A Problem in Group Theory

Gerhard Pfister

pfister@mathematik.uni-kl.de

Departement of Mathematics

University of Kaiserslautern

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

Computeralgebra and finite Groups

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

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**)

  $v_1 := [x, y] = xyx^{-1}y^{-1}$ (commutator)
  $v_{n+1} := [v_n, y]$

nilpotent groups

Let G be a finite group

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

Let $G^{(i)} := [G^{(i-1)}, G]$, then G is called nilpotent, if $G^{(m)} = \{e\}$ for a suitable m.

nilpotent groups

Let G be a finite group

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

Let $G^{(i)} := [G^{(i-1)}, G]$, then G is called nilpotent, if $G^{(m)} = \{e\}$ for a suitable m.

- abelian groups are nilpotent.
- if the order of the group is a power of a prime it is nilpotent.
- G ist nilpotent $\Leftrightarrow$ it is the direct product of its Sylow groups.
- S_3 is not nilpotent.

solvable groups

Let

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

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

solvable groups

Let

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

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.

Main result

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 $U_n(x, y) = 1 \; \forall\, x, y \in G$.

Main result

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 $U_n(x, y) = 1\ \forall\, x, y \in G$.

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

Proof

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

Proof

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:

Proof

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

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

Proof

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

Proof

Technische Universität Kaiserslautern

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**$(3, \mathbb{F}_3)$

Proof

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.

Proof

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.

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

Motivation of the choice of the word

Let w be a word in X, Y, X^{-1}, Y^{-1} and

$$U_1 = w$$
$$U_{n+1} = [XU_nX^{-1}, YU_nY^{-1}].$$

Motivation of the choice of the word

Let w be a word in X, Y, X^{-1}, Y^{-1} and

$$U_1 = w$$
$$U_{n+1} = [XU_nX^{-1}, YU_nY^{-1}].$$

A Computer–search through the 10,000 shortest words in X, X^{-1}, Y, Y^{-1} found the following four words such that the equation $U_1 = U_2$ has a non-trivial solution in $\mathrm{PSL}(2, p)$ for all $p < 1000$:

$$w_1 = X^{-2}Y^{-1}X$$
$$w_2 = X^{-1}YXY^{-1}X$$
$$w_3 = Y^{-2}X^{-1}$$
$$w_4 = XY^{-2}X^{-1}YX^{-1}$$

PSL

$$\mathsf{PSL}(2,K) = \mathsf{SL}(2,K) / \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \;\middle|\; a^2 = 1 \right\}$$

PSL

$$\mathsf{PSL}(2,K) = \mathsf{SL}(2,K)/\left\{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \;\middle|\; a^2 = 1\right\}$$

especially

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

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

PSL

$$\mathsf{PSL}(2,K) = \mathsf{SL}(2,K)/\left\{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \;\middle|\; a^2 = 1\right\}$$

especially

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

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

It holds:

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

Translation to algebraic Geometry

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Let us consider $G = \textsf{PSL}(\mathbf{2}, \mathbb{F}_{\boldsymbol{p}}),\ \mathbf{p} \geq \mathbf{5}$

Translation to algebraic Geometry

Let us consider $G = \textbf{PSL}(\mathbf{2}, \mathbb{F}_{\boldsymbol{p}}),\ \mathbf{p} \geq \mathbf{5}$

Consider the matrices

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

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

Translation to algebraic Geometry

Let us consider $G = \textbf{PSL}(\mathbf{2}, \mathbb{F}_{\boldsymbol{p}}),\ \mathbf{p} \geq \mathbf{5}$

Consider the matrices

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

$x^{-1} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & t \end{smallmatrix}\right)$ 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 equations

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

$$\begin{aligned}
p_1 = \quad & b^3c^2t^2 + b^2c^2t^3 - b^2c^2t^2 - bc^2t^3 - b^3ct + b^2c^2t + b^2ct^2 + 2bc^2t^2 \\
& +bct^3 + b^2c^2 + b^2ct + bc^2t - bct^2 - c^2t^2 - ct^3 - b^2t + bct + c^2t \\
& +ct^2 + 2bc + c^2 + bt +^2 ct + c + 1 \\
p_2 = \quad & -b^3ct^2 - b^2ct^3 + b^2c^2t + bc^2t^2 + b^3t - b^2ct - 2bct^2 - b^2c + bct \\
& +c^2t + ct^2 - bt - ct - b - c - 1 \\
p_3 = \quad & b^3c^3t^2 + b^2c^3t^3 - b^2c^2t^3 - bc^2t^4 - b^3c^2t + b^2c^3t +^2 b^2c^2t^2 \\
& +2bc^3t^2 +^2 bc^2t^3 + b^2c^2t +^2 b^2ct^2 + bc^2t^2 - c^2t^3 - ct^4 - 2b^2ct \\
& +bc^2t + c^3t + bct^2 + 2c^2t^2 + ct^3 - b^2c - b^2t + bct + c^2t + bt^2 \\
& +3ct^2 + bc - bt - b - c + 1 \\
p_4 = \quad & -b^3c^2t^2 - b^2c^2t^3 + b^2c^2t^2 + bc^2t^3 + b^3ct - b^2c^2t - b^2ct^2 - 2bc^2t^2 \\
& -bct^3 - 2b^2ct + c^2t^2 + ct^3 + b^2t - bct - c^2t - ct^2 + b^2 - bt \\
& -2ct - b - t + 1
\end{aligned}$$

Hasse–Weil–Theorem

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

Hasse–Weil–Theorem

Theorem von Hasse–Weil (generalized by Aubry and Perret for singulare 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 = degree, p_a = arithmetic genus of $\overline{C}$).

Hasse–Weil–Theorem

Theorem von Hasse–Weil (generalized by Aubry and Perret for singulare 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 = degree, p_a = 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 $H(t) = 10t - 11 \Rightarrow d = 10$, $p_a = 12$.

Hasse–Weil–Theorem

Theorem von Hasse–Weil (generalized by Aubry and Perret for singulare 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 = degree, p_a = 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.

absolute irreduciblity

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

absolute irreducibliy

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

Using **SINGULAR** we show:

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

absolute irreduciblity

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

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

Using **SINGULAR** we show:

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

$$\begin{aligned}
f_1 = \quad & t^2 b^4 + (t^4 - 2t^3 - 2t^2)b^3 - (t^5 - 2t^4 - t^2 - 2t - 1)b^2 \\
& -(t^5 - 4t^4 + t^3 + 6t^2 + 2t)b + (t^4 - 4t^3 + 2t^2 + 4t + 1) \\
f_2 = \quad & (t^3 - 2t^2 - t)c + t^2 b^3 + (t^4 - 2t^3 - 2t^2)b^2 \\
& -(t^5 - 2t^4 - t^2 - 2t - 1)b - (t^5 - 4t^4 + t^3 + 6t^2 + 2t) \\
h = \quad & t^3 - 2t^2 - t
\end{aligned}$$

We give explicitely matrices M and N with entries in $\mathbb{Z}[b, c, t]$ such

that $M \begin{pmatrix} p_1 \\ \vdots \\ p_4 \end{pmatrix} = \begin{pmatrix} f_1 \\ f_2 \end{pmatrix}$ and $N \begin{pmatrix} f_1 \\ f_2 \end{pmatrix} = \begin{pmatrix} h^2 p_1 \\ \vdots \\ h^2 p_4 \end{pmatrix}$

We give explicitely matrices M and N with entries in $\mathbb{Z}[b,c,t]$ such

that $M\begin{pmatrix} p_1 \\ \vdots \\ p_4 \end{pmatrix} = \begin{pmatrix} f_1 \\ f_2 \end{pmatrix}$ and $N\begin{pmatrix} f_1 \\ f_2 \end{pmatrix} = \begin{pmatrix} h^2 p_1 \\ \vdots \\ h^2 p_4 \end{pmatrix}$

We obtain for all fields K

$$IK[b,c,t] = \big(\langle f_1, f_2\rangle K[b,c,t]\big) : h^2 \,.$$

Schritt 2

f_2 is linear in c , it is enough to show, that f_1 is absolutely irreducibel.

Schritt 2

f_2 is linear in c , it is enough to show, that f_1 is absolutely irreducibel.

algebraically the following is equivalent:

- $IK[b, c, t]$ is prime
- $\langle f_1, f_2 \rangle K(t)[b, c]$ prime
- f_1 irreducibel in $K(t)[b]$ resp. in $K[t, b]$.

Schritt 2

f_2 is linear in c , it is enough to show, that f_1 is absolutely irreducibel.

algebraically the following is equivalent:

- $IK[b, c, t]$ is prime
- $\langle f_1, f_2 \rangle K(t)[b, c]$ prime
- f_1 irreducibel in $K(t)[b]$ resp. in $K[t, b]$.

geometrically:
Curve $V(I)$ is irreducibel, if the projection to the b, t–plane is irreducibel.

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 irreducibel for all primes $p \geq 2$.
(Using the lemma of Gauß this is equivalent to P being irreducibel in $\overline{\mathbb{F}}_p(t)[x]$.)

Ansatz

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

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 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 $1 \in$ 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 $\mathbb{Z}\big[\{a(i)\},\ \{b(i)\},\ \{g(i)\},\ \{d(i)\}\big]$

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

Suzuki groups

This case is much more complicated.

We have to prove that on a surface U any odd power of a certain endomorphism θ has fixed points.

Suzuki groups

Technische Universität Kaiserslautern

This case is much more complicated.
We have to prove that on a surface U any odd power of a certain endomorphism θ has fixed points.
Here we use the **Lefschetz–Weil–Grothendieck trace formulae** generalized by Deligne–Lusztig, Th. Zink, Pink, Katz and Adolphson–Sperber:

$$2^n - b_1(U) \cdot 2^{\frac{3}{4}n} - b_2(U) \cdot 2^{\frac{1}{2}n} \leq \#\,\text{Fix}\,(\theta^n, U)$$

for n sufficientely large.