Elimination Theory

James Carlson

CIMAT Lectures

February 27, 2008

Elimination theory

The j-th elimination ideal of I is $I \cap k[x_{j+1}, \ldots, x_n]$

We eliminated the first j variables to obtain I_j

If $I \subset k[x, y]$, then $I_x = I \cap k[y]$ and I are the elimination ideals. The closure of the projection of $V(I)$ on the y-axis is the variety defined by the elimination ideal I_x.

Theorem

Let G be a Groebner basis for I in the lex order. Then $G \cap k[x_{j+1}, \ldots, x_n]$ is a Groebner basis for the j-th elimination ideal I_j.

Example. Let $I = \langle x^3 + xy + 1, x^2y^2, y^4 \rangle$

Its Groebner basis in the lex order is $y^2, x^3 + xy + 1$. Therefore $I_x = \langle y^2 \rangle$

The projection of $V(I)$ on the y-axis is the (doubled) origin.

Example, continued

Note: `I.dimension() = 0`, `I.vector_space_dimension() = 6`.

$V(I)$ consists of three doubled points.

Elimination theory makes it easy to find $V(I)$. First solve $y^2 = 0$. Then substitute $y = 0$ in $y^2, x^3 + xy + 1$ to obtain $x^3 = -1$.

Thus

$$V(I) = \{ (-1, 0), (-\omega, 0), (-\omega^2, 0) \}$$

Let $K = \mathbf{Q}$ and let $L = \mathbf{Q}[\omega]$.Then $V(K)$, the set of K-rational points, consists of a single element. But $V(L)$ has three points.

The action of the Galois group of L/K, which is $\mathbf{Z}/2$, breaks $V(L)$ into a one-point orbit and a two-point orbit.

Intersection of two conics

We will compute the interection of the circle $x^2 + y^2 = 1$ with the ellipse $x^2/2 + 2y^2 = 1$.

```
R.<x,y> = PolynomialRing(QQ)
f = x^2 + y^2 - 1
g = x^2/2 + 2*y^2 - 1
I = ideal(f,g)
B = I.groebner_basis()
I.dimension(); I.vector_space_dimension(); B
0, 4, [y^2 - 1/3, x^2 - 2/3]
```

$V(I) = \{ \ (\pm 1/\sqrt{3}, \pm\sqrt{2}/\sqrt{3}) \ \}$

Projection onto the y-axis is not in general position relative to $V(I)$.

Intersection of two conics, continued

Let K be the field obtained by adjoining a root of $y^2 - 1/3 = 0$: $K = \mathbf{Q}[\sqrt{3}]$. Its Galois group is of order two.

Let L be the field obtained from K by adjoining a root of $x^2 - 2/3$: $L = \mathbf{Q}[\sqrt{2}, \sqrt{3}]$.

Then $Gal(L/\mathbf{Q}) \cong \mathbf{Z}/2 \times \mathbf{Z}/2$.

$Gal(L/\mathbf{Q})$ acts transitively on $V(L)$.

$Gal(K/\mathbf{Q})$ permutes the fibers.

Intersection of a conic and a quintic

Let's study the intersection of the unit circle and the quintic $x^5/2 + 2y^5 = 1$.

Thus let $I = \langle x^2 + y^2 - 1, x^5/2 + 2x^5 - 1 \rangle$

We find that I has dimension zero, and the $\mathbf{Q}[x, y]/I$ is a vector space of dimension ten.

The Groebner basis is

```
[ y^10 - 5/17*y^8 + 10/17*y^6 - 16/17*y^5 - 10/17*y^4 +
    5/17*y^2 + 3/17,
  x + 238/9*y^9 + 170/9*y^8 + 13*y^7 + 21/2*y^6 + 221/9*y^5
    - 95/18*y^4 - 145/9*y^3 - 265/18*y^2 - 17/3*y - 35/6  ]
```

It has the form $F(y), x + G(y)$, where $I_x = \langle F(y) \rangle$.

Conic and quintic, continued

From the form of the Groebner basis we see that projection onto the y-axis is generic.

Also, the Galois group of $F(y)$ gives the action of $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$ on $V(\bar{\mathbf{Q}})$.

Assuming G is the Groebner basis in $R = \mathbf{Q}[x, y]$, we compute the Galois group:

```
S.<u> = PolynomialRing(QQ)
phi = R.hom([0,u], S)
h = phi(B[0])
K.<a> = NumberField(h/h.leading_coefficient())
K.galois_group()
Galois group PARI group [3628800, -1, 45, "S10"]
of degree 10 of the number field Number Field
in a with defining polynomial ...
```

Conic and quintic, continued

Thus $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$ acts on $V(\bar{\mathbf{Q}})$ through $Gal(K/\mathbf{Q}) \cong S_{10}$.

And $V(\bar{\mathbf{Q}}) = V(K)$.

Lines on the cubic surface

As an illustration of what we have done so far, we will compute the number of lines on a cubic surface S.

This will be a warmup for our study of the Elsenhans-Jahnel paper.

There they study the image of the group $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$ one the set of lines $\mathcal{L}$ of S.

It is known that that the image is a subgroup of $W(E_6)$.

It is also known that generically the image is $W(E_6)$.

The Elsenhans-Jahnel algorithm allows us to exihibit specific cubic surfaces with maximal Galois image.

See http://www.uni-math.gwdg.de/jahnel/linkstopaperse.html

Set up the rings to be used, read in cubic polynomial

We will write a program `lines.sage` that we can execute at the commmand line: `sage lines.sage 2 3 5 7`. This command will attempt to find the Galois image for
$x^3 + y^3 + z^3 + w^3 + 2yzw + 3xzw + 5xyw + 7xyz$

```
import sys

K = QQ
R.<a,b,c,d> = PolynomialRing(K, order = "lex")
S.<x,y,z,w> = PolynomialRing(K)

p1, p2, p3, p4 = map( lambda x: int(x), sys.argv[1:] )

F = x^3 + y^3 + z^3 + w^3 +
      p1*y*z*w + p2*x*z*w + p3*x*y*w + p4*x*y*z
print "F =", F
```

Verify that surface is smooth; set up ideal of lines

```
J = ideal(F.jacob())
pd = J.dimension() - 1

print "Projective dimension of singular locus =", pd

L = lambda t: (1,t,a+b*t,c+d*t)
FL = lambda t: F(L(t))
J = ideal(FL(0), FL(1), FL(2), FL(3) )
B = J.groebner_basis()
```

Check Groebner basis; draw conclusions

```
print "Variables on which g[i] depends:"
for i in range(0,len(B)):
  print i, B[i].variables()

g = B[0]; dg = g.degree(); nf = len(factor(g))

print "degree(g) =", g.degree()
print "number of factors of g =", len(factor(g))

if nf == 1 and dg == 27:
print "cubic surface has 27 lines"
```

Example and usage

```
[chiquito:jc] sage lines.sage 2 3 5 7


F = x^3 + y^3 + 7*x*y*z + z^3 +
      5*x*y*w + 3*x*z*w + 2*y*z*w + w^3
Projective dimension of singular locus = -1
Variables on which g[i] depends:
0 [d]
1 [d, c]
2 [d, b]
3 [d, a]
degree(g) = 27
number of factors of g = 1
cubic surface has 27 lines
```

The polynomial $g = B[0]$

```
1631363571648*d^27 + 2582867599790 4*d^26 +
17405826144379 2*d^25 + 67042026851493 6*d^24 +
16764055242233 04*d^23 + 29754841871234 16*d^22 +
47829403626651 36*d^21 + 10123074083576 106*d^20 +
23578095466184706*d^19 + 40873449674344679*d^18 +
49700044180519437*d^17 + 56665434448534617*d^16 +
91887374548676657*d^15 + 15395145493353 2346*d^14 +
19070650476685 0386*d^13 + 14007429097582 2037*d^12 +
53432695230612333*d^11 + 66098863812061161*d^10 +
12757238782558 2827*d^9 + 97842438970193286*d^8 +
27880556381159262*d^7 + 14563730364420960*d^6 +
26236696128820584*d^5 + 18211964913020760*d^4 +
5315592754434120*d^3 + 944024070738000*d^2 +
3429372025160 0*d - 47674198376000
```

Remarks

Why can't we just look at the number field that g defines and compute the Galois group directly using Sage?

Answer: <type 'exceptions.NotImplementedError'>: Sorry, computation of Galois groups of fields of degree bigger than 11 is not yet implemented. Try installing the optional free (closed source) KASH package, which supports up to degree 23.