A search for (positive) polynomial identities in groups

M. Farrokhi D. G.

IASBS

May 29, 2018

What is a polynomial identity?

A polynomial in $x_1, \ldots, x_n$ with coefficients in a group G is any element of $G * F(x_1, \ldots, x_n)$, that is, a word

$$g_1 x_{i_{1,1}}^{e_{1,1}} \ldots x_{i_{1,n_1}}^{e_{1,n_1}} \cdot \ldots \cdot g_m x_{i_{m,1}}^{e_{m,1}} \ldots x_{i_{m,n_m}}^{e_{m,n_m}} g_{m+1}.$$

The above polynomial is positive if all $e_{i,j}$ are non-negative.

What is a polynomial identity?

A typical <u>one-variable</u> polynomial is given as

$$p(x) = g_1 x^{n_1} \cdot \ldots \cdot g_m x^{n_m} g_{m+1},$$

which can be rewritten as

$$p(x) = x^{g'_1} \cdots x^{g'_n} g'_{n+1}$$

for some $g'_1, \ldots, g'_{n+1} \in G$.

What is a polynomial identity?

A typical <u>one-variable</u> polynomial is given as

$$p(x) = g_1 x^{n_1} \cdot \ldots \cdot g_m x^{n_m} g_{m+1},$$

which can be rewritten as

$$p(x) = x^{g'_1} \cdots x^{g'_n} g'_{n+1}$$

for some $g'_1, \ldots, g'_{n+1} \in G$.

The polynomial identity $p(x) = 1$ holds in G only if $g'_{n+1} = 1$, i.e.

$$x^{g'_1} \cdots x^{g'_n} = 1$$

for all $x \in G$.

Main problems

Problem

Compute the shortest positive polynomial identity a given group satisfies.

Main problems

Problem

Compute the shortest positive polynomial identity a given group satisfies.

Question

What information one can infer if a group satisfies a given positive polynomial identity?

Origins

William Burnside (1852–1927)

The Theory of Groups of Finite Order, Cambridge University Press, 1897.

The Theory of Groups of Finite Order, Second Edition, Cambridge University Press, 1911.

Burnside problem: General case

General Burnside Problem

Is every finitely generated periodic group finite?

Burnside problem: General case

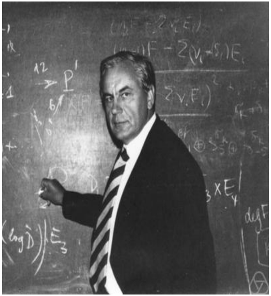
General Burnside Problem

Is every finitely generated periodic group finite?

Theorem (E. Golod and I. R. Shafarevich, 1964)

There exists an infinite three-generator p-group for all primes p.

Evgeny Golod (1935–2018)



Igor R. Shafarvich (1923–2017)

Burnside problem: Bounded case

Bounded Burnside Problem

Is every finitely generated group of a given exponent finite?

Burnside problem: Bounded case

Bounded Burnside Problem

Is every finitely generated group of a given exponent finite?

Free Burnside group of rank m and exponent n:

$$B(m, n) := \frac{F(x_1, \ldots, x_m)}{F(x_1, \ldots, x_m)^n}.$$

Burnside problem: Bounded case

Bounded Burnside Problem

Is every finitely generated group of a given exponent finite?

Free Burnside group of rank m and exponent n:

$$B(m, n) := \frac{F(x_1, \ldots, x_m)}{F(x_1, \ldots, x_m)^n}.$$

Trivial cases

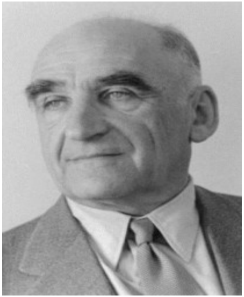
1. $B(1, n) \cong C_n$;
2. $B(m, 1) \cong 1$;
3. $B(m, 2) \cong C_2^m$.

Burnside problem: Bounded case

Theorem (F. W. Levi and B. L. van der Warden, 1932)

The group $B(m,3)$ is a finite 3-group of order

$$3^{m+\binom{m}{2}+\binom{m}{3}}.$$



Friedrich W. Levi (1888–1966)

Bartel L. van der Waerden (1903–1996)

Burnside problem: Bounded case

Theorem (I. N. Sanov, 1940)

The group $B(m, 4)$ is a finite 2-group. The exact order is still unknown!

Burnside problem: Bounded case

Theorem (I. N. Sanov, 1940)

The group $B(m,4)$ is a finite 2-group. The exact order is still unknown!

m	$\lvert B(m,4)\rvert$	Discoveres
1	2^2	
2	2^{12}	J. J. Tobin, 1954
3	2^{69}	A. J. Bayes, J. Kautsky, and J. W. Wamsley, 1974
4	2^{422}	G. Havas and M. F. Newman, 1980
5	2^{2728}	E. O'Brien and M. F. Newman, 1996

Burnside problem: Bounded case

Theorem (M. Hall, 1958)

The group $B(m,6)$ is a finite group of order

$$2^{1+(m-1)3^{m+\binom{m}{2}+\binom{m}{3}}}3^{r+\binom{r}{2}+\binom{r}{3}},$$

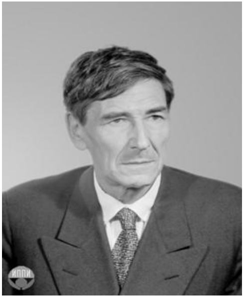
where $r = 1+(m-1)2^m$.

Marshal Hall (1910–1990)

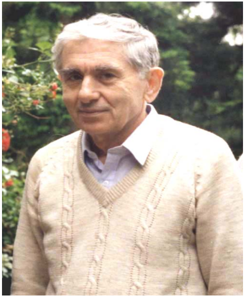
Burnside problem: Bounded case

Theorem (P. Novikov and S. Adian, 1968)

There exist infinite finitely generated groups of exponent n for every odd $n > \cancel{4381}.$ 665



Pyotr S. Novikovch (1901–1975)



Sergei Adian (1931–2020)

Burnside problem: Bounded case

Theorem (S. V. Ivanov, 1994 (308 pages))

The group $B(m,n)$ $(m>1)$ is infinite for all even $n \geqslant \cancel{2^{48}}^{\,8000}$.

Burnside problem: Bounded case

Theorem (S. V. Ivanov, 1994 (308 pages))

The group $B(m,n)$ $(m > 1)$ is infinite for all even $n \geqslant \cancel{2^{48}}$. 8000

Theorem (I. G. Lysënok, 1996 (222 pages))

The group $B(m,n)$ $(m > 1)$ is infinite for all even $n \geqslant 8000$.

Burnside problem: Bounded case

Theorem (A. Yu Ol'shanskii, 1982)

There exists a Tarski monster p-group for all prime $p > 10^{75}$, that is, a finitely generated infinite p-group whose all nontrivial proper subgroups are cyclic of order p.

Alexander Yu. Ol'shanskii

Burnside problem: Restericted case

Restricted Burnside Problem

Are there only finitely many finite groups with m generators of exponent n?

Burnside problem: Resetricted case

Restricted Burnside Problem

Are there only finitely many finite groups with m generators of exponent n?

Let

$$B_0(m,n) = \frac{B(m,n)}{\bigcap\limits_{\substack{H \leqslant B(m,n) \\ f.i.}} H}.$$

Burnside problem: Resterícted case

Restricted Burnside Problem

Are there only finitely many finite groups with m generators of exponent n?

Let

$$B_0(m,n) = \frac{B(m,n)}{\bigcap\limits_{\substack{H \leqslant B(m,n) \\ f.i.}} H}.$$

The Restricted Burnside Problem is true if $B_0(m,n)$ is finite.

Burnside problem: Resterected case

Theorem (A. I. Kostrikin, 1986 (232 pages))

The resterected Burnside problem is true for all prime exponents.

Alexei I. Kostrikin (1929–2000)

Burnside problem: Resterícted case

Theorem (E. I. Zelmanov, 1990)

The resterícted Burnside problem is true for all exponents.

Effim I. Zelmanov (1955–)
Fields Medal in 1994

Burnside problem: ResterictED case (a related result)

Conjecture (W. Burnside)

Every finite group of odd exponent is solvable.

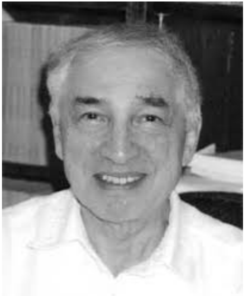
Burnside problem: Resterícted case (a related result)

Conjecture (W. Burnside)

Every finite group of odd exponent is solvable.

Theorem (W. Feit and J. G. Thompson, 1963 (254 pages))

Every finite group of odd exponents is solvable.



Walter Feit (1930–2004)

Burnside problem: Restericted case (a related result)

John G. Thompson (1932–)

Cole Prize (1965)
Fields Medal (1970)
Fellow of the Royal Society (1979)
Senior Berwick Prize (1982)
Sylvester Medal (1985)
Wolf Prize (1992)
Médaille Poincaré (1992)
National Medal of Science (2000)
Abel Prize (2008)
De Morgan Medal (2013)

Another important identity

Theorem (J. G. Thompson, 1959)

Finite groups with fixed-point-free automorphisms of prime order are nilpotent.

Another important identity

Theorem (J. G. Thompson, 1959)

Finite groups with fixed-point-free automorphisms of prime order are nilpotent.

Every fixed-point-free automorphism θ of a group G is split, that is,

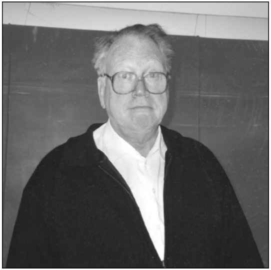
$$xx^{\theta} \cdots x^{\theta^{n-1}} = 1$$

for all $x \in G$, where n is the order of θ.

Another important identity

Theorem (O. H. Kegel, 1961)

Finite groups with split automorphisms of prime order are nilpotent.



Otto H. Kegel (1934–)

The generalized exponent of groups

Let A be a group of automorphisms of a group G. Then the generalized exponent $\mathrm{gexp}(G, A)$ of G with respect to A is the minimum number n for which G satisfies the identity

$$x^{\alpha_1} \cdots x^{\alpha_n} = 1$$

for some $\alpha_1, \ldots \alpha_n \in A$.

The generalized exponent $\mathrm{gexp}(G)$ of G is defined as

$$\mathrm{gexp}(G) := \mathrm{gexp}(G, G).$$

Examples

Examples

1. Abelian groups and p-groups of exponent p:

$$x^{\exp(G)} = 1 \quad \text{and} \quad \mathrm{gexp}(G) = \exp(G).$$

Examples

1. Abelian groups and p-groups of exponent p:

$$x^{\exp(G)} = 1 \quad \text{and} \quad \mathrm{gexp}(G) = \exp(G).$$

2. Groups with a cyclic subgroup of index two:
   - Dihedral groups $D_{2n} = \langle a, b : a^n = b^2 = 1, a^b = a^{-1} \rangle$,
   - Quaternion groups $Q_{4n} = \langle a, b : a^n = 1, a^{2^{n-2}} = b^2, a^b = a^{-1} \rangle$,
   - Quasidihedral groups $QD_{2^n} = \langle a, b : a^{2^{n-1}} = b^2 = 1, a^b = a^{2^{n-2}-1} \rangle$,

$$x^2 x^{2b} = 1 \quad \text{and} \quad \mathrm{gexp}(G) = 4.$$

Examples

1. Abelian groups and p-groups of exponent p:

$$x^{\exp(G)} = 1 \quad \text{and} \quad \mathrm{gexp}(G) = \exp(G).$$

2. Groups with a cyclic subgroup of index two:
   - Dihedral groups $D_{2n} = \langle a, b : a^n = b^2 = 1, a^b = a^{-1} \rangle$,
   - Quaternion groups $Q_{4n} = \langle a, b : a^n = 1, a^{2^{n-2}} = b^2, a^b = a^{-1} \rangle$,
   - Quasidihedral groups $QD_{2^n} = \langle a, b : a^{2^{n-1}} = b^2 = 1, a^b = a^{2^{n-2}-1} \rangle$,

$$x^2 x^{2b} = 1 \quad \text{and} \quad \mathrm{gexp}(G) = 4.$$

3. Symmetric group S_4:

$$x^2 x^{(1\ 2\ 3)} x^2 x^{(1\ 2\ 3)} = 1 \quad \text{and} \quad \mathrm{gexp}(S_4) = 6.$$

Examples

4. $G = \langle a, b : a^{2b} = a^{-2}, b^{2a} = b^{-2} \rangle$ (Čurin, 1973):

$$x^2 x^{2a} x^{2b} x^{2ab} = 1 \quad \text{and} \quad \mathrm{gexp}(G) = 8.$$

Examples

4. $G = \langle a, b : a^{2b} = a^{-2}, b^{2a} = b^{-2} \rangle$ (Čurin, 1973):

$$x^2 x^{2a} x^{2b} x^{2ab} = 1 \quad \text{and} \quad \mathrm{gexp}(G) = 8.$$

5. $G = \langle a, b : a^{125} = b^5 = [a, b, a] = 1, [a, b, b] = a^{25} \rangle$:

$$x^{b^3} x^b x^2 x^b x^5 = 1 \quad \text{and} \quad \mathrm{gexp}(G) = 10.$$

Examples

4 $G = \langle a, b : a^{2b} = a^{-2}, b^{2a} = b^{-2} \rangle$ (Čurin, 1973):

$$x^2 x^{2a} x^{2b} x^{2ab} = 1 \quad \text{and} \quad \mathrm{gexp}(G) = 8.$$

5 $G = \langle a, b : a^{125} = b^5 = [a, b, a] = 1, [a, b, b] = a^{25} \rangle$:

$$x^{b^3} x^b x^2 x^b x^5 = 1 \quad \text{and} \quad \mathrm{gexp}(G) = 10.$$

6 $G = \langle a, b : a^{p^{m-2}} = b^p = [a, b, a] = 1, [a, b, b] = a^{rp^{m-3}} \rangle$ ($p^m > 3^4$ and r is a quadratic non-residue modulo p):

$$\underbrace{x^{b^{\alpha+2\beta}} x^{b^{-2\alpha-3\beta}} x^{b^{\alpha}} x^{b^{\beta}} x^{p^{m-3}-4} = 1}_{3\alpha^2+8\alpha\beta+7\beta^2 \equiv -r^{-1} \pmod{p}} \quad \text{and} \quad \mathrm{gexp}(G) = p^{m-3}.$$

Conversion rules

An identity $x^{g_1} \cdots x^{g_n} = 1$ in a group G can be converted to

1. $x^{g_n} \cdots x^{g_1} = 1$;
   Apply $x \longmapsto x^{-1}$ and inversion, respectively

Conversion rules

An identity $x^{g_1} \cdots x^{g_n} = 1$ in a group G can be converted to

1. $x^{g_n} \cdots x^{g_1} = 1$;
   Apply $x \longmapsto x^{-1}$ and inversion, respectively
2. $x^{g g_1} \cdots x^{g g_n} = 1$, for all $g \in G$;
   Apply $x \longmapsto x^g$

Conversion rules

An identity $x^{g_1} \cdots x^{g_n} = 1$ in a group G can be converted to

1. $x^{g_n} \cdots x^{g_1} = 1$;
   Apply $x \longmapsto x^{-1}$ and inversion, respectively
2. $x^{g g_1} \cdots x^{g g_n} = 1$, for all $g \in G$;
   Apply $x \longmapsto x^{g}$
3. $x^{g_1 g} \cdots x^{g_n g} = 1$, for all $g \in G$;
   Apply conjugation by g

Conversion rules

An identity $x^{g_1} \cdots x^{g_n} = 1$ in a group G can be converted to

1. $x^{g_n} \cdots x^{g_1} = 1$;
   Apply $x \longmapsto x^{-1}$ and inversion, respectively
2. $x^{gg_1} \cdots x^{gg_n} = 1$, for all $g \in G$;
   Apply $x \longmapsto x^g$
3. $x^{g_1 g} \cdots x^{g_n g} = 1$, for all $g \in G$;
   Apply conjugation by g
4. $x^{g_1^g} \cdots x^{g_n^g} = 1$, for all $g \in G$;
   Apply (2) with g^{-1} and (3) with g, respectively

Conversion rules

An identity $x^{g_1} \cdots x^{g_n} = 1$ in a group G can be converted to

1. $x^{g_n} \cdots x^{g_1} = 1$;
   Apply $x \longmapsto x^{-1}$ and inversion, respectively
2. $x^{gg_1} \cdots x^{gg_n} = 1$, for all $g \in G$;
   Apply $x \longmapsto x^{g}$
3. $x^{g_1 g} \cdots x^{g_n g} = 1$, for all $g \in G$;
   Apply conjugation by g
4. $x^{g_1^g} \cdots x^{g_n^g} = 1$, for all $g \in G$;
   Apply (2) with g^{-1} and (3) with g, respectively
5. $x^{g_1^\theta} \cdots x^{g_n^\theta} = 1$, for all $\theta \in \mathrm{Aut}(G)$;
   Apply $x \longmapsto x^{\theta^{-1}}$ and θ, respectively

Conversion rules

6. $xx^{g_2'} \cdots x^{g_n'} = 1$, where $g_i' = g_1^{-1} g_i$ for $i = 2, \ldots, n$;
Apply (2) with $g = g_1^{-1}$

[1] G. Endimioni, On certain classes of generalized periodic groups, *Ischia Group Theory* (2006), 93–102, World Sci. Publ., Hackensack, NJ, 2007.

Conversion rules

6. $xx^{g_2'}\cdots x^{g_n'} = 1$, where $g_i' = g_1^{-1}g_i$ for $i = 2, \ldots, n$;
   Apply (2) with $g = g_1^{-1}$
7. $x^2x^{g_3''}\cdots x^{g_n''} = 1$, where

$$g_i'' = (g_ig_{i-1}^{-1}g_2^{-1})\cdots(g_3g_2^{-1}g_2^{-1}),$$

for all $i = 3, \ldots, n$ (G. Endimioni[1]);
Apply $x \longmapsto xg_2'$ and collect, respectively

[1] G. Endimioni, On certain classes of generalized periodic groups, *Ischia Group Theory* (2006), 93–102, World Sci. Publ., Hackensack, NJ, 2007.

Conversion rules

6. $xx^{g_2'} \cdots x^{g_n'} = 1$, where $g_i' = g_1^{-1} g_i$ for $i = 2, \ldots, n$;
   Apply (2) with $g = g_1^{-1}$
7. $x^2 x^{g_3''} \cdots x^{g_n''} = 1$, where

   $$g_i'' = (g_i g_{i-1}^{-1} g_2^{-1}) \cdots (g_3 g_2^{-1} g_2^{-1}),$$

   for all $i = 3, \ldots, n$ (G. Endimioni[1]);
   Apply $x \longmapsto x g_2'$ and collect, respectively
8. $x^{g_1} x^{g_2 y^{g_1}} \cdots x^{g_n y^{g_{n-1}} \cdots y^{g_1}} = 1$, for all $y \in G$.
   Apply (1), $x \longmapsto yx$, collect, and (1), respectively

[1] G. Endimioni, On certain classes of generalized periodic groups, *Ischia Group Theory* (2006), 93–102, World Sci. Publ., Hackensack, NJ, 2007.

Groups with small generalized exponents

Theorem (Endimioni[1])

Let G be a group of generalized exponent 3. Then

[1] G. Endimioni, On certain classes of generalized periodic groups, *Ischia Group Theory* (2006), 93–102, World Sci. Publ., Hackensack, NJ, 2007.

Groups with small generalized exponents

Theorem (Endimioni[1])

Let G be a group of generalized exponent 3. Then

(1) *G is 3-abelian, i.e. $(ab)^3 = a^3 b^3$, for all $a, b \in G$);*

[1] G. Endimioni, On certain classes of generalized periodic groups, *Ischia Group Theory* (2006), 93–102, World Sci. Publ., Hackensack, NJ, 2007.

Groups with small generalized exponents

Theorem (Endimioni[1])

Let G be a group of generalized exponent 3. Then

(1) *G is 3-abelian, i.e. $(ab)^3 = a^3b^3$, for all $a, b \in G$);*

(2) *$G^3 \subseteq Z(G)$;*

[1] G. Endimioni, On certain classes of generalized periodic groups, *Ischia Group Theory* (2006), 93–102, World Sci. Publ., Hackensack, NJ, 2007.

Groups with small generalized exponents

Theorem (Endimioni[1])

Let G be a group of generalized exponent 3. Then

(1) *G is 3-abelian, i.e. $(ab)^3 = a^3b^3$, for all $a, b \in G$);*

(2) *$G^3 \subseteq Z(G)$;*

(3) *the exponent of G divides 9;*

[1] G. Endimioni, On certain classes of generalized periodic groups, *Ischia Group Theory* (2006), 93–102, World Sci. Publ., Hackensack, NJ, 2007.

Groups with small generalized exponents

Theorem (Endimioni[1])

Let G be a group of generalized exponent 3. Then

(1) *G is 3-abelian, i.e. $(ab)^3 = a^3b^3$, for all $a, b \in G$);*

(2) *$G^3 \subseteq Z(G)$;*

(3) *the exponent of G divides 9;*

(4) *G is nilpotent of class at most 3.*

[1] G. Endimioni, On certain classes of generalized periodic groups, *Ischia Group Theory* (2006), 93–102, World Sci. Publ., Hackensack, NJ, 2007.

Groups with small generalized exponents

Theorem (Endimioni[1])

Let G be a group of generalized exponent 3. Then

(1) *G is 3-abelian, i.e. $(ab)^3 = a^3b^3$, for all $a, b \in G$);*

(2) *$G^3 \subseteq Z(G)$;*

(3) *the exponent of G divides 9;*

(4) *G is nilpotent of class at most 3.*

Theorem (Endimioni[1])

Let G be a group of generalized exponent 4. Then

[1] G. Endimioni, On certain classes of generalized periodic groups, *Ischia Group Theory* (2006), 93–102, World Sci. Publ., Hackensack, NJ, 2007.

Groups with small generalized exponents

Theorem (Endimioni[1])

Let G be a group of generalized exponent 3. Then

(1) *G is 3-abelian, i.e. $(ab)^3 = a^3 b^3$, for all $a, b \in G$);*

(2) *$G^3 \subseteq Z(G)$;*

(3) *the exponent of G divides 9;*

(4) *G is nilpotent of class at most 3.*

Theorem (Endimioni[1])

Let G be a group of generalized exponent 4. Then

(1) *G^4 is nilpotent of class $\leqslant 2$;*

[1] G. Endimioni, On certain classes of generalized periodic groups, *Ischia Group Theory* (2006), 93–102, World Sci. Publ., Hackensack, NJ, 2007.

Groups with small generalized exponents

Theorem (Endimioni[1])

Let G be a group of generalized exponent 3. Then

(1) *G is 3-abelian, i.e. $(ab)^3 = a^3 b^3$, for all $a, b \in G$);*

(2) *$G^3 \subseteq Z(G)$;*

(3) *the exponent of G divides 9;*

(4) *G is nilpotent of class at most 3.*

Theorem (Endimioni[1])

Let G be a group of generalized exponent 4. Then

(1) *G^4 is nilpotent of class $\leqslant 2$;*

(2) *G^8 is abelian.*

[1] G. Endimioni, On certain classes of generalized periodic groups, *Ischia Group Theory* (2006), 93–102, World Sci. Publ., Hackensack, NJ, 2007.

Some general results

Theorem

Let $G = H \rtimes K$ *be a finite group. Then*

$$\mathrm{gexp}(G) \leqslant \exp(K) \cdot \mathrm{gexp}(H, K).$$

Theorem

Let $G = H \rtimes K$ be a finite group. Then

$$\mathrm{gexp}(G) \leqslant \exp(K) \cdot \mathrm{gexp}(H, K).$$

Theorem

Assume $G = H \rtimes K$ is a finite group, in which H is a minimal normal Sylow p-subgroup and K is a Sylow q-subgroup of G. Then

$$\mathrm{gexp}(G) \geqslant \exp(Z(K)) \cdot \mathrm{gexp}(H, K).$$

Proof

1. Let $n = \mathrm{gexp}(G) = q^e m$, where $m \geqslant 1$ and $q^e = \exp(Z(K))$.

Proof

1. Let $n = \mathrm{gexp}(G) = q^e m$, where $m \geqslant 1$ and $q^e = \exp(Z(K))$.
2. The group G satisfies $x^{g_1} \dots x^{g_n} = 1$ for some $g_1, \dots, g_n \in G$.

Proof

1. Let $n = \mathrm{gexp}(G) = q^e m$, where $m \geqslant 1$ and $q^e = \exp(Z(K))$.
2. The group G satisfies $x^{g_1} \dots x^{g_n} = 1$ for some $g_1, \dots, g_n \in G$.
3. Le $g_i = h_i k_i$ for $i = 1, \dots, n$, in which $h_i \in H$ and $k_i \in K$.

Proof

1. Let $n = \mathrm{gexp}(G) = q^e m$, where $m \geqslant 1$ and $q^e = \exp(Z(K))$.
2. The group G satisfies $x^{g_1} \dots x^{g_n} = 1$ for some $g_1, \dots, g_n \in G$.
3. Le $g_i = h_i k_i$ for $i = 1, \dots, n$, in which $h_i \in H$ and $k_i \in K$.
4. Choose $y \in Z(K)$ with $|y| = q^e$.

Proof

1. Let $n = \mathrm{gexp}(G) = q^e m$, where $m \geqslant 1$ and $q^e = \exp(Z(K))$.
2. The group G satisfies $x^{g_1} \dots x^{g_n} = 1$ for some $g_1, \dots, g_n \in G$.
3. Le $g_i = h_i k_i$ for $i = 1, \dots, n$, in which $h_i \in H$ and $k_i \in K$.
4. Choose $y \in Z(K)$ with $|y| = q^e$.
5. From $(y^i x)^{g_1} \dots (y^i x)^{g_n} = 1$ for $x \in H$ and $i = 0, \dots, q^e - 1$, we get

$$x^{g_1 y^{ig_2} \dots y^{ig_n}} \dots x^{g_{n-1} y^{ig_n}} x^{g_n} = 1,$$

which simplifies to

$$x^{g_1 y^{i(n-1)}} \dots x^{g_{n-1} y^i} x^{g_n} = 1.$$

Proof

6 Let

$$X = \begin{bmatrix} w_1(g_1, \ldots, g_n; x) \\ \vdots \\ w_{q^e}(g_1, \ldots, g_n; x) \end{bmatrix}, \; Y = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ y^{q^e-1} & \cdots & y & 1 \\ \vdots & \ddots & \vdots & \vdots \\ y^{(q^e-1)^2} & \cdots & y^{q^e-1} & 1 \end{bmatrix},$$

and

$$w_i(g_1, \ldots, g_n; x) = x^{g_i} x^{g_{i+q^e}} \ldots x^{g_{i+(m-1)q^e}},$$

for $i = 1, \ldots, q^e$.

Proof

6 Let

$$X = \begin{bmatrix} w_1(g_1,\dots,g_n;x) \\ \vdots \\ w_{q^e}(g_1,\dots,g_n;x) \end{bmatrix}, \ Y = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ y^{q^e-1} & \cdots & y & 1 \\ \vdots & \ddots & \vdots & \vdots \\ y^{(q^e-1)^2} & \cdots & y^{q^e-1} & 1 \end{bmatrix},$$

and

$$w_i(g_1,\dots,g_n;x) = x^{g_i}x^{g_{i+q^e}}\dots x^{g_{i+(m-1)q^e}},$$

for $i = 1,\dots,q^e$.

7 We have $YX = 0$.

Proof

8. Let
$$H_i = \langle w_i(g_1^k, \ldots, g_n^k; h) : h \in H, k \in K \rangle$$
for $i = 1, \ldots, q^e$.

Proof

8 Let

$$H_i = \langle w_i(g_1^k, \ldots, g_n^k; h) : h \in H, k \in K \rangle$$

for $i = 1, \ldots, q^e$.

9 We have $H_i \trianglelefteq G$, hence $H_i = 1$ or H, for $i = 1, \ldots, q$.

Proof

8 Let

$$H_i = \langle w_i(g_1^k, \dots, g_n^k; h) : h \in H, k \in K \rangle$$

for $i = 1, \dots, q^e$.

9 We have $H_i \trianglelefteq G$, hence $H_i = 1$ or H, for $i = 1, \dots, q$.

10 Assume $H_i = H$ for some $i = 1, \dots, q^e$.

Proof

8 Let

$$H_i = \langle w_i(g_1^k, \ldots, g_n^k; h) : h \in H, k \in K \rangle$$

for $i = 1, \ldots, q^e$.

9 We have $H_i \trianglelefteq G$, hence $H_i = 1$ or H, for $i = 1, \ldots, q$.

10 Assume $H_i = H$ for some $i = 1, \ldots, q^e$.

11 Then $\det(Y)X = Y^* YX = 0$ so that $\det(Y) = 0$.

Proof

8 Let

$$H_i = \langle w_i(g_1^k, \dots, g_n^k; h) : h \in H, k \in K \rangle$$

for $i = 1, \dots, q^e$.

9 We have $H_i \trianglelefteq G$, hence $H_i = 1$ or H, for $i = 1, \dots, q$.

10 Assume $H_i = H$ for some $i = 1, \dots, q^e$.

11 Then $\det(Y)X = Y^* YX = 0$ so that $\det(Y) = 0$.

12 On the other hand,

$$\det(Y) = \prod_{0 \leqslant i < j \leqslant q^e - 1} (y^j - y^i) = y^d \prod_{1 \leqslant i \leqslant q^e - 1} (y^i - 1)^{q^e - i}$$

for some d, which yields, as y is non-singular,

$$\prod_{1 \leqslant i \leqslant q^e - 1} (y^i - 1)^{q^e - i} = 0.$$

Proof

12 Let $\delta = \mathrm{lcm}(m \leqslant q^e : \mathrm{gcd}(m, q) = 1)$.

Proof

12 Let $\delta = \mathrm{lcm}(m \leqslant q^e : \mathrm{gcd}(m, q) = 1)$.

13 As
$$\prod_{1 \leqslant i \leqslant q^e - 1} (t^i - 1)^{q^e - i} \,\Big|\, (t^{q^{e-1}\delta} - 1)^{q^e - 1},$$
$y^{q^{e-1}\delta} - 1$ is nilpotent.

Proof

12 Let $\delta = \operatorname{lcm}(m \leqslant q^e : \gcd(m, q) = 1)$.

13 As
$$\prod_{1 \leqslant i \leqslant q^e - 1} (t^i - 1)^{q^e - i} \Big| (t^{q^{e-1}\delta} - 1)^{q^e - 1},$$
$y^{q^{e-1}\delta} - 1$ is nilpotent.

14 Then $y^{q^{e-1}\delta} - 1 = 0$ in $GF(p)\langle y \rangle$, a contradiction.

Proof

12 Let $\delta = \mathrm{lcm}(m \leqslant q^e : \gcd(m, q) = 1)$.

13 As

$$\prod_{1 \leqslant i \leqslant q^e - 1} (t^i - 1)^{q^e - i} \Big| (t^{q^{e-1}\delta} - 1)^{q^e - 1},$$

$y^{q^{e-1}\delta} - 1$ is nilpotent.

14 Then $y^{q^{e-1}\delta} - 1 = 0$ in $GF(p)\langle y \rangle$, a contradiction.

15 Thus $H_i = 1$, hence

$$h^{k_i} h^{k_{i+q^e}} \dots h^{k_{i+(m-1)q^e}} = w_i(k_1, \dots, k_n; h) = 1$$

for $i = 1, \dots, q^e$.

Proof

12 Let $\delta = \operatorname{lcm}(m \leqslant q^e : \gcd(m, q) = 1)$.

13 As
$$\prod_{1 \leqslant i \leqslant q^e - 1} (t^i - 1)^{q^e - i} \Big| (t^{q^{e-1}\delta} - 1)^{q^e - 1},$$
$y^{q^{e-1}\delta} - 1$ is nilpotent.

14 Then $y^{q^{e-1}\delta} - 1 = 0$ in $GF(p)\langle y \rangle$, a contradiction.

15 Thus $H_i = 1$, hence
$$h^{k_i} h^{k_{i+q^e}} \dots h^{k_{i+(m-1)q^e}} = w_i(k_1, \dots, k_n; h) = 1$$
for $i = 1, \dots, q^e$.

16 Therefore, $m \geqslant \operatorname{gexp}(H, K)$ so that $n \geqslant q^e m$.

Some general results

Corollary

Assume $G = H \rtimes K$ is a finite group, in which H is a minimal normal Sylow p-subgroup and K is a Sylow q-subgroup of G. If, in addition, $\exp(K) = \exp(Z(K))$ *then*

$$\mathrm{gexp}(G) = \exp(Z(K)) \cdot \mathrm{gexp}(H, K).$$

Some general results

Corollary

Let G be a minimal Frobenius group. Then

$$\mathrm{gexp}(G) = |H| \cdot \mathrm{gexp}(N, H),$$

in which H and N are a Frobenius complement and the Frobenius kernel of G, respectively.

Moreover, $\mathrm{gexp}(N, H)$ is the minimum coefficient sum among all multiples of the minimal polynomial of a generator of H on N whose coefficients are non-negative integers.

Some general results

Example

Group	Identity	gexp
$A_4 \cong (C_2 \times C_2) \rtimes C_3$	$x^6 = 1$	6
$C_7 \rtimes C_3 = \langle a \rangle \rtimes \langle b \rangle$	$x^{3b^2} x^{3b} x^3 = 1$	9
$C_{11} \rtimes C_5 = \langle a \rangle \rtimes \langle b \rangle$	$x^{b^2} x^{10} = 1$	15

Polynomial identities of prime degree

Theorem

Every finitely generated solvable group satisfying a positive polynomial identity of prime degree p is a finite p-group.

Polynomial identities of prime degree

Theorem

Every finitely generated solvable group satisfying a positive polynomial identity of prime degree p is a finite p-group.

Corollary

A solvable group satisfying a positive polynomial identity of prime degree is a p-group.

Conjecture

The exponent of a finite p-group satisfying a positive generalized identity of degree p is bounded above by p^2.

Conjecture

The exponent of a finite p-group satisfying a positive generalized identity of degree p is bounded above by p^2.

Problem

Is every finite group satisfying a positive generalized identity of prime degree nilpotent?

Conjecture

The exponent of a finite p-group satisfying a positive generalized identity of degree p is bounded above by p^2.

Problem

Is every finite group satisfying a positive generalized identity of prime degree nilpotent?

Problem

Are there only finitely many simple groups that satisfy a positive generalized identity of a given degree n, for every n?

Polynomial identities of prime degree

Proposition

Assume a finite group G satisfies a positive generalized identity

$$x^{g_1} \dots x^{g_p} = 1$$

of prime degree.

Polynomial identities of prime degree

Proposition

Assume a finite group G satisfies a positive generalized identity

$$x^{g_1} \dots x^{g_p} = 1$$

of prime degree. Then

G is solvable if and only if $\langle g_1, \dots, g_p \rangle$ is solvable.

Groups with generalized exponents five

Theorem

Every finite group satisfying a positive generalized identity of prime degree $p \leqslant 5$ is a p-group of exponent dividing p^2.

Groups with generalized exponents five

Theorem

Every finite group satisfying a positive generalized identity of prime degree $p \leqslant 5$ is a p-group of exponent dividing p^2.

Proof.

Assume G satisfies $x^2x^ux^vx^w = 1$. Then $\langle u, v, w\rangle$ is isomorphic to a quotient of the group

$$\langle a, b, c : x^2x^ax^bx^c = x^2x^cx^bx^a = 1,\ x = a, b, c\rangle$$

of order 5^5, hence it is solvable. Thus G is solvable and hence a 5-group. Using HAP, it follows that $\exp(G) \leqslant 25$. $\square$

Positive polynomial identities of non-prime degrees

Let $\mathfrak{B}_n$ denote the class of all groups satisfying a positive polynomial identity of degree n.

Positive polynomial identities of non-prime degrees

Let $\mathfrak{B}_n$ denote the class of all groups satisfying a positive polynomial identity of degree n.

Theorem

The class $\mathfrak{B}_n$ contains an infinite finitely generated solvable group for every non-squarefree natural number n.

Positive polynomial identities of non-prime degrees

Let $\mathfrak{B}_n$ denote the class of all groups satisfying a positive polynomial identity of degree n.

Theorem

The class $\mathfrak{B}_n$ contains an infinite finitely generated solvable group for every non-squarefree natural number n.

Corollary

The class $\mathfrak{B}_n$ contains a finite solvable group of exponent divisible by any given number for every non-squarefree natural number n.

Positive polynomial identities of non-prime degrees

For all $n \geqslant 1$, let

$$\Phi_n(x) := \prod_{\substack{1 \leqslant k \leqslant n \\ \gcd(k,n)=1}} (x - e^{2\pi i \frac{k}{n}})$$

be the nth cyclotomic polynomial.

Notice that $\Phi_n(x)$ is an irreducible polynomial with integer coefficients for all $n \geqslant 1$.

For $n \geqslant 1$, we have

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x).$$

Conjecture

For all distinct primes $p < q < r$, the cyclotomic polynomial $\Phi_{pq}(x)$ has a multiple with non-negative coefficients and coefficient sum r.

Conjecture

For all distinct primes $p < q < r$, the cyclotomic polynomial $\Phi_{pq}(x)$ has a multiple with non-negative coefficients and coefficient sum r.

The following result is true provided that the answer to the above conjecture is positive.

Theorem

The class $\mathfrak{B}_n$ contains a finite solvable group of exponent divisible by any given number for every squarefree natural number n divisible by three distinct primes.

$$\begin{aligned}\Phi_{15}(x) = & x^8 - x^7 + x^5 - x^4 + x^3 - x + 1\\ f(x) = & kx^4 + kx^3 + (k+i)x^2 + kx + k \ (0 \leqslant i \leqslant k)\end{aligned}$$

$$\begin{aligned}\Phi_{21}(x) = & x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1\\ f(x) = & kx^6 + (k+j)x^5 + (k+i)x^4 + (k+i)x^3 + (k+i)x^2\\ & +(k+j)x + k \ (0 \leqslant j \leqslant i,\ j \leqslant k)\end{aligned}$$

$$\begin{aligned}\Phi_{35}(x) = & x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - x^{13} + x^{12}\\ & -x^{11} + x^{10} - x^8 + x^7 - x^6 + x^5 - x + 1\\ f(x) = & kx^6 + (k+j)x^5 + (k+i)x^4 + (k+i)x^3 + (k+i)x^2\\ & +(k+j)x + k \ (0 \leqslant j \leqslant i \leqslant k+j)\end{aligned}$$

Thank You for Your Attention!