Polynomial Identities, Permutational Groups and Rewritable Groups

D. S. Passman

University of Wisconsin–Madison

14th Iranian International Group Theory Conference
Iran University of Science and Technology
Tehran, Iran, February 2022

Finiteness Conditions

This talk concerns three finiteness conditions on groups:

1. PI_n - the polynomial identity property
2. P_n - the permutational property
3. Q_n - the rewritable property

with implications

$$PI_n \Rightarrow P_n \Rightarrow Q_n$$

We will discuss them in chronological order.

Polynomial Identity Algebras

Let K be a field and let

$$\mathcal{F} = K\langle \zeta_1, \zeta_2, \zeta_3, \ldots \rangle$$

be the free K-algebra in the noncommuting variables $\zeta_1, \zeta_2, \zeta_3, \ldots$.
A K-algebra R is said to satisfy the polynomial identity

$$f(\zeta_1, \zeta_2, \ldots, \zeta_k) \in \mathcal{F}$$

if $f(r_1, r_2, \ldots, r_k) = 0$ for all $r_1, r_2, \ldots, r_k \in R$. For example, any commutative algebra satisfies $[\zeta_1, \zeta_2] = \zeta_1\zeta_2 - \zeta_2\zeta_1$. In general, we think of polynomial identities as weakened versions of commutativity. Wagner (1937) observed that if x, y are 2×2 matrices over K then $[x, y]^2$ is a scalar matrix and hence $\mathbf{M}_2(K)$ satisfies $[[x, y]^2, z]$.

Multilinear Identities

The following linearization is due to Kaplansky.

Lemma

If R satisfies a polynomial identity of degree n, then R satisfies a multilinear identity of degree n, namely one of the form

$$f(\zeta_1, \zeta_2, \ldots, \zeta_n) = \sum_{\sigma \in \mathrm{Sym}_n} k_\sigma \, \zeta_{\sigma(1)} \zeta_{\sigma(2)} \cdots \zeta_{\sigma(n)}$$

with $k_\sigma \in K$ and $k_1 = 1$.

If each coefficient k_σ is equal to $(-1)^\sigma$, the sign of σ, then f is the standard identity s_n of degree n and it behaves like the determinant. In particular if two entries are equal, the function vanishes. From this it follows easily that if $\dim_K R = n$, then R satisfies s_{n+1}.

The Amitsur-Levitzki Theorem

For matrix rings, one can do better. Recall that the standard polynomial of degree n is given by

$$s_n(\zeta_1, \zeta_2, \ldots, \zeta_n) = [\zeta_1, \zeta_2, \ldots, \zeta_n]$$

$$= \sum_{\sigma \in \mathrm{Sym}_n} (-1)^\sigma \, \zeta_{\sigma(1)} \zeta_{\sigma(2)} \cdots \zeta_{\sigma(n)}$$

and the result of Amitsur and Levitzki (1950) asserts

Theorem

The matrix ring $\mathbf{M}_n(K)$ satisfies s_{2n} but no identity of degree strictly less than $2n$.

Indeed, $\mathbf{M}_n(K)$ satisfies all s_d with $d \geq 2n$.

Polynomial Identity Groups

We say that group G satisfies PI_n if its group algebra $K[G]$ satisfies a polynomial identity of degree n. Of course, this depends somewhat on the field K. Indeed it follows from linearization that this property only depends upon the characteristic of K.

Kaplansky (1949) observed that if G has an abelian subgroup A of finite index n, then $K[G]$ satisfies the standard identity s_{2n} and hence G satisfies PI_{2n}. We seek a converse of the form: If G satisfies PI_n, then G has an abelian subgroup A of index $\leq f(n)$.

Assume K has characteristic 0. If $n \leq 5$, Amitsur (1961) proved such a result using central polynomials. Only Wagner's polynomial (1937) for 2×2 matrices was known at that time. Since the existence of a polynomial identity for the group algebra $K[G]$ bounds the "degrees" of its irreducible representations, Isaacs and I (1964) were able to prove the general result first by using the character theory of finite groups and then lifting the result from finite to arbitrary groups.

Characteristic $p > 0$

Now let K have characteristic $p > 0$. M. Smith (1971) in her thesis, used certain "linear identities" to obtain strong partial results on the converse. Building on this, and using more group theory, I obtained the following result (1972).

Theorem

Let K be a field of characteristic $p > 0$ and assume that the group algebra $K[G]$ satisfies a polynomial identity of degree n. Then G has a normal subgroup A of index $\leq a(n)$ such that its commutator subgroup A' is a finite p-group of order $\leq b(n)$.

A group A whose commutator subgroup A' is a finite p-group is said to be p-abelian. The above result actually characterizes groups with PI_n for some n, in characteristic $p > 0$. Indeed, G is such a group if and only if it has a p-abelian subgroup of finite index.

The Permutational Property P_n

Following Curzio, Longobardi, Maj and Robinson (1985), a group G is said to have the permutational property P_n if for all $x_1, x_2, \ldots, x_n \in G$ (in that order), there exists a nonidentity permutation $\pi \in \mathrm{Sym}_n$ (depending on these elements) with $x_1 x_2 \cdots x_n = x_{\pi(1)} x_{\pi(2)} \cdots x_{\pi(n)}$.

As they showed, examples can be constructed using

Lemma

If $|G : H| = a$ and H satisfies P_b, then G satisfies P_{ab}.

Lemma

If $|G'| = a$, then G satisfies P_{a+1}.

PI_n Implies P_n

Another sufficient condition is

Lemma

If G satisfies PI_n for any field K, then it satisfies P_n.

Indeed, suppose $K[G]$ satisfies a polynomial identity of degree n. Then, via linearization, $K[G]$ satisfies a multilinear polynomial f of the form

$$f(\zeta_1, \zeta_2, \ldots, \zeta_n) = \sum_{\sigma \in \mathrm{Sym}_n} k_\sigma \zeta_{\sigma(1)} \zeta_{\sigma(2)} \cdots \zeta_{\sigma(n)}$$

with coefficient $k_1 = 1$. Now note that if $x_1, x_2, \ldots, x_n \in G$, then $f(x_1, x_2, \ldots, x_n) = 0$, so the identity term in f must be cancelled by at least one other term.

The Finite Conjugate Center

Let $\Delta(G)$ be the set of elements of group G having finitely many G-conjugates. This is the F. C. center of G. It is a characteristic subgroup and the main result of [CLMR] asserts

Theorem

If G satisfies P_n, then $|G : \Delta(G)| \le a(n)$ and $\Delta(G)'$ is finite.

The latter is the best they can do because $|\Delta(G)'|$ is not bounded by a function of n. For example, if G is a finite dihedral group, then G has an abelian subgroup of index 2, so it satisfies P_4. Furthermore, $G = \Delta(G)$ and G' can be arbitrarily large.

Classes of Bounded Size

Notice that the previous result offers no information on finite groups. To sharpen it, we return to the old PI techniques. Some of the methods used there are listed below.

Let $\Delta_k(G)$ be the set of all elements of G having $\leq k$ conjugates. Note that $\Delta_r(G)\Delta_s(G) \subseteq \Delta_{rs}(G)$ and $\Delta_r(G)^{-1} = \Delta_r(G)$. Of course these subsets are not necessarily subgroups. The following was proved by Wiegold (1957).

Theorem

Let G be a group and let k be an integer.

1. *If $|G'| \leq k$, then $G = \Delta_k(G)$.*
2. *If $G = \Delta_k(G)$, then $|G'| \leq (k^4)^{k^4}$.*

Part (2) above was a conjecture of B. H. Neumann (1954), of course without the particular bound.

Subsets of Finite Index

Since $\Delta_r(G)$ is not a subgroup, one has to deal with subsets of G. We say a subset T of G has index $\leq k$ if there exist group elements $x_1, x_2, \ldots, x_k$ with $\bigcup_1^k Tx_i = G$. This is not right-left symmetric. For example, if $G = \langle x, y \mid y^2 = 1, x^y = x^{-1} \rangle$ is the infinite dihedral group and if $S = \{x^n, x^{-n}y \mid n \geq 0\}$, then $G = S \cup Sy$, but $yS = S$ easily implies that G cannot be written as a finite union of left cosets of S.

Lemma

If $|G : T| \leq k$ and $T^* = T \cup 1 \cup T^{-1}$, then $(T^*)^{4^k}$ is a subgroup of G.

Lemma

Suppose $H_1, H_2, \ldots, H_k$ are subgroups of G and set $S = \bigcup_1^k H_i x_i$.

1. *If $S = G$, then $|G : H_i| \leq k$ for some i.*
2. *If $S \neq G$. then there exist g_j for $1 \leq j \leq (k+1)!$ with $\bigcap_j Sg_j = \emptyset$. In particular, if $S \cup T = G$, then $|G : T| \leq (k+1)!$.*

Characterization of P_n-Groups

Combining the above methods with the work of [CLMR], my student Mustafa Elashiry and I obtained the following result (2011).

Theorem

Let G be a group satisfying the permutational property P_n and set $k = n!$. Then we have

1. $|G : \Delta_k(G)| \leq k\cdot(k+1)!$, *and*
2. *G has a characteristic subgroup $N = \langle \Delta_k \rangle$ with $|G : N| \leq k\cdot(k+1)!$ and with $|N'|$ finite and bounded by a function of n.*

The latter bound is big. Set $l = k\cdot(k+1)!$. Then $N = (\Delta_k(G))^{4^l} \subseteq \Delta_m(G)$ where $m = k^{4^l}$. So $N = \Delta_m(N)$ and hence $|N'| \leq (m^4)^{m^4}$.

The Rewritable Property Q_n

Following R. D. Blyth (1988), we say that a group G satisfies the rewritable property Q_n if for all $x_1, x_2, \ldots, x_n \in G$ (in that order) there exist distinct permutations $\sigma, \tau \in \mathrm{Sym}_n$, depending on these elements, with $x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)} = x_{\tau(1)} x_{\tau(2)} \cdots x_{\tau(n)}$. Obviously

Lemma

If G satisfies P_n, then it satisfies Q_n.

Lemma

If $|G'| < n!$, then G satisfies Q_n.

Recall, if $|G'| \leq n - 1$ then G satisfies P_n. Are these properties the same or just similar?

Examples and Blyth's Theorem

$G = \mathrm{Sym}_3$ satisfies Q_3 but not P_3. Q_3 follows from the previous lemma. For P_3, notice that the product $(1\,2\,3)\cdot(2\,3)\cdot(1\,3\,2) = (1\,2)$ is not equal to any other permuted product. Blyth has a generalization of this with G_n a cyclic group of odd order acted on by a cyclic 2-group. These groups have property Q_n but not P_n for all $n \geq 3$. We will discuss other examples later on.

Theorem

If G satisfies Q_n, then $|G : \Delta(G)| \leq a(n)$ and $\Delta(G)'$ is finite.

Obviously this is similar to the P_n result. But the proof is surprisingly much more difficult and uses a really neat trick. Fortunately, Blyth's trick can be merged with the PI techniques to yield another result with my student Elashiry.

Characterization of Q_n-Groups

Theorem

Let G be a group satisfying the rewritable property Q_n. Then there exist functions k, l and m of n with

1. $|G : \Delta_k(G)| \leq l$, *and*
2. *G has a characteristic subgroup $N = \langle \Delta_k \rangle$ with $|G : N| \leq l$ and with $|N'| \leq m$.*

Corollary

If G is a group satisfying the rewritable property Q_n, then G satisfies the permutational property P_c for some function c of n.

The bounds here are big. For example, k, l and c are determined via

$$j = n!, \quad p = j^2, \quad q = p{\cdot}2^p, \quad k = j{\cdot}q^p, \quad l = k{\cdot}(k+1)!, \quad c = (m+1)l$$

The Rewritable Degree

Note that $P_n \Rightarrow P_{n+1}$ and $Q_n \Rightarrow Q_{n+1}$. Thus for any group G with either property it makes sense to define the *permutational degree* by $p(G) = \min\{n \mid G \text{ has } P_n\}$ and the *rewritable degree* by $q(G) = \min\{n \mid G \text{ has } Q_n\}$.

Lemma

$q(\mathrm{Sym}_n) = n$ for all $n \geq 2$.

This follows since $G = \mathrm{Sym}_n$ has $|G'| = n!/2 < n!$ so G satisfies Q_n. On the other hand, by considering the $n-1$ transpositions $(1\,2), (1\,3), \ldots, (1\,n)$ we see that G does not satisfy Q_{n-1}. In particular for any $n \geq 2$ there exists a finite group G_n with $q(G_n) = n$.

The Permutational Degree

Much more difficult is

Proposition

$p(\mathrm{Sym}_n) \geq n+1$ for all $n \geq 3$.

Thus we see that the properties P_n and Q_n are definitely different. We are left with the seemingly difficult combinatorial problem of determining $p(\mathrm{Sym}_n)$.

Proposition

For every integer $n \geq 2$ there exists a finite solvable group G_n with $p(G_n) = n$.

Finite Groups

If G is finite, an upper bound for $p(G)$ can be obtained from the degrees of its irreducible complex representations. Let $d(G) \le \sqrt{|G|}$ denote the largest such degree.

Lemma

If G is a finite group, then $p(G) \le 2d(G) \le 2\sqrt{|G|}$.

To see this, note that the complex group algebra $C[G]$ is a direct sum of various $\mathbf{M}_d(C)$ for suitable degrees $d \le d(G)$. The Amitsur-Levitzki Theorem now implies that each of these direct summands satisfies the standard identity $s_{2d(G)}$ and hence the same is true for $C[G]$. Thus G satisfies $P_{2d(G)}$. Question: Can the inequality $p(G) \le 2\sqrt{|G|}$ be proved without representation theory and how sharp is it?

References 1

- S. A. Amitsur. *Groups with representations of bounded degree II*, Illinois J. Math., **5** (1961), 198–205.
- S. A. Amitsur and J. Levitzki, *Minimal identities for algebras*, Proc. AMS, **1** (1950), 449–463.
- R. D. Blyth, *Rewriting products of group elements, I*, J. Algebra, **116** (1988), 506-521.
- M. Curzio, P. Longobardi, M. Maj, and D. J. S. Robinson, *A permutational property of groups*, Arch. Math., **44** (1985), 385-389.
- M. I. Elashiry and D. S. Passman, *Rewritable groups*, J. Algebra, **345** (2011), 190–201.
- I. M. Isaacs and D. S. Passman, *Groups with representations of bounded degree*, Canadian J. Math., **16** (1964), 299–309.

References 2

- I. Kaplansky, *Groups with representations of bounded degree*, Canad. J. Math., **1** (1949), 105–112.
- B. H. Neumann, *Groups covered by finitely many cosets*, Publ. Math. Debrecen, **3** (1955), 227–242.
- D. S. Passman, *Group rings satisfying a polynomial identity*, J. Algebra, **20** (1972), 103–117.
- D. S. Passman, *Permutational and rewritable groups*, Proc. AMS, **147** (2019), 995–1003.
- M. K. Smith, *Group algebras*, J. Algebra, **18** (1971), 477-499.
- W. Wagner, *Über die Grundlagen der projektiven Geometrie und allgemeine Zahlsysteme*, Math. Z., **113** (1936–37), 528–567.
- J. Wiegold, *Groups with boundedly finite classes of conjugates*, Proc. Royal Soc. London, Ser. A **238** (1957), 389–401.