

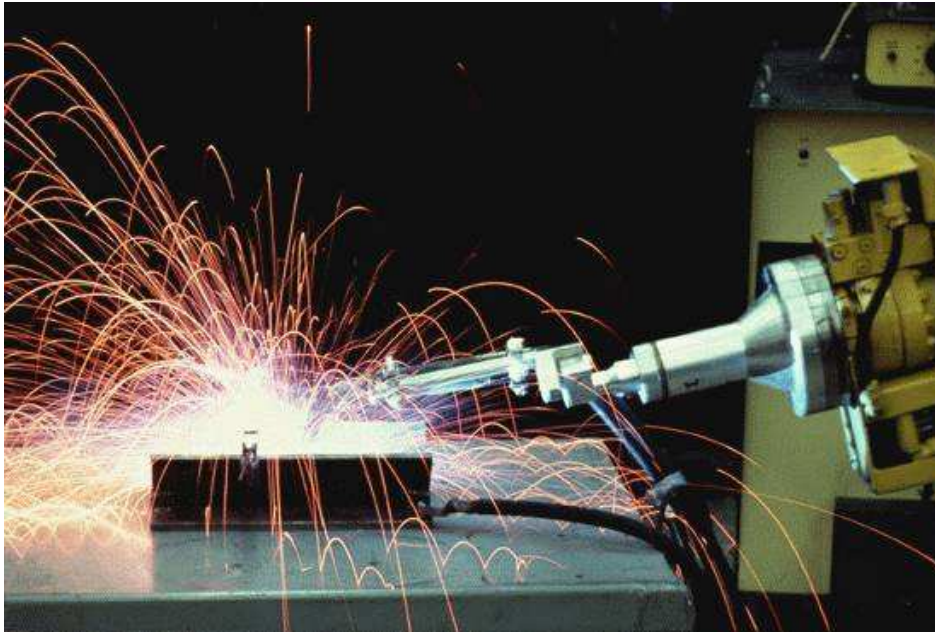
SINGULAR and Applications
talk at the
CIMPA School Lahore 2012

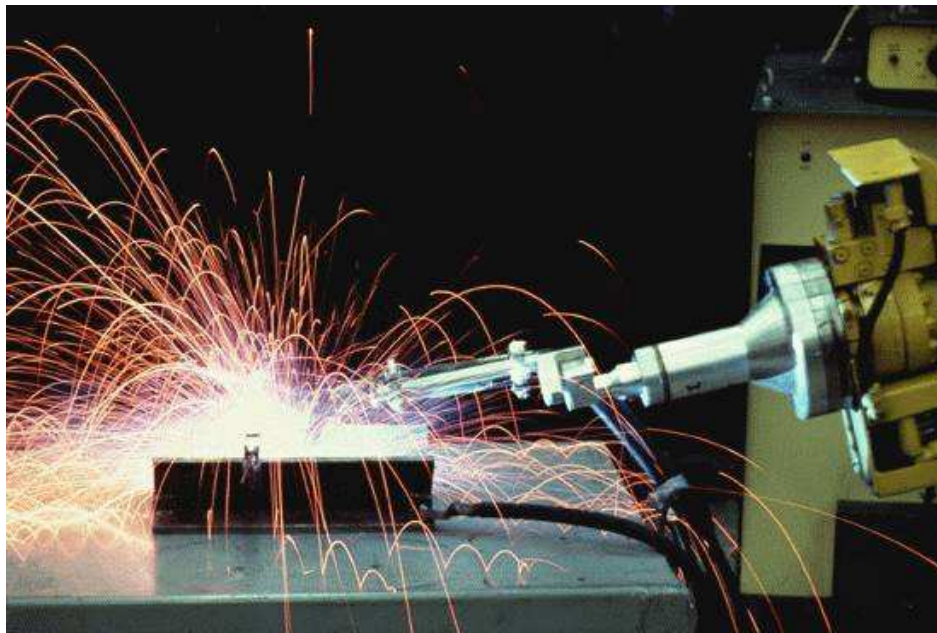
Gerhard Pfister

`pfister@mathematik.uni-kl.de`

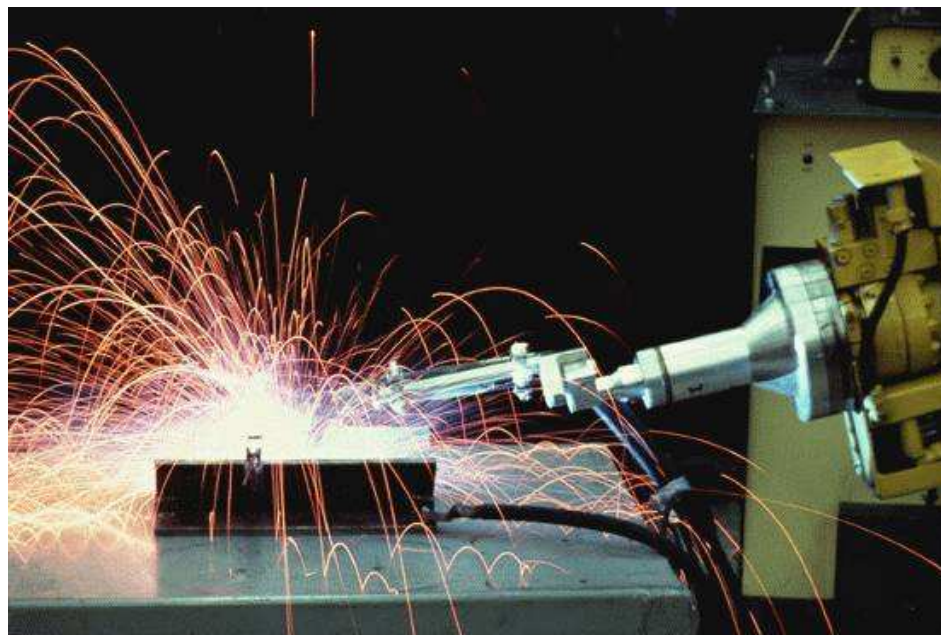
Departement of Mathematics
University of Kaiserslautern

Robotics and the Cycloheptane Molecule

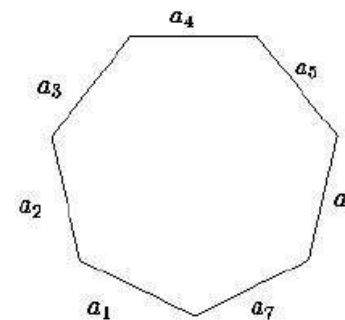
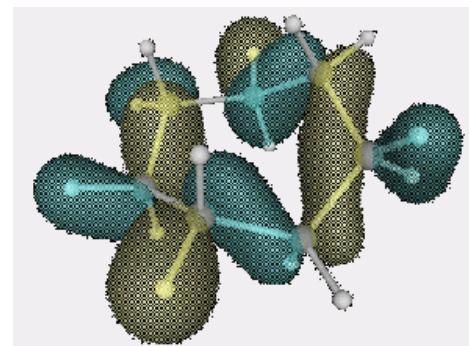




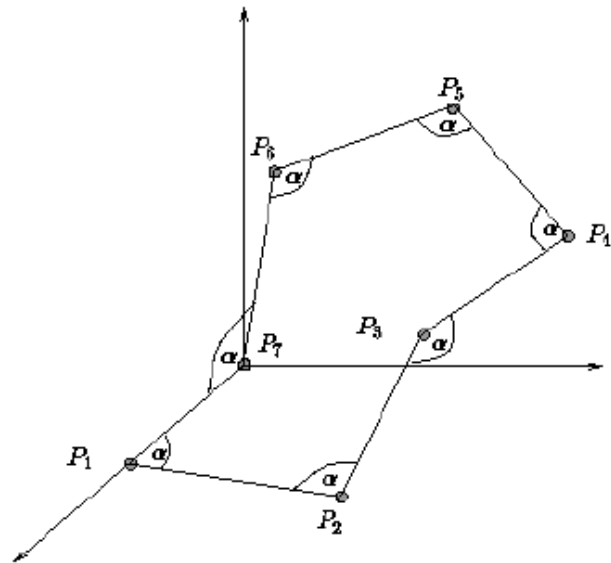
A.H.M. Levelt



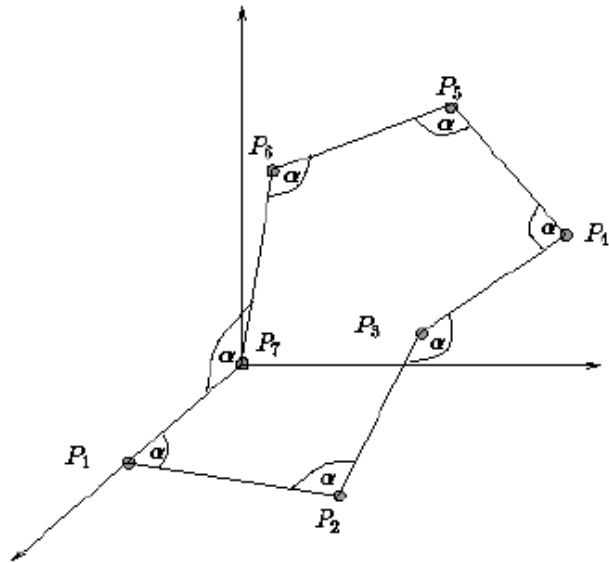
A.H.M. Levelt



The Heptagon



The Heptagon

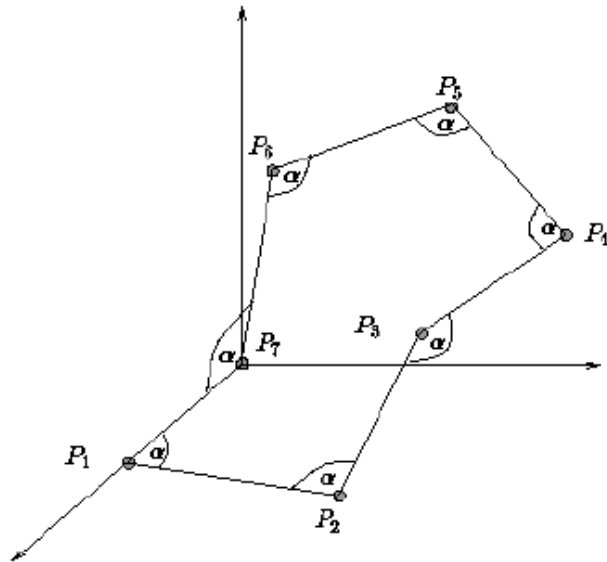


Equations for the vectors:

- $(a_1, a_2) = (a_2, a_3) = \dots = (a_7, a_1) = c$
- $(a_1, a_1) = (a_2, a_2) = \dots = (a_7, a_7) = 1$
- $a_1 + a_2 + \dots + a_7 = 0$

$c = \cos(\alpha)$ and $(,)$ is the scalar product.

The Heptagon



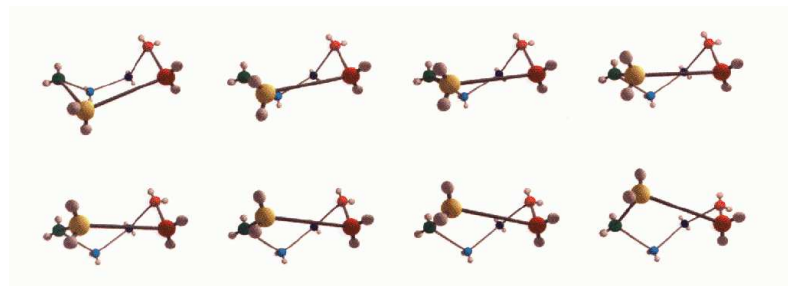
Equations for the vectors:

- $(a_1, a_2) = (a_2, a_3) = \dots = (a_7, a_1) = c$
- $(a_1, a_1) = (a_2, a_2) = \dots = (a_7, a_7) = 1$
- $a_1 + a_2 + \dots + a_7 = 0$

$c = \cos(\alpha)$ and $(,)$ is the scalar product.

- For $c = 0$: equations for the configuration space of a robot
- For $c = \frac{1}{3}$: equations for the configurations space of a molecule

Equations for the configuration space (in SINGULAR):



```
ring R=0, (v,w,x,y,z), dp;
```

```
ideal I=
```

```
81y2z2-54wyz+54y2z+54yz2-72w2+198wy-207y2+198wz-225yz-207z2+114w-141y-141z+10,
```

```
81w2x2+54w2x+54wx2-54wxz-207w2-225wx-207x2+198wz+198xz-72z2-141w-141x+114z+10,
```

```
324vw2x+432vw2+540vwx+432w2x-432wxy-432vwz+324wyz+180vw+846w2-576vx+180wx-
```

```
306wy+144xy+144vz-306wz-36yz+12v+585w+12x-318y-318z-79,
```

```
81v2w2+54v2w+54vw2-54vwy-207v2-225vw-207w2+198vy+198wy-72y2-141v-141w+114y+10;
```

```
eliminate(I, vyz);
```

The Projection

The equations describe a **curve in \mathbb{R}^5** . The **projection** to the w, x -plane is difficult to compute:

The Projection

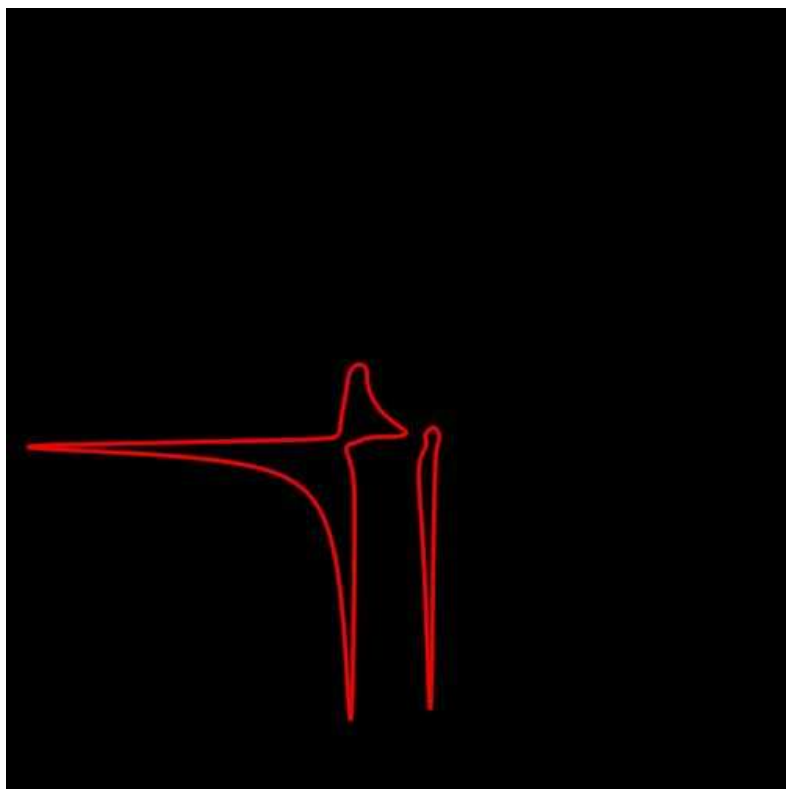
The equations describe a **curve in \mathbb{R}^5** . The **projection** to the w, x -plane is difficult to compute:

$$\begin{aligned} &13343098629642274643741505w^{20}x^{16}+18458805154059402163602552w^{20}x^{15} \\ &+12528539096440613433050772w^{19}x^{16}-307469543636682571308498792w^{20}x^{14} \\ &-308745089273555811810514188w^{19}x^{15}-335770469789305978523636514w^{18}x^{16} \end{aligned}$$

·
·
·

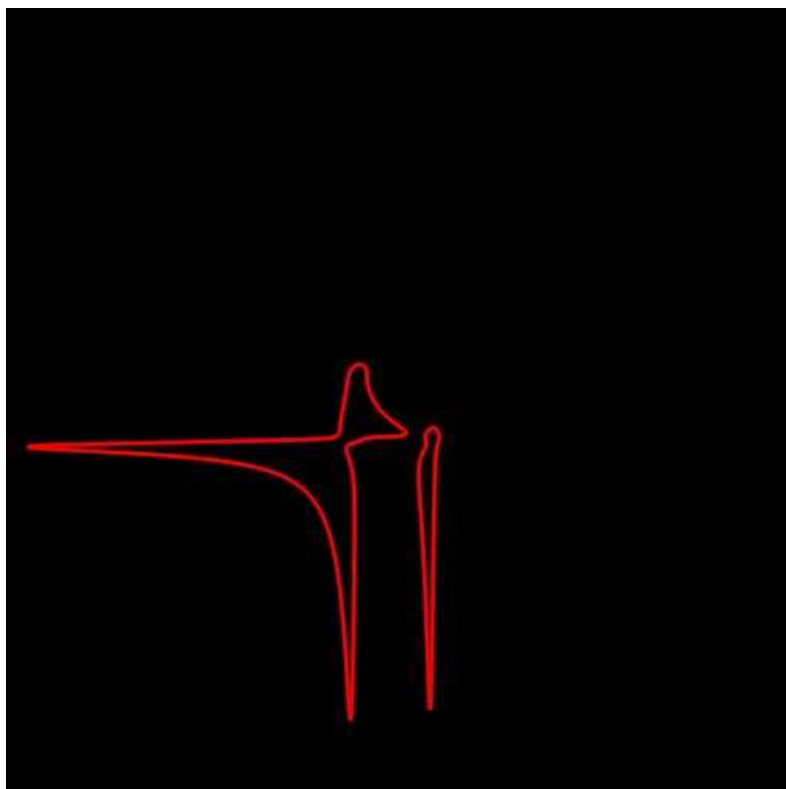
$$\begin{aligned} &-57603722394732542788396875000w^2x-56209703485755917382271875000wx^2 \\ &-29459059311819369252628125000x^3-3456386878638867977468750000w^2 \\ &-388065077492910629437500000wx-3500955605594366547468750000x^2 \\ &+1264097844032306972500000000w+1126578705265908772500000000x \\ &+240658492841196850000000000 \end{aligned}$$

Projection of the curve to the w, x -plane



```
ideal K = eliminate(I,vyz);  
LIB''surf.lib'';  
plot(K[1]);
```

Projection of the curve to the w, x -plane



```
ideal K = eliminate(I, vyz);  
LIB "surf.lib";  
plot(K[1]);
```

The curve shows the possible w, x -coordinates of the molecule.

```
ring r=0,(a,b),dp;  
poly f=33375/100*b6+a2*(11a2b2-b6-121b4-2)+55/10*b8+a/(2*33096);  
f=subst(f,a,77617);  
f=subst(f,b,33096);  
f;  
-54767/66192
```

```
ring s=(real,30),(a,b),dp;  
poly g=imap(r,f);  
g;  
-0.82739605994682136814116509548
```

```
ring s1=real,(a,b),dp;
```

```
poly f=33375/100*b6+a2*(11a2b2-b6-121b4-2)+55/10*b8+a/(2*33096);
```

```
f=subst(f,a,77617);
```

```
f=subst(f,b,33096);
```

```
f;
```

```
-1.205e+10
```

```
ring s2=(real,10),(a,b),dp;
```

```
poly f=33375/100*b6+a2*(11a2b2-b6-121b4-2)+55/10*b8+a/(2*33096);
```

```
f=subst(f,a,77617);
```

```
f=subst(f,b,33096);
```

```
f;
```

```
-0.1204879738e+11
```

```
ring s3=(real,20),(a,b),dp;  
poly f=33375/100*b6+a2*(11a2b2-b6-121b4-2)+55/10*b8+a/(2*33096);  
f=subst(f,a,77617);  
f=subst(f,b,33096);
```

```
f;  
-12048797376.82739606
```

```
ring s4=(real,30),(a,b),dp;  
poly f=33375/100*b6+a2*(11a2b2-b6-121b4-2)+55/10*b8+a/(2*33096);  
f=subst(f,a,77617);  
f=subst(f,b,33096);
```

```
f;  
-0.82739605994682136814116509548
```

Let G be a finite group, define

$$G^{(1)} := [G, G] = \langle aba^{-1}b^{-1} \mid a, b \in G \rangle .$$

and $G^{(i)} := [G^{(i-1)}, G]$.

G is called **nilpotent**, if $G^{(m)} = \{e\}$ for some m .

Let G be a finite group, define

$$G^{(1)} := [G, G] = \langle aba^{-1}b^{-1} \mid a, b \in G \rangle .$$

and $G^{(i)} := [G^{(i-1)}, G]$.

G is called **nilpotent**, if $G^{(m)} = \{e\}$ for some m .

- Abelian groups are nilpotent.
- If the order of G is a power of a prime, G is nilpotent.
- G is nilpotent \Leftrightarrow it is a direct product of its Sylow groups.
- S_3 is not nilpotent.

Magma:

```
> G:=Sym(3);
```

```
> H:=CommutatorSubgroup(G,G);
```

```
H;
```

```
Permutation group acting on a set of cardinality 3
```

```
Order = 3
```

```
(1, 2, 3)
```

```
> CommutatorSubgroup(H,G);
```

```
Permutation group acting on a set of cardinality 3
```

```
Order = 3
```

```
(1, 2, 3)
```

with GAP:

```
gap> G:=SymmetricGroup(3);  
Sym( [ 1 .. 3 ] )  
gap> CommutatorSubgroup(G,G);  
Group([ (1,2,3) ])
```

with sage:

```
sage: G = SymmetricGroup(3)  
sage: H = G.commutator(G)  
sage: H  
Permutation Group with generators [(1,2,3)]
```

$$D_4 = \langle r, s \mid r^4 = s^2 = e, srs = r^{-1} \rangle$$

```
> #DihedralGroup(4);
```

```
8
```

```
> G:=CommutatorSubgroup(DihedralGroup(4),DihedralGroup(4));
```

```
Permutation group acting on a set of cardinality 4
```

```
Order = 2
```

```
(1, 3)(2, 4)
```

```
> CommutatorSubgroup(G,DihedralGroup(4));
```

```
Permutation group acting on a set of cardinality 4
```

```
Order = 1
```

Now define

$$G^{(i)} := [G^{(i-1)}, G^{(i-1)}],$$

then G is called **solvable**, if $G^{(m)} = \{e\}$ for a suitable m .

Now define

$$G^{(i)} := [G^{(i-1)}, G^{(i-1)}],$$

then G is called **solvable**, if $G^{(m)} = \{e\}$ for a suitable m .

- nilpotente groups are solvable.
- S_3, S_4 are solvable.
- groups of odd order are solvable.
- S_5, A_5 are not solvable.

```
> CommutatorSubgroup(Sym(5),Sym(5));
```

Permutation group acting on a set of cardinality 5

Order = 60 = $2^2 * 3 * 5$

(1, 2, 3)

(2, 3, 4)

(3, 4, 5)

```
> Alt(5) eq CommutatorSubgroup(Sym(5),Sym(5));
```

true

```
> CommutatorSubgroup(Alt(5),Alt(5));
```

Permutation group acting on a set of cardinality 5

Order = 60 = $2^2 * 3 * 5$

(1, 2, 3)

(2, 3, 4)

(3, 4, 5)

```
> G:=CommutatorSubgroup(Sym(4),Sym(4));
```

```
> G;
```

Permutation group G acting on a set of cardinality 4

Order = 12 = $2^2 * 3$

(1, 2, 3)

(2, 3, 4)

```
> H:=CommutatorSubgroup(G,G);
```

```
> H;
```

Permutation group H acting on a set of cardinality 4

Order = 4 = 2^2

(1, 4)(2, 3)

(1, 3)(2, 4)

```
> CommutatorSubgroup(H,H);
```

Permutation group acting on a set of cardinality 4

Order = 1

$$\mathrm{PSL}(2, K) = \mathrm{SL}(2, K) / \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a^2 = 1 \right\}$$

$$\mathrm{PSL}(2, K) = \mathrm{SL}(2, K) / \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a^2 = 1 \right\}$$

especially

$$\mathrm{PSL}(2, \mathbb{F}_5) = \left\{ \left[\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \right], a_{11}a_{22} - a_{21}a_{12} = 1 \right\}$$

$$\left[\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \right] = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \begin{pmatrix} 4a_{11} & 4a_{12} \\ 4a_{21} & 4a_{22} \end{pmatrix} \right\} .$$

$$\mathrm{PSL}(2, K) = \mathrm{SL}(2, K) / \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a^2 = 1 \right\}$$

especially

$$\mathrm{PSL}(2, \mathbb{F}_5) = \left\{ \left[\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \right], a_{11}a_{22} - a_{21}a_{12} = 1 \right\}$$

$$\left[\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \right] = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \begin{pmatrix} 4a_{11} & 4a_{12} \\ 4a_{21} & 4a_{22} \end{pmatrix} \right\} .$$

It holds:

$$\mathrm{PSL}(2, \mathbb{F}_5) \cong \mathrm{PSL}(2, \mathbb{F}_4) \cong A_5$$

```
> G:=PSL(2,5);
```

```
> G;
```

Permutation group G acting on a set of cardinality 6

```
Order = 60 = 2^2 * 3 * 5
```

```
(3, 4)(5, 6)
```

```
(1, 6, 2)(3, 4, 5)
```

```
> IsIsomorphic(G,Alt(5));
```

```
true Homomorphism of GrpPerm: G, Degree 6, Order 2^2 * 3 * 5 into
```

```
GrpPerm: $, Degree 5, Order 2^2 * 3 * 5 induced by
```

```
(3, 4)(5, 6) |--> (1, 3)(2, 5)
```

```
(1, 6, 2)(3, 4, 5) |--> (1, 4, 2)
```

Problem: Characterize the class of **finite solvable groups** G by 2–variable identities.

Problem: Characterize the class of **finite solvable groups** G by 2–variable identities.

Example:

- G is **abelian** $\Leftrightarrow xy = yx \forall x, y \in G$
- (Zorn, 1930) A finite group G is **nilpotent** $\Leftrightarrow \exists n \geq 1$, such that $v_n(x, y) = 1 \forall x, y \in G$
(Engel Identity)

$$v_1 := [x, y] = xyx^{-1}y^{-1} \text{ (commutator)}$$

$$v_{n+1} := [v_n, y]$$

Theorem (T. Bandman, G.-M. Greuel, F. Grunewald, B. Kunyavsky, G. Pfister, E. Plotkin)

$$U_1 = U_1(x, y) := x^2 y^{-1} x,$$

$$U_{n+1} = U_{n+1}(x, y) = [xU_n x^{-1}, yU_n y^{-1}].$$

A finite group G is **solvable** $\Leftrightarrow \exists n$, such that $U_n(x, y) = 1 \forall x, y \in G$.

Theorem (T. Bandman, G.-M. Greuel, F. Grunewald, B. Kunyavsky, G. Pfister, E. Plotkin)

$$U_1 = U_1(x, y) := x^2 y^{-1} x,$$

$$U_{n+1} = U_{n+1}(x, y) = [xU_n x^{-1}, yU_n y^{-1}].$$

A finite group G is **solvable** $\Leftrightarrow \exists n$, such that $U_n(x, y) = 1 \forall x, y \in G$.

- $U_1(x, y) = 1 \Leftrightarrow y = x^{-1}$
- $U_1(x, y) = U_2(x, y)$
 $\Leftrightarrow x^{-1} y x^{-1} y^{-1} x^2 = y x^{-2} y^{-1} x y^{-1}$
- **Let $x, y \in G$ such that $y \neq x^{-1}$ and $U_1(x, y) = U_2(x, y) \Rightarrow U_n(x, y) \neq 1 \forall n \in \mathbb{N}$.**

G solvable \Rightarrow Identity is true (by definition).

G solvable \Rightarrow Identity is true (by definition).

Idea of \Leftarrow

Theorem (Thompson, 1968)

Let G minimally not solvable. Then G is one of the following groups:

G solvable \Rightarrow Identity is true (by definition).

Idea of \Leftarrow

Theorem (Thompson, 1968)

Let G minimally not solvable. Then G is one of the following groups:

- **PSL**(2, \mathbb{F}_p), p a prime number ≥ 5

G solvable \Rightarrow Identity is true (by definition).

Idea of \Leftarrow

Theorem (Thompson, 1968)

Let G minimally not solvable. Then G is one of the following groups:

- **PSL**(2, \mathbb{F}_p), p a prime number ≥ 5
- **PSL**(2, \mathbb{F}_{2^p}), p a prime number
- **PSL**(2, \mathbb{F}_{3^p}), p a prime number

G solvable \Rightarrow Identity is true (by definition).

Idea of \Leftarrow

Theorem (Thompson, 1968)

Let G minimally not solvable. Then G is one of the following groups:

- **PSL**(2, \mathbb{F}_p), p a prime number ≥ 5
- **PSL**(2, \mathbb{F}_{2^p}), p a prime number
- **PSL**(2, \mathbb{F}_{3^p}), p a prime number
- **PSL**(3, \mathbb{F}_3)

G solvable \Rightarrow Identity is true (by definition).

Idea of \Leftarrow

Theorem (Thompson, 1968)

Let G minimally not solvable. Then G is one of the following groups:

- **PSL**(2, \mathbb{F}_p), p a prime number ≥ 5
- **PSL**(2, \mathbb{F}_{2^p}), p a prime number
- **PSL**(2, \mathbb{F}_{3^p}), p a prime number
- **PSL**(3, \mathbb{F}_3)
- **Sz**(2^p) p a prime number.

G solvable \Rightarrow Identity is true (by definition).

Idea of \Leftarrow

Theorem (Thompson, 1968)

Let G minimally not solvable. Then G is one of the following groups:

- **PSL**(2, \mathbb{F}_p), p a prime number ≥ 5
- **PSL**(2, \mathbb{F}_{2^p}), p a prime number
- **PSL**(2, \mathbb{F}_{3^p}), p a prime number
- **PSL**(3, \mathbb{F}_3)
- **Sz**(2^p) p a prime number.

It is enough to prove (for G in Thompson's list): $\exists x, y \in G$, such that $y \neq x^{-1}$ and $U_1(x, y) = U_2(x, y)$.

Let us consider $G = \mathrm{PSL}(2, \mathbb{F}_p)$, $p \geq 5$

Let us consider $G = \text{PSL}(2, \mathbb{F}_p)$, $p \geq 5$

Consider the matrices

$$x = \begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix} \quad y = \begin{pmatrix} 1 & b \\ c & 1 + bc \end{pmatrix}$$

$x^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}$ implies $y \neq x^{-1}$ for all $(b, c, t) \in \mathbb{F}_p^3$.

Let us consider $G = \text{PSL}(2, \mathbb{F}_p)$, $p \geq 5$

Consider the matrices

$$x = \begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix} \quad y = \begin{pmatrix} 1 & b \\ c & 1 + bc \end{pmatrix}$$

$x^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}$ implies $y \neq x^{-1}$ for all $(b, c, t) \in \mathbb{F}_p^3$.

It is enough to prove that the equation

$$U_1(x, y) = U_2(x, y), \text{ i.e.} \\ x^{-1}yx^{-1}y^{-1}x^2 = yx^{-2}y^{-1}xy^{-1}$$

has a solution $(b, c, t) \in \mathbb{F}_p^3$.

The entries of $U_1(x, y) - U_2(x, y)$ are the following polynomials in $\mathbb{Z}[b, c, t]$ Let $I = \langle p_1, \dots, p_4 \rangle$ and $I^{(p)}$ the induced ideal over \mathbb{Z}/p :

$$p_1 = b^3 c^2 t^2 + b^2 c^2 t^3 - b^2 c^2 t^2 - bc^2 t^3 - b^3 ct + b^2 c^2 t + b^2 ct^2 + 2bc^2 t^2 \\ + bct^3 + b^2 c^2 + b^2 ct + bc^2 t - bct^2 - c^2 t^2 - ct^3 - b^2 t + bct + c^2 t \\ + ct^2 + 2bc + c^2 + bt + ct + c + 1$$

$$p_2 = -b^3 ct^2 - b^2 ct^3 + b^2 c^2 t + bc^2 t^2 + b^3 t - b^2 ct - 2bct^2 - b^2 c + bct \\ + c^2 t + ct^2 - bt - ct - b - c - 1$$

$$p_3 = b^3 c^3 t^2 + b^2 c^3 t^3 - b^2 c^2 t^3 - bc^2 t^4 - b^3 c^2 t + b^2 c^3 t + b^2 c^2 t^2 \\ + 2bc^3 t^2 + bc^2 t^3 + b^2 c^2 t + b^2 ct^2 + bc^2 t^2 - c^2 t^3 - ct^4 - 2b^2 ct \\ + bc^2 t + c^3 t + bct^2 + 2c^2 t^2 + ct^3 - b^2 c - b^2 t + bct + c^2 t + bt^2 \\ + 3ct^2 + bc - bt - b - c + 1$$

$$p_4 = -b^3 c^2 t^2 - b^2 c^2 t^3 + b^2 c^2 t^2 + bc^2 t^3 + b^3 ct - b^2 c^2 t - b^2 ct^2 - 2bc^2 t^2 \\ - bct^3 - 2b^2 ct + c^2 t^2 + ct^3 + b^2 t - bct - c^2 t - ct^2 + b^2 - bt \\ - 2ct - b - t + 1$$

Groups: SINGULAR session

```
LIB"linalg.lib";    option(redSB);
ring R = 0,(c,b,t),(c,lp);
matrix X[2][2] = t, -1,
                1,  0;
matrix Y[2][2] = 1, b,
                c, 1+bc;
matrix iX = inverse(X);    matrix iY = inverse(Y);
matrix M=iX*Y*iX*iY*X*X-Y*iX*iX*iY*X*iY;    ideal I=flatten(M);    I;
I[1]=c2b3t2+c2b2t3-c2b2t2+c2b2t+c2b2-c2bt3+2c2bt2+c2bt-c2t2+c2t+c2-cb3t
      +cb2t2+cb2t+cbt3-cbt2+cbt+2cb-ct3+ct2+2ct+c-b2t+bt+1
I[2]=c2b2t+c2bt2+c2t-cb3t2-cb2t3-cb2t-cb2-2cbt2+cbt+ct2-ct-c+b3t-bt-b-1
I[3]=c3b3t2+c3b2t3+c3b2t+2c3bt2+c3t-c2b3t-c2b2t3+2c2b2t2+c2b2t-c2bt4
      +2c2bt3+c2bt2+c2bt-c2t3+2c2t2+c2t+2cb2t2-2cb2t-cb2+cbt2+cbt+cb-ct4
      +ct3+3ct2-c-b2t+bt2-bt-b+1
I[4]=-c2b3t2-c2b2t3+c2b2t2-c2b2t+c2bt3-2c2bt2+c2t2-c2t+cb3t-cb2t2-2cb2t
      -cbt3-cbt+ct3-ct2-2ct+b2t+b2-bt-b-t+1
```

Theorem von Hasse–Weil (generalized by [Aubry and Perret](#) for
singulare curves):

Theorem von Hasse–Weil (generalized by Aubry and Perret for singular curves):

Let $C \subseteq \mathbb{A}^n$ be an absolutely irreducible affine curve defined over the finite field \mathbb{F}_q and $\overline{C} \subset \mathbb{P}^n$ its projective closure \Rightarrow

$$\#C(\mathbb{F}_q) \geq q + 1 - 2p_a\sqrt{q} - d$$

($d = \text{degree}$, $p_a = \text{arithmetic genus of } \overline{C}$).

Theorem von Hasse–Weil (generalized by Aubry and Perret for singular curves):

Let $C \subseteq \mathbb{A}^n$ be an absolutely irreducible affine curve defined over the finite field \mathbb{F}_q and $\overline{C} \subset \mathbb{P}^n$ its projective closure \Rightarrow

$$\#C(\mathbb{F}_q) \geq q + 1 - 2p_a\sqrt{q} - d$$

($d = \text{degree}$, $p_a = \text{arithmetic genus of } \overline{C}$).

The Hilbert–polynomial of \overline{C} , $H(t) = d \cdot t - p_a + 1$, can be computed using the ideal I_h of \overline{C} :

We obtain $H(t) = 10t - 11 \Rightarrow d = 10, p_a = 12$.

Theorem von Hasse–Weil (generalized by Aubry and Perret for singular curves):

Let $C \subseteq \mathbb{A}^n$ be an absolutely irreducible affine curve defined over the finite field \mathbb{F}_q and $\overline{C} \subset \mathbb{P}^n$ its projective closure \Rightarrow

$$\#C(\mathbb{F}_q) \geq q + 1 - 2p_a\sqrt{q} - d$$

($d = \text{degree}$, $p_a = \text{arithmetic genus of } \overline{C}$).

The Hilbert–polynomial of \overline{C} , $H(t) = d \cdot t - p_a + 1$, can be computed using the ideal I_h of \overline{C} :

We obtain $H(t) = 10t - 11 \Rightarrow d = 10, p_a = 12$.

Since $p + 1 - 24\sqrt{p} - 10 > 0$ if $p > 593$, we obtain the result.

Groups: SINGULAR session

```
ring S=0,(c,b,t,w),dp;  
ideal I=imap(R,I);  
I=std(I);  
I=homog(I,w);  
hilbPoly(std(I));  
-11,10
```

Proposition: $V(I^{(p)})$ is absolutely irreducible for all primes $p \geq 5$.

Proposition: $V(I^{(p)})$ is absolutely irreducible for all primes $p \geq 5$.

proof:

Using **SINGULAR** we show:

$$\langle f_1, f_2 \rangle : h^2 = I.$$

Proposition: $V(I^{(p)})$ is absolutely irreducible for all primes $p \geq 5$.

proof:

Using **SINGULAR** we show:

$$\langle f_1, f_2 \rangle : h^2 = I.$$

$$f_1 = t^2b^4 + (t^4 - 2t^3 - 2t^2)b^3 - (t^5 - 2t^4 - t^2 - 2t - 1)b^2 \\ - (t^5 - 4t^4 + t^3 + 6t^2 + 2t)b + (t^4 - 4t^3 + 2t^2 + 4t + 1)$$

$$f_2 = (t^3 - 2t^2 - t)c + t^2b^3 + (t^4 - 2t^3 - 2t^2)b^2 \\ - (t^5 - 2t^4 - t^2 - 2t - 1)b - (t^5 - 4t^4 + t^3 + 6t^2 + 2t)$$

$$h = t^3 - 2t^2 - t$$

```
setring R;
ideal J=(t2)*b4+(-t4+2t3)*b3+(-t5+3t4-2t3+2t+1)*b2+(t5-4t4+3t3+2t2)*b+(t4-4t3+2t2+4t+1),
(t3-2t2-t)*c+(t2)*b3+(-t4+2t3)*b2+(-t5+3t4-2t3+2t+1)*b+(t5-4t4+3t3+2t2);
poly h=t*(t2-2t-1);
ideal K=quotient(J,h^2);
reduce(K,std(I));
_[1]=0
_[2]=0
_[3]=0
_[4]=0
_[5]=0
reduce(I,std(K));
_[1]=0
_[2]=0
_[3]=0
_[4]=0
```

Let $P(x) := t^2 J[1]|_{b=x/t}$ then P is monic of degree 4.

Let $P(x) := t^2 J[1]|_{b=x/t}$ then P is monic of degree 4.

$$x^4 + (t^3 - 2t^2 - 2t)x^3 - (t^5 - 2t^4 - t^2 - 2t - 1)x^2 - \\ (t^6 - 4t^5 + t^4 + 6t^3 + 2t^2)x + (t^6 - 4t^5 + 2t^4 + 4t^3 + t^2).$$

We prove, that the induced polynomial $P \in \mathbb{F}_p[t, x]$ is absolutely irreducible for all primes $p \geq 2$.

(Using the lemma of Gauß this is equivalent to P being irreducible in $\overline{\mathbb{F}_p}(t)[x]$.)

Ansatz

$$(*) \quad P = (x^2 + ax + b)(x^2 + gx + d)$$

a, b, g, d polynomials in t with variable coefficients

$$a(i), b(i), g(i), d(i).$$

Ansatz

$$(*) \quad P = (x^2 + ax + b)(x^2 + gx + d)$$

a, b, g, d polynomials in t with variable coefficients

$$a(i), b(i), g(i), d(i).$$

The decomposition $(*)$ with $a(i), b(i), g(i), d(i) \in \overline{\mathbb{F}}_p$ does not exist iff the ideal \mathbb{C} generated by the coefficients with respect to x, t of $P - (x^2 + ax + b)(x^2 + gx + d)$ has no solution in $\overline{\mathbb{F}}_p$. This is equivalent to the fact that $1 \in \mathbb{C}$.

The ideal of the coefficients of C :

$$C[1] = -b(5) * d(3)$$

$$C[2] = -b(5) * g(2)$$

$$C[3] = -b(4) * d(3) - b(5) * d(2)$$

$$C[4] = -b(4) * g(2) - b(5) * g(1) - d(3) - 1$$

$$C[5] = -b(3) * d(3) - b(4) * d(2) - b(5) * d(1) + 1$$

$$C[6] = -b(5) - g(2) - 1$$

$$C[7] = a(0) * b(5) - a(2) * d(3) - b(3) * g(2) - b(4) * g(1) - d(2) + 4$$

$$C[8] = -a(0)^2 * b(5) + b(0) * b(5) - b(2) * d(3) - b(3) * d(2) - b(4) * d(1) - b(5) - 4$$

$$C[9] = -a(2) * g(2) - b(4) - g(1) + 2$$

$$C[10] = a(0) * b(4) - a(1) * d(3) - a(2) * d(2) - b(2) * g(2) - b(3) * g(1) - d(1) - 1$$

$$C[11] = -a(0)^2 * b(4) + b(0) * b(4) - b(1) * d(3) - b(2) * d(2) - b(3) * d(1) - b(4) + 2$$

$$C[12] = a(0) - a(1) * g(2) - a(2) * g(1) - b(3) - d(3)$$

$$C[13] = -a(0)^2 + a(0) * b(3) - a(0) * d(3) - a(1) * d(2) - a(2) * d(1) + b(0) - b(1) * g(2) - b(2) * g(1) - 7$$

$$C[14] = -a(0)^2 * b(3) + b(0) * b(3) - b(0) * d(3) - b(1) * d(2) - b(2) * d(1) - b(3) + 4$$

$$C[15] = -a(2) - g(2) - 2$$

$$C[16] = a(0) * a(2) - a(0) * g(2) - a(1) * g(1) - b(2) - d(2) + 1$$

$$C[17] = -a(0)^2 * a(2) + a(0) * b(2) - a(0) * d(2) - a(1) * d(1) + a(2) * b(0) - a(2) - b(0) * g(2) - b(1) * g(1) - 2$$

$$C[18] = -a(0)^2 * b(2) + b(0) * b(2) - b(0) * d(2) - b(1) * d(1) - b(2) + 1$$

$$C[19] = -a(1) - g(1) - 2$$

$$C[20] = a(0) * a(1) - a(0) * g(1) - b(1) - d(1) + 2$$

$$C[21] = -a(0)^2 * a(1) + a(0) * b(1) - a(0) * d(1) + a(1) * b(0) - a(1) - b(0) * g(1)$$

$$C[22] = -a(0)^2 * b(1) + b(0) * b(1) - b(0) * d(1) - b(1)$$

$$C[23] = -a(0)^3 + 2 * a(0) * b(0) - a(0)$$

$$C[24] = -a(0)^2 * b(0) + b(0)^2 - b(0)$$

Using SINGULAR, one shows that over
 $\mathbb{Z}[\{a(i)\}, \{b(i)\}, \{g(i)\}, \{d(i)\}]$

$$4 = \sum_{i=1}^{24} M_i C[i].$$

We want to compute

● $\frac{3}{4} + \frac{1}{3} = \frac{13}{12}$

We want to compute

● $\frac{3}{4} + \frac{1}{3} = \frac{13}{12}$

0	$\frac{3}{4}$	$\frac{1}{3}$		$\frac{13}{12}$
5	2	2		4
			+	
181	46	121		167
905	227	302		529

$$N = p_1 \cdot \dots \cdot p_m$$

$$N = p_1 \cdot \dots \cdot p_m$$

$$\bullet \quad \mathbb{Z}/N \xrightarrow{\sim} \bigoplus_{i=1}^m \mathbb{Z}/p_i$$

$$N = p_1 \cdot \dots \cdot p_m$$

$$\bullet \quad \mathbb{Z}/N \xrightarrow{\sim} \bigoplus_{i=1}^m \mathbb{Z}/p_i$$

$$\bullet \quad F_n = \left\{ \frac{a}{b} \in \mathbb{Q} \mid \gcd(a, b) = 1, 0 \leq |a| \leq n, 0 < b < n \right\}$$

$$N = p_1 \cdot \dots \cdot p_m$$

$$\bullet \quad \mathbb{Z}/N \xrightarrow{\sim} \bigoplus_{i=1}^m \mathbb{Z}/p_i$$

$$\bullet \quad F_n = \left\{ \frac{a}{b} \in \mathbb{Q} \mid \gcd(a, b) = 1, 0 \leq |a| \leq n, 0 < b < n \right\}$$

$$\bullet \quad \mathbb{Q}_N = \left\{ \frac{a}{b} \in \mathbb{Q} \mid \gcd(a, b) = \gcd(b, N) = 1 \right\}$$

$$\bullet \quad f_N : \mathbb{Q}_N \rightarrow \mathbb{Z}/N$$

$$\bullet \quad f_N \left(\frac{a}{b} \right) = (a \bmod N)(b \bmod N)^{-1}$$

$$N = p_1 \cdot \dots \cdot p_m$$

$$\bullet \quad \mathbb{Z}/N \xrightarrow{\sim} \bigoplus_{i=1}^m \mathbb{Z}/p_i$$

$$\bullet \quad F_n = \left\{ \frac{a}{b} \in \mathbb{Q} \mid \gcd(a, b) = 1, 0 \leq |a| \leq n, 0 < b < n \right\}$$

$$\bullet \quad \mathbb{Q}_N = \left\{ \frac{a}{b} \in \mathbb{Q} \mid \gcd(a, b) = \gcd(b, N) = 1 \right\}$$

$$\bullet \quad f_N : \mathbb{Q}_N \rightarrow \mathbb{Z}/N$$

$$\bullet \quad f_N \left(\frac{a}{b} \right) = (a \bmod N)(b \bmod N)^{-1}$$

$$\bullet \quad \text{If } 2n^2 < N \text{ then } f_N \text{ is injective on } F_n \cap \mathbb{Q}_N.$$

- we want to compute the fraction corresponding to $529 \bmod 905$

- we want to compute the fraction corresponding to $529 \bmod 905$

$$\begin{pmatrix} 905 \\ 0 \end{pmatrix} = \begin{pmatrix} 529 \\ 1 \end{pmatrix} + \begin{pmatrix} 376 \\ -1 \end{pmatrix}$$

$$\begin{pmatrix} 529 \\ 1 \end{pmatrix} = \begin{pmatrix} 376 \\ -1 \end{pmatrix} + \begin{pmatrix} 153 \\ 2 \end{pmatrix}$$

$$\begin{pmatrix} 376 \\ -1 \end{pmatrix} = 2 \cdot \begin{pmatrix} 153 \\ 2 \end{pmatrix} + \begin{pmatrix} 70 \\ -5 \end{pmatrix}$$

$$\begin{pmatrix} 153 \\ 2 \end{pmatrix} = 2 \cdot \begin{pmatrix} 70 \\ -5 \end{pmatrix} + \begin{pmatrix} 13 \\ 12 \end{pmatrix}$$

- we want to compute the fraction corresponding to $529 \bmod 905$

$$\begin{pmatrix} 905 \\ 0 \end{pmatrix} = \begin{pmatrix} 529 \\ 1 \end{pmatrix} + \begin{pmatrix} 376 \\ -1 \end{pmatrix}$$

$$\begin{pmatrix} 529 \\ 1 \end{pmatrix} = \begin{pmatrix} 376 \\ -1 \end{pmatrix} + \begin{pmatrix} 153 \\ 2 \end{pmatrix}$$

$$\begin{pmatrix} 376 \\ -1 \end{pmatrix} = 2 \cdot \begin{pmatrix} 153 \\ 2 \end{pmatrix} + \begin{pmatrix} 70 \\ -5 \end{pmatrix}$$

$$\begin{pmatrix} 153 \\ 2 \end{pmatrix} = 2 \cdot \begin{pmatrix} 70 \\ -5 \end{pmatrix} + \begin{pmatrix} 13 \\ 12 \end{pmatrix}$$

- we stop because $2 \cdot 13^2 < 905$

Primes are available in SINGULAR

Primes up to:

- 1985 (8 bit) : 251
- we used usually 181

Primes are available in SINGULAR

Primes up to:

- 1985 (8 bit) : 251
 - we used usually 181
- 1995 (16 bit): 32003
 - Macaulay used 31991

Primes are available in SINGULAR

Primes up to:

- 1985 (8 bit) : 251
 - we used usually 181
- 1995 (16 bit): 32003
 - Macaulay used 31991
- 2005 (32 bit): 2147483647

- Let N be the product of all primes smaller than 2^{32}

- Let N be the product of all primes smaller than 2^{32}

- let

$$I = \langle v + w + x + y + z, vw + wx + xy + yz + vz, vwx + wxy + xyz + vyz + vwz, vwx + wxy + xyz + vyz + vwz, vwx + wxy + xyz + vyz + vwz, vwx + wxy + xyz + vyz + vwz, vwx + wxy + xyz + vyz + vwz, vwx + wxy + xyz + vyz + vwz \rangle \subseteq \mathbb{Q}[v, w, x, y, z].$$

Then MAGMA V2.16–11 (64-bit version) computes a wrong Gröbner basis, in particular it computes the Gröbner basis of the ideal

$$J = \langle v + w + x + y + z, vw + wx + xy + yz + vz, vwx + wxy + xyz + vyz + vwz, vwx + wxy + xyz + vyz + vwz, vwx + wxy + xyz + vyz + vwz, vwx + wxy + xyz + vyz + vwz, vwx + wxy + xyz + vyz + vwz \rangle \subseteq \mathbb{Q}[v, w, x, y, z]$$

which obviously differs from I