Advanced Robotics

Lecture 11

Affine varieties

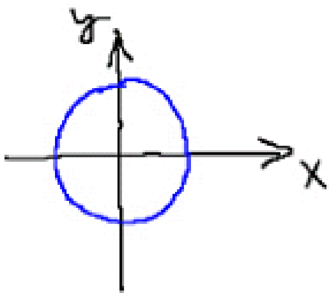
$f_k(x_1, x_2, \dots, x_n)$ ... algebraic equations

Algebraic variety $\equiv$ the set of points for which all equations f_k are satisfied

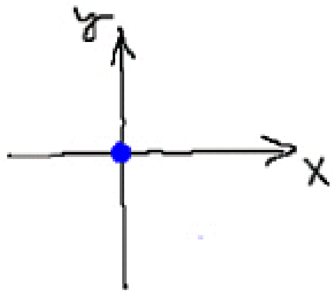
$$V = \{ (x_1, x_2, \dots, x_n) \mid \underline{f_k(x_1, x_2, \dots, x_n) = 0}, \; k = 1, 2, \dots, s \}$$

Examples:

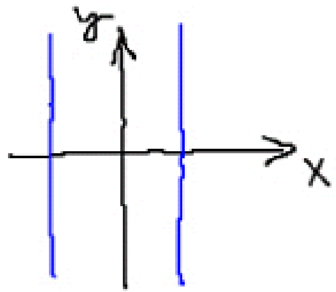
$\{x^2 + y^2 = 2\}$



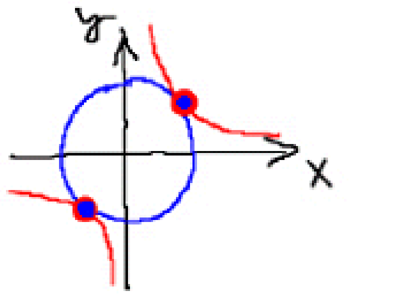
$\{x^2 + y^2 = 0\}$



$\{x^2 = 1\}$



$\{x^2 + y^2 = 1, \; xy = 1\}$



For solving IKU, we are interested in situations when there is a finite number of solutions $\equiv$ finite affine varieties

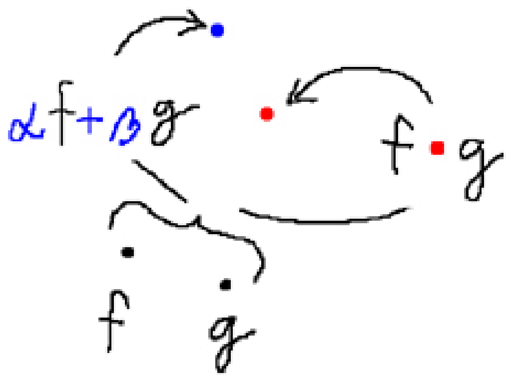
Notice that:

1) $f(a_1,a_2,\dots,a_n)=0$ & $g\in k[x_1,x_2,\dots,x_n] \Rightarrow (f\cdot g)(a_1,a_2,\dots,a_n)=0$

2) $f(a_1,a_2,\dots,a_n)=0$ & $g(a_1,a_2,\dots,a_n)=0 \Rightarrow (f+g)(a_1,a_2,\dots,a_n)=0$

$\Rightarrow$ there is an infinite number of different sets of algebraic equations defining the same variety

new "true" equations can be generated by algebraic operations with polynomials



Ideal: A subset $I \subseteq k[x_1, x_2, \dots, x_n]$ is an ideal if it satisfies:

(i) $0 \in I$

(ii) $f, g \in I \Rightarrow f + g \in I$

(iii) $f \in I$ & $h \in k[x_1, x_2, \dots, x_n] \Rightarrow h \cdot f \in I$

The ideal generated by polynomials $\{f_1, f_2, \dots, f_s\}$

The ideal generated by variety V

$$I(\{f_1, f_2, \dots, f_s\}) \subseteq I(V) \subseteq k[x_1, x_2, \dots, x_n]$$

$$V(\{f_1, f_2, \dots, f_s\})$$

Variety generated by a set of polynomials

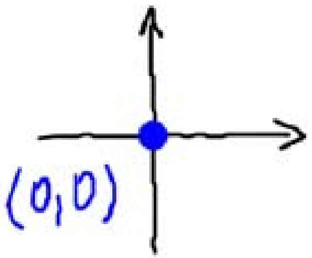
Excercises:

1. Let V be an affine variety. Prove that $I(V) = \{f \in k[x_1, \ldots, x_n] \,|\, f(x) = 0, \forall x \in V\}$ is an ideal.

$$I(\{f_1, f_2, \ldots, f_s\}) \subseteq I(V) \subseteq k[x_1, x_2, \ldots, x_n]$$

$$V(\{f_1, f_2, \ldots, f_s\})$$

Example



$$\{x^2, y^2\}$$

$$V(\{x^2, y^2\}) = \{(0,0)\}$$

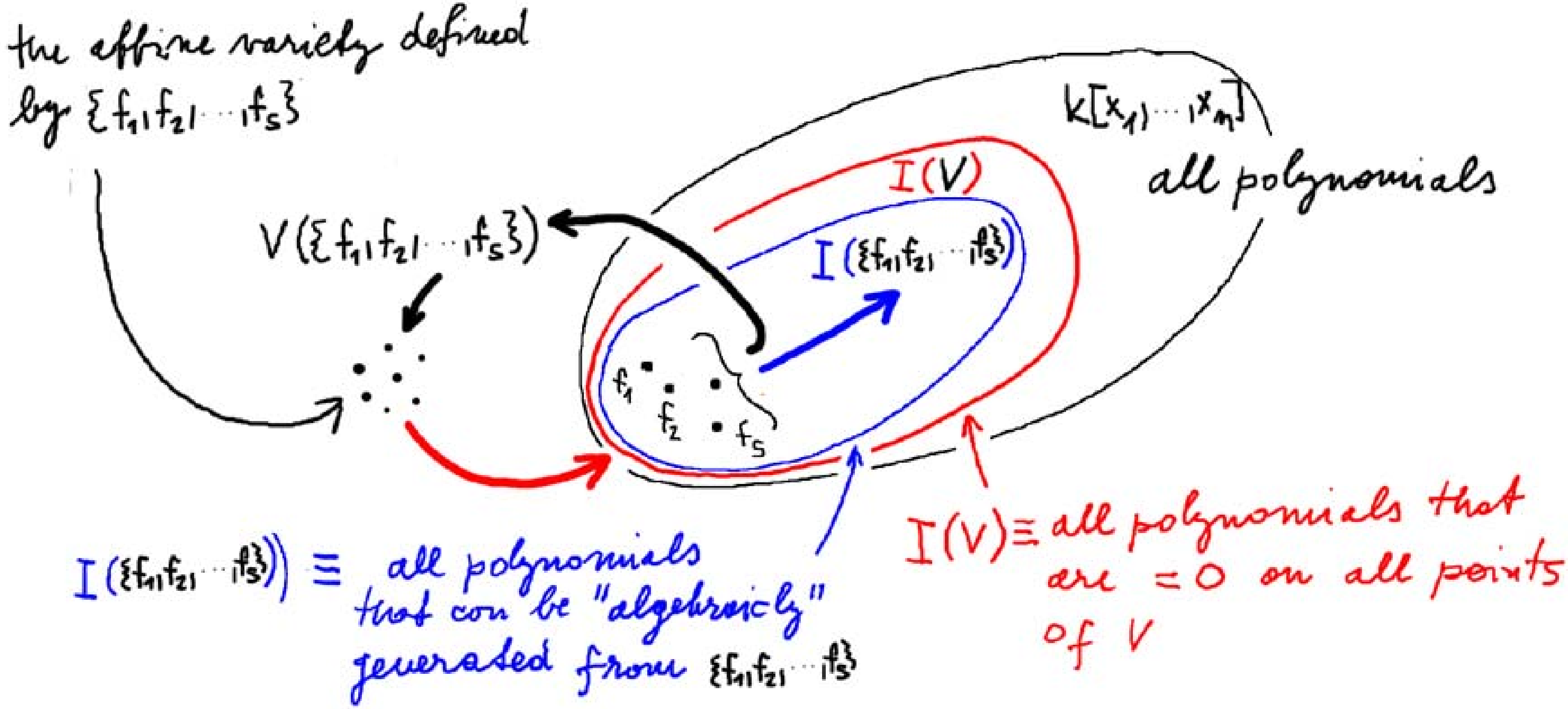
$$I(V(\{x^2, y^2\})) = I(\{x, y\})$$

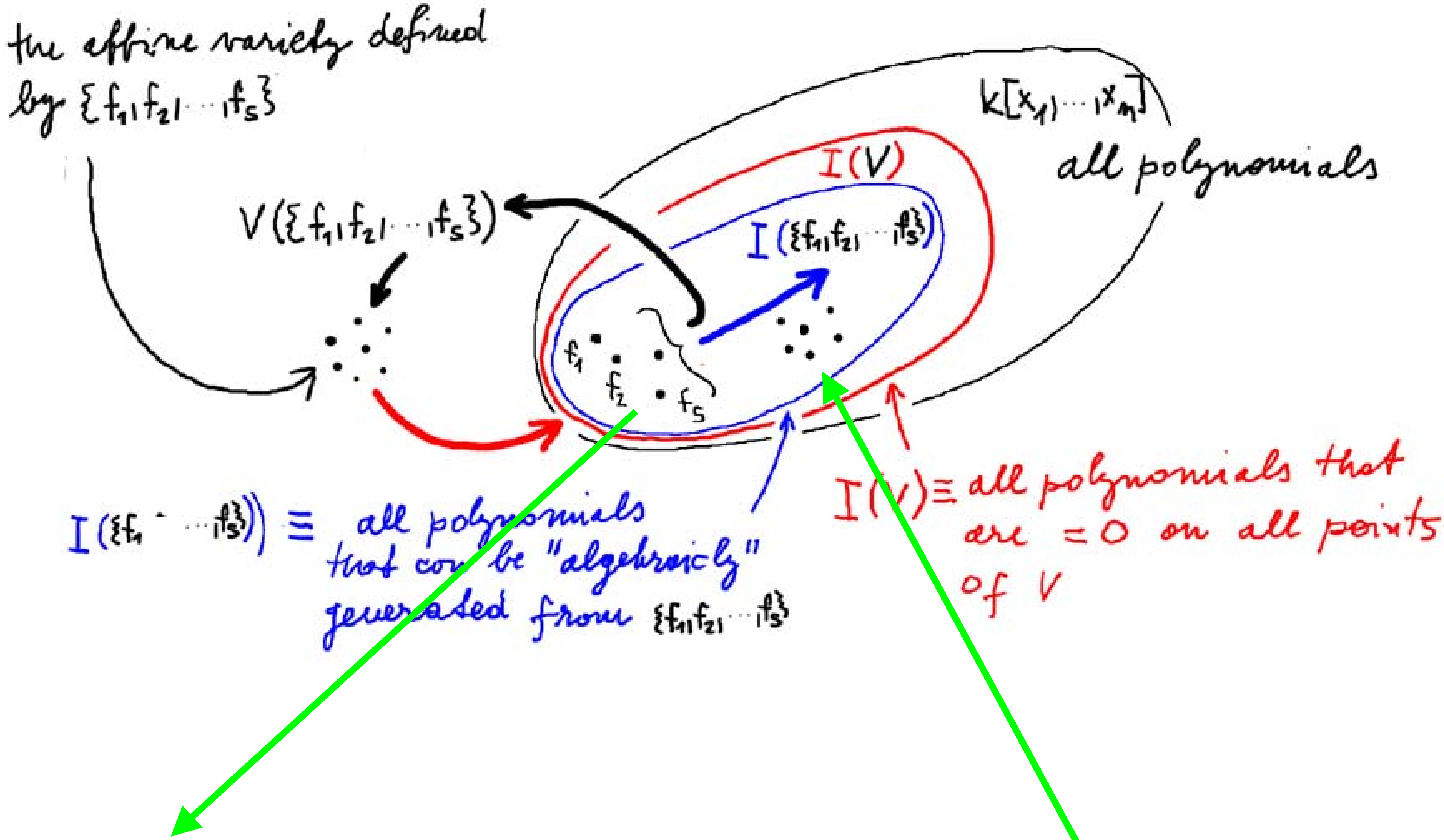
$$I(\{x^2, y^2\}) \subset I(\{x, y\})$$

because $x, y \in I(\{x, y\})$ but $x, y \notin I(\{x^2, y^2\})$

as every $h_1(x,y)\,x^2 + h_2(x,y)\,y^2$ has total degree at least two

pajdla@cmp.felk.cvut.cz


the affine variety defined by $\{f_1, f_2, \dots, f_s\}$
$k[x_1, \dots, x_n]$
all polynomials
$I(V)$
$V(\{f_1, f_2, \dots, f_s\})$
$I(\{f_1, f_2, \dots, f_s\})$
f_1
f_2
f_s
$I(\{f_1, f_2, \dots, f_s\}) \equiv$ all polynomials that can be "algebraicly" generated from $\{f_1, f_2, \dots, f_s\}$
$I(V) \equiv$ all polynomials that are $= 0$ on all points of V



Basis:
$B = \{f_1, f_2, \ldots, f_s\}$

$\xrightarrow[\text{manipulation}]{\text{Algebraic}}$

Groebner basis w.r.t. $<_{lex}$:
$G = \{g_1, g_2, \ldots, g_n\}$

Reading the solution out from a Groebner basis

Theorem 3: Let G be a Groebner basis constructed by the Buchberger algorithm w.r.t. $x_1 >_{lex} \cdots >_{lex} x_n$ from polynomials $\{f_1, \ldots, f_s\} \in \mathbb{C}[x_1, \ldots, x_n]$ for which equations $\{f_i = 0\}_{i=1,\ldots,s}$ have a finite number of solutions. Then G contains a polynomial $g \in \mathbb{C}[x_n]$.

There is often even more:

G often consists of a set of polynomials

$g_n(x_n)$

$g_{n-1}(x_n, x_{n-1})$

$g_{n-2}(x_n, x_{n-1}, x_{n-2})$

$\vdots$ $g_1(x_n, x_{n-1}, x_{n-2}, \ldots, x_1)$

"Division" by more than one polynomial

$$f = 3x^4 - x^2 + 2x \quad , \quad f_1 = x - 1 \quad , \quad f_2 = x^2 + 1$$

$$\begin{aligned}
f &= 0\cdot(x-1) + 0\cdot(x^2+1) + 3x^4 - x^2 + 2x & + \quad 0 \\
&= 3x^3(x-1) + 0\cdot(x^2+1) + 3x^3 - x^2 + 2x & + \quad 0 \\
&= (3x^3 + 3x^2)(x-1) + 0\cdot(x^2+1) + 2x^2 + 2x & + \quad 0 \\
&= (3x^3 + 3x^2 + 2x)(x-1) + 0\cdot(x^2+1) + 4x & + \quad 0 \\
&= (3x^3 + 3x^2 + 2x + 4)(x-1) + 0\cdot(x^2+1) & + \quad 4 \\
\hline
&= 3x(x^2+1) + 0\cdot(x-1) \qquad - x^2 - x & + \quad 0 \\
&= (3x-1)(x^2+1) + 0\cdot(x-1) \qquad - x + 1 & + \quad 0 \\
&= (3x-1)(x^2+1) - 1\cdot(x-1) & + \quad 0
\end{aligned}$$

We see that $f:(f_1, f_2) \neq f:(f_2, f_1) \Rightarrow f:\{f_1, f_2\}$ not well defined

pajdla@cmp.felk.cvut.cz

"Division theorem" for more than one divisor in $k[x_1, \dots, x_n]$

Let $>$ be a monomial order on $\mathbb{Z}^n_{\geq}$ and $F = (f_1, \dots, f_s)$ an ordered s-tuple, $f_i \in k[x_1, \dots, x_n]$. Then every $f \in k[x_1, \dots, x_n]$ can be written as

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

$a_i, r \in k[x_1, \dots, x_n]$ and either

$r = 0$ or none of the monomials of r is divisible by any of $LT(f_1), \dots, LT(f_s)$.

Furthermore

$$a_i f_i \neq 0 \Rightarrow \text{multideg}(f) \geq \text{multideg}(a_i f_i)$$

$r \equiv$ remainder of f on division by F ... $r = \overline{f}^F$

with the notation $F = (f_1, \dots, f_s)$

pajdla@cmp.felk.cvut.cz

"Division algorithm" for more than one divisor in $k[x_1, \dots, x_n]$

Input: $F = (f_1, \dots, f_s)$, f Output: $a_1, \dots, a_s, r \equiv \overline{f}^F$

$a_1 := a_2 := \dots a_s := r := 0,\ p := f$

WHILE $p \neq 0$ DO

{ $i := 1$

divisionoccured := FALSE

WHILE $i \leq s$ AND divisionoccured = FALSE DO

{IF $LT(f_i)$ divides $LT(p)$ THEN

{ $a_i := a_i + \dfrac{LT(p)}{LT(f_i)}$

$p := p - \dfrac{LT(p)}{LT(f_i)} \cdot f_i$

divisionoccured := TRUE }

ELSE { $i := i + 1$ } }

IF divisionoccured = FALSE THEN

{ $r := r + LT(p)$

$p := p - LT(p)$ }

}

Proof as for 1 variable

degree $\rightarrow$ multidegree

$r \rightarrow p$

Example

$x >_{lex} y \qquad f = \underset{\downarrow\,(1,2)}{xy^2} + \underset{\downarrow\,(1,0)}{x} + \underset{\downarrow\,(0,0)}{1}, \quad f_1 = \underset{\downarrow\,(1,1)}{xy} + \underset{\downarrow\,(0,0)}{1}, \quad f_2 = \underset{\downarrow\,(0,1)}{y} + \underset{\downarrow\,(0,0)}{1}$

$$f = y\,(xy+1) + \underset{\downarrow\,(1,0)}{x} - \underset{\downarrow\,(0,1)}{y} + \underset{\downarrow\,(0,0)}{1} = \underset{\downarrow\,a_1}{y}\,(xy+1) \underset{\downarrow\,a_2}{-1}\,(y+1) + \underbrace{x+2}_{\downarrow\,r}$$

$$f = \overbrace{0}^{a_1} \cdot f_1 + \overbrace{0}^{a_2} \cdot f_2 + \overbrace{xy^2 + x + 1}^{p} + \overbrace{0}^{r}$$

$$= y \cdot f_1 + 0 \cdot f_2 + x - y + 1 + 0$$

$$= y \cdot f_1 + 0 \cdot f_2 \qquad - y + 1 + x$$

$$= y \cdot f_1 - 1 \cdot f_2 \qquad + 2 + x$$

$$= y \cdot f_1 - 1 \cdot f_2 \qquad + x + 2$$

Example:

$$f = xy^2 - x \qquad f_1 = xy + 1 \qquad f_2 = y^2 - 1$$

$>_{lex}$, $x >_{lex} y$

a) $f : (f_1, f_2)$

$$xy^2 - x = \underbrace{y}_{a_1}(xy + 1) + \underbrace{0}_{a_2} \cdot (y^2 - 1) + \underbrace{(-x - y)}_{r}$$

b) $f : (f_2, f_1)$

$$xy^2 - x = \underbrace{x}_{a_1}(y^2 - 1) + \underbrace{0}_{a_2} \cdot (xy + 1) + \underbrace{0}_{r}$$

The order of polynomials in F matters