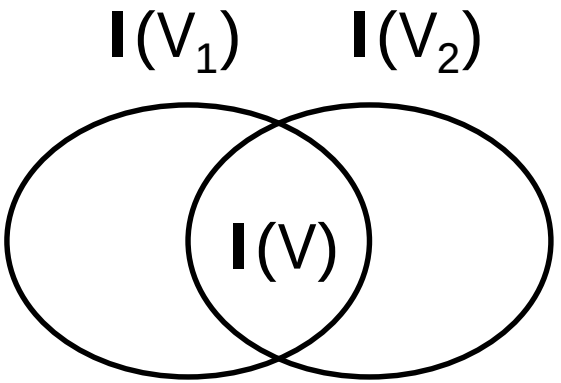
$g \in \mathbf{I}(V_2) \cap \mathbf{I}(V)^c$

がとれる。仮定から $f(x)g(x) \in \mathbf{I}(V)$

$\mathbf{I}(V)$が素イデアルと仮定したから

$f(x)g(x) \in \mathbf{I}(V)$

$\Rightarrow f(x) \in \mathbf{I}(V)$ または $g(x) \in \mathbf{I}(V)$:矛盾。



既約な代数多様体

定理。任意の代数多様体 V に対して既約な代数多様体 $V_1, V_2, \ldots, V_K$ が存在して $V = V_1 \cup V_2 \cup \cdots \cup V_K$

(証明) Vが既約なら証明終わり。
V　が既約でないとき $V = V_1 \cup V_2$ とできる ($V \neq V_1, V \neq V_2$)。
どちらも既約なら証明終わり。
V2が既約でない場合を考えて一般性を失わない。
V_2が既約でないときは $V_2 = V_3 \cup V_4$
同様の議論を繰り返すと既約でないものがある限り
$V \supset V_1 \supset V_2 \supset \cdots$の列が作れるが
対応する定義イデアルの列は有限の大きさでとまるので
Vの列も途中で止まる。(証明終わり)。

なぜ　既約な代数多様体

任意の代数多様体は既約なものの有限和であることがわかった。代数多様体を調べるとき、既約な代数多様体を調べることが非自明な課題になる。