Polynomial functions on classical groups and Frobenius groups

E. Aichinger and P. Mayr
Institut für Algebra, Universität Linz, Austria

1 Introduction

Polynomial functions can be defined on arbitrary algebras. We will describe and count the unary polynomial functions for some classes of finite groups.

1.1 Definitions

Let $(G, \cdot)$ be a group. A *unary polynomial function* $p : G \to G$ is a function that can be written in the form

$$p(x) := a_0 x^{e_0} a_1 x^{e_1} \cdots a_{n-1} x^{e_{n-1}} a_n,$$

where $n \geq 1$, $a_0, \ldots, a_n$ are in G, and $e_0, \ldots, e_{n-1}$ are integers.

Let $P(G)$ denote the set of all polynomial functions on G. Then $P(G)$ forms a subgroup of $(G^G, \cdot)$, the group of all functions from G to G. Further, $P(G)$ is generated by the identity function on G and all constant functions.

1.2 Examples

Inner automorphisms are polynomial functions. For $g \in G$, the function $G \to G, x \mapsto [x, g]$, is polynomial.

1.3 Simple facts

Since $P(G)$ is closed under composition of functions, $P(G)$ forms a near-ring [Pil83].

If G is abelian, then $\{f \in P(G) \mid f(1) = 1\}$ is a ring and $|P(G)| = \exp(G) \cdot |G|$.

Let $N \trianglelefteq G$. Then $f \in P(G)$ is compatible with N, that is: If $xN = yN$ for $x, y \in G$, then $f(x)N = f(y)N$. Hence we have a natural homomorphism from $P(G)$ onto $P(G/N)$ with kernel

$$\{f \in P(G) \mid f(G) \subseteq N\}.$$

1.4 Problems

Given a group G, we consider the following:

- Is a given function $f : G \to G$ a polynomial?
- Determine the size of $P(G)$.
- Are all automorphisms of G in $P(G)$?
- Are all endomorphisms of G in $P(G)$?

1.5 Some known results

Polynomial functions have been investigated for several classes of groups. Still, a general theory for all groups seems to be out of reach.

- [Frö58]: Let $|G| > 2$. Then $P(G) = G^G$ iff G is a finite simple non-abelian group.
- [Mel78]: All endomorphisms of S_n are polynomial functions.
- [LP95]: For a semidirect product $G = AB$ of groups A and B of relatively prime order, all endomorphisms of G are in $P(G)$ if $\mathrm{End}(A) \subseteq P(A)$ and $\mathrm{End}(B) \subseteq P(B)$.

2 Linear groups

2.1 A criterion for non-solvable groups

Lemma 2.1 ([AM03]). *Let G be a finite non-solvable group such that every normal subgroup of G is central or contains the derived subgroup G'. For a function $f : G \to G'$, the following are equivalent:*

(1) The function f is in $P(G)$;

(2) There exists an integer μ such that

$$f(gz) = f(g) z^{\mu \cdot \exp(G/G')}$$

for all $g \in G, z \in Z(G)$.

Sketch of the proof. The implication (1) $\Rightarrow$ (2) is immediate. For the converse, we use induction and commutators, to show the existence of "Lagrange interpolation functions":

For $t \in G$, $n \in G'$, we have $p_{t,n} \in P(G)$ such that

$$p_{t,n}(tZ(G)) = \{n\} \text{ and } p_{t,n}(G - tZ(G)) = \{1\}.$$

Then every function satisfying (2) is equal to a product of $e(x) := x^{\mu \cdot \exp(G/G')}$ and some functions $p_{t,n}$. □

By Lemma 2.1, the polynomial functions from G to G' are precisely those functions that are linear on the cosets of the center $Z(G)$ in G. From this characterization we obtain the next formula:

Theorem 2.2 ([AM03]). *For G as in Lemma 2.1, we have*

$$|P(G)| =$$

$$|G'|^{|G:Z(G)|} \cdot \mathrm{lcm}(\exp(G/G'), \exp(Z(G))) \cdot |G : G'|.$$

2.2 Classical linear groups

The finite linear, unitary, symplectic, and orthogonal groups (with the exception of certain groups acting on vector spaces of low dimension) satisfy the assumptions of Lemma 2.1.

Theorem 2.3 ([May04]). *Let V be a finite vector space over the field F, and let G be a non-solvable group satisfying one of the following:*

- $\mathrm{SL}(V, F) \leq G \leq \mathrm{GL}(V, F)$,
- $\mathrm{SU}(V, F) \leq G \leq \mathrm{U}(V, F) \cdot F^*$,
- $G = \mathrm{Sp}(V, F)$,
- $\Omega(V, F) \leq G < \mathrm{O}(V, F)$ *where* $\dim_F V \geq 5$.

Then we have:

(1) All automorphisms of G are in $P(G)$.

(2) All endomorphisms of G are in $P(G)$ iff $G \in \{\mathrm{SL}(V, F), \mathrm{SU}(V, F), \mathrm{Sp}(V, F), \Omega(V, F)\}$ or ($\Omega(V, F) < G < \mathrm{O}(V, F)$ and $Z(G) = 1$).

For G as in Theorem 2.3, the size of $P(G)$ is given by Theorem 2.2. By (2), we have $\mathrm{End}(G) \subseteq P(G)$ iff $G = G'$ or $Z(G) = 1$.

In [May04], there are similar results for the non-solvable quotients of linear groups (e.g. the projective linear groups). For groups of semilinear transformations the number of polynomial functions is not known.

2.3 Determinant and transposition

Let $G = \mathrm{GL}(n, q)$ for a natural number n and a prime power q. The functions

$$d : G \to G, \ x \mapsto \det(x) \cdot 1,$$

and

$$\tau : G \to G, \ x \mapsto x^t.$$

are in $P(G)$ [May04].

3 Semidirect products

3.1 A criterion for Frobenius groups

A function on a Frobenius group is polynomial if it is "locally polynomial" on each coset of the Frobenius kernel.

Theorem 3.1 ([Aic02]). *Let $G = AB$ be a Frobenius group with kernel A and complement B. For a function $f : G \to A$, the following are equivalent:*

(1) The function f is in $P(G)$;

(2) For every $b \in B$ there is $p_b \in P(G)$ such that

$$f(ab) = p_b(a) \text{ for all } a \in A.$$

Theorem 3.2 ([Aic02]). *Let $G = AB$ be a Frobenius group with kernel A and complement B, and let*

$$R := \{f|_A \mid f \in P(G), f(A) \subseteq A\}.$$

Then we have

$$|P(G)| = |P(B)| \cdot |R|^{|B|}.$$

If A is abelian, then $\{f \in R \mid f(1) = 1\}$ is a ring of endomorphisms on A.

Corollary 3.3 ([May04]). *Let G be a Frobenius group with kernel A and a complement B that is isomorphic to the quaternion group of order 8 or to $\mathrm{SL}(2, 3)$. Then*

$$|P(G)| = |P(B)| \cdot (|A| \cdot \exp(V)^4)^{|B|}.$$

3.2 Extensions of cyclic groups

Theorem 3.4 ([May04]). *Let G be a finite group, and let A be a cyclic normal subgroup of G such that $|A|$ and $|G : A|$ are relatively prime. Let M be the set of Sylow subgroups of A. Then we have*

$$|P(G)| = |P(G/A)| \cdot \prod_{P \in M} |P|^{2 \cdot |G:C_G(P)|},$$

and all endomorphisms of G are in $P(G)$ iff all endomorphisms of G/A are in $P(G/A)$.

3.3 Further applications

From Theorem 3.4 we obtain (see [May04]):

- $|P(G)|$ for all solvable groups all of whose abelian subgroups are cyclic;
- $|P(G)|$ for all Frobenius complements.

Theorem 3.5 ([May04]). *For a non-solvable Frobenius complement, all endomorphisms are polynomial.*

Advertisements

The computer algebra system SONATA [ABE+99] under GAP4 provides algorithms to investigate polynomial functions on small groups.

Acknowledgments

This work has been supported by grant P15691 of the Austrian Science Foundation (Fonds zur Förderung der wissenschaftlichen Forschung).

References

[ABE+99] E. Aichinger, F. Binder, J. Ecker, P. Mayr, and C. Nöbauer, *SONATA - system of near-rings and their applications, package for the group theory system GAP4*, Division of Algebra, Johannes Kepler University Linz, Austria, 1999.

[Aic02] E. Aichinger, *The polynomial functions on certain semidirect products of groups*, Acta Sci. Math. (Szeged) **68** (2002), 63–81.

[AM03] E. Aichinger and P. Mayr, *Polynomial functions and endomorphism near-rings on certain linear groups*, Communications in Algebra **31** (2003), no. 11, 5627–5651.

[Frö58] A. Fröhlich, *The near-ring generated by the inner automorphisms of a finite simple group*, J. London Math. Soc. **33** (1958), 95–107.

[LP95] C. G. Lyons and G. L. Peterson, *Semidirect products of I-E groups*, Proc. Amer. Math. Soc. **123** (1995), no. 8, 2353–2356.

[May04] P. Mayr, *Polynomial functions on classical groups and Frobenius groups*, Ph.D. thesis, Johannes Kepler University Linz, submitted March 2004.

[Mel78] J. D. P. Meldrum, *On the structure of morphism near-rings*, Proc. Roy. Soc. Edinburgh Sect. A **81** (1978), no. 3-4, 287–298.

[Pil83] G. F. Pilz, *Near-rings*, 2nd ed., North-Holland Publishing Company – Amsterdam, New York, Oxford, 1983.