Unary polynomial functions on a class of finite groups

Peeter Puusemp

University of Tartu

Novi Sad, March 15-18, 2012

Abstract

We describe unary polynomial functions on finite groups G that are semidirect products of an elementary abelian group of exponent p and a cyclic group of prime order q, $p \neq q$.

This is a joint work with prof. Kalle Kaarli (University of Tartu).

Definition

Given an algebraic structure A, an n-ary **polynomial function** on A is a mapping $A^n \to A$ that can be presented as a compostition of fundamental operations of A, projection maps and constant maps.

Note

We consider only unary polynomial functions.

Examples

Example 1

Polynomial functions on a **commutative ring** R are precisely the usual polynomial functions, that is, the functions $f : R \to R$ that can be defined by the formula

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_s x^s$$

where $a_0, a_1, \ldots, a_s \in R$.

Example 2

If A is a **left module over a ring** R then a function $f : A \to A$ is a polynomial function on A if and only if there exist $r \in R$ and $a \in A$ such that $f(x) = rx + a$ for each $x \in A$.

Examples

Example 3

Let $(G;+)$ be a **group**. Then a function $f : G \to G$ is a polynomial function if and only if there are $a_1, a_2, \ldots a_{s+1} \in G$ and $e_1, e_2, \ldots, e_{s+1} \in \mathbb{Z}$, such that for each $x \in G$

$$f(x) = a_1 + e_1x + a_2 + e_2x + \ldots + a_s + e_sx + a_{s+1}.$$

Example 4

If G is a **finite group**, any function $f \in P(G)$ has the following form:

$$f(x) = (a_1 + x - a_1) + (a_2 + x - a_2) + \ldots + (a_{s-1} + x - a_{s-1}) + a_s.$$

Studied cases

The size of $P(G)$ is known

- for all groups with $|G| \leq 100$
- all simple groups
- all abelian groups
- the symmetric groups S_n
- dihedral and generalized dihedral groups
- generalized quaternion groups
- dicyclic groups
- certain subdirectly irreducible groups (including the nonabelian groups of order qp)
- general linear groups

The group in consideration

Our aim is to describe $P(G)$ in case when G is a semidirect product of an elementary abelian group of exponent p and a cyclic group of prime order q, $q \neq p$.

Definition

Suppose that we are given two groups A and B, and a homomorphism $\alpha : B \to \operatorname{Aut} A$. The **external semidirect product** $G = A \rtimes_\alpha B$ is defined as the direct product of sets $A \times B$ with the group operation

$$(a_1, b_1) + (a_2, b_2) = (a_1 + \alpha(b_1)(a_2), b_1 + b_2).$$

The group in consideration

We shall identify every $a \in A$ with $(a, 0) \in G$ and every $b \in B$ with $(0, b) \in G$.
After such identifiction

- A is a normal subgroup of G ($A \trianglelefteq G$)
- B is a subgroup of G ($B \leq G$)
- $b + a - b = \alpha(b)(a)$ for all $a \in A, b \in B$

Given finite $G = A \rtimes_\alpha B$ natural homomorphism $G \to G/A$ induces the surjective group homomorphism $\Phi : P(G) \to P(G/A)$.

$$K := \operatorname{Ker}\Phi = \{p \in P(G) \mid p(G) \subseteq A\}.$$

Let T be a transversal of cosets of K in $P(G)$. **Then each polynomial of G has a unique representation** in the form of sum $f + g$ where $f \in T$, $g \in K$.

Let $|B| = q$, $B = \{0 = b_0, \ldots, b_{q-1}\}$ and $K_i = \{p|_{b_i+A} \mid p \in K\}$, $i = 0, 1, \ldots, q-1$.

Obviously, every $p \in K$ determines a q-tuple $(p|_{b_0+A}, \ldots, p|_{b_{q-1}+A})$. Hence, we have a one-to-one mapping

$$\Psi : K \to K_0 \times \cdots \times K_{q-1}\,.$$

Theorem 1 (E. Aichinger)

Let $G = A \trianglelefteq_\alpha B$ and let K, $K_0, \dots, K_{q-1}$, Ψ be as defined above. Assume that the homomorphism α is one-to-one and all automorphisms $\alpha(b)$, $b \neq 0$, are fixed-point-free. Then the mapping Ψ is bijective.

Clearly the mapping $\kappa_i : K_i \to K_0$, $f \mapsto g$, where $g(x) = f(b_i + x)$, $i = 0, \dots, q-1$, is a bijection.

It follows that under assumptions of Theorem 1, in order to understand the polynomials of G it suffices to know polynomials of G/A and polynomials $f \in P(G)$ such that $f(A) \subseteq A$. In particular, the following formula holds:

$$|P(G)| = |P(G/A)| \cdot |K_0|^{|B|} .$$

Structure of the group G

In what follows $G = A \rtimes_\alpha B$, where $A = \mathbb{Z}_p^n$, $B = \mathbb{Z}_q$ with p and q distinct primes and α a non-trivial group homomorphism, that is, $|\alpha(B)| > 1$.

Clearly

$$\alpha(B) = \{1, \phi, \phi^2, \ldots, \phi^{q-1}\},$$

where $\alpha(1) = \phi \in \mathrm{Aut}(A) \setminus \{1\}$.

Let S be the subring of $\mathrm{End}\, A$ generated by ϕ. Then A has a natural structure of an S-module.

The homomorphism α can be considered as a GF(p)-representation of the group $\mathbb{Z}_q$. Since $(q, p) = 1$, the Maschke's Theorem implies that α is completely reducible.

Maschke's Theorem

Let G be a finite group and let F be a field whose characteristic does not divide the order of G. Then every F-representation of G is completely reducible.

So

$$A = A_1 + A_2 + \ldots + A_k$$

where A_i, $i = 1, \ldots, k$, are irreducible S-modules.

Let ϕ_i be the restriction of ϕ to A_i, $i = 1, \ldots, k$.

Let

$$A = \tilde{A}_1 + \tilde{A}_2 + \ldots + \tilde{A}_k$$

where $\tilde{A}_i$, $i = 1, \ldots, k$, are homogeneous components of the S-module A. If there exists i such that $\phi_i = 1$, then let $\tilde{A}_1$ be the sum of all such A_j that $\phi_j = 1$.

In the latter case we put $C = \tilde{A}_1$ and $D = \tilde{A}_2 + \cdots + \tilde{A}_l$. Obviously $A = C \oplus D$ and it follows easily from the multiplication law that C is the center of the group G. If there is no i with $\phi_i = 1$, we put $C = \{0\}$ and $D = A$.

Normal subgroups of the group G

Proposition 1

The group G is direct product of normal subgroups C and $D \rtimes B$. Every normal subgroup of G is the sum of two normal subgroups of G, one contained in C and the other in $D \rtimes B$.

The direct product $C \times (D \rtimes B)$ has no skew congruences.

Polynomial functions on the group G

From Proposition 1 we have that the mapping

$$\chi : P(G) \to P(C) \times P(D \rtimes B),\ \chi(p) = (p|_C, p|_{D \rtimes B})$$

is one-to-one. In fact, given $x = y + z \in G$ where $x \in C$, $y \in D \rtimes B$, we have

$$p(x) = p|_C(y) + p|_{D \rtimes B}(z).$$

Due to the result of Kaarli and Mayr [1], Proposition 1 also implies that χ is surjective. Hence the problem of characterization of polynomials of G reduces to the same problem for groups C and $D \rtimes B$.

[1] K. Kaarli, P. Mayr, *Polynomial functions on subdirect products*, Monatsh. Math. **159** (2010), 341–359.

Since for the abelian group C the problem is trivial, we have to deal only with group $D \rtimes B$. In this situation Theorem 1 applies.

It follows that in order to describe polynomials of G one has to describe polynomials of $P(G/A)$ and the polynomials of G that map A to A. The first problem is trivial because $G/A \simeq \mathbb{Z}_q$ and polynomials of $\mathbb{Z}_q$ have the form $f(x) = kx + u$ with $k, u \in \mathbb{Z}_q$. In particular, $|P(G/A)| = q^2$.

It remains to describe the polynomials of G that map A to A. As above, let $K_0 = \{p|_A \mid p \in P(G), p(A) \subseteq A\}$.

Lemma 1

The set K_0 consists of all functions $f : A \to A$ of the form $f(x) = s(x) + a$ where $s \in S$, $a \in A$. In particular,

$$|K_0| = |S| \cdot |A| .$$

It turns out that S is direct sum of Galois fields and these direct summands S_j are in one-to-one correspondence with the homogenous components $\tilde{A}_j$, $j = 1, \ldots, l$. Moreover, $S_j \simeq \mathrm{GF}(p^{m_i})$ where m_i is the dimension of any A_i over $\mathrm{GF}(p)$ in $\tilde{A}_j$.

Theorem 2

Let $G = A \rtimes_\alpha B$ where $A = \mathbb{Z}_p^n$ and $B = \mathbb{Z}_q$ where p and q are distinct primes. Assume that the center of G is trivial (equivalently, $\alpha(1)$ is fixed-point-free). Let S be the subring of $\mathrm{End}\, A$ generated by $\alpha(1)$ and let $A_1, \ldots, A_l$ be a complete list of pairwise non-isomorphic irreducible S-submodules of A. Denote $|A_i| = p^{m_i}$, $i = 1, \ldots, l$. Then

$$|P(G)| = q^2 p^{q(m_1 + \cdots + m_l + n)} .$$

Example 1

Let $G = A \rtimes B$ where $A = \mathbb{Z}_5^3$, $B = \mathbb{Z}_2$, and let

$$\phi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

Then $G = C \times (D \rtimes B)$ where $C = \mathbb{Z}_5^2$ is the center of the group G, $D = \mathbb{Z}_5$, $\phi|_C = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and $\phi|_D = \begin{pmatrix} 4 \end{pmatrix}$ is fixed-point-free.
Each polynomial function p on G is of the form
$p(x) = p|_C(y) + p|_{D \rtimes B}(z)$, $x = y + z \in G$, $y \in C, z \in D \rtimes B$.
Since D is a S-module, $S \cong \mathrm{GF}(5)$, we get using Theorem 2 that

$$|P(G)| = |P(C)||P(D \rtimes B)| = 5^3 \cdot 2^2 \cdot 5^{2(1+3)} = 2^2 \cdot 5^{11}.$$

Example 2

Let $G = A \rtimes B$ where $A = \mathbb{Z}_5^3$, $B = \mathbb{Z}_2$, and let

$$\phi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

Then $G = C \times (D \rtimes B)$ where $C = \mathbb{Z}_5$ is the center of the group G, $D = \mathbb{Z}_5^2$, $\phi|_C = (1)$, $\phi|_D = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$ is fixed-point-free. Each polynomial function p on G is of the form
$p(x) = p|_C(y) + p|_{D \rtimes B}(z)$, $x = y + z \in G$, $y \in C, z \in D \rtimes B$.
Since D is a $(S_1 \times S_2)$-module, $S \cong S_1 \times S_2$, $S_1 \cong \mathrm{GF}(5)$, $S_2 \cong \mathrm{GF}(5)$, we get using Theorem 2 that

$$|P(G)| = |P(C)||P(D \rtimes B)| = 5^2 \cdot 2^2 \cdot 5^{2(1+1+3)} = 2^2 \cdot 5^{12}.$$

Example 3 (There's a mistake in it)

Let $G = A \rtimes B$ where $A = \mathbb{Z}_7^3$, $B = \mathbb{Z}_3$, and let

$$\phi = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 2 \\ 0 & 2 \cdot 2 & 3 \end{pmatrix}.$$

Since the characteristic polynomial of ϕ is ..., S is direct sum $S_1 \times S_2$ where $S_1 \cong \mathrm{GF}(7)$, $S_2 \cong \mathrm{GF}(7^2)$. So the center of G is trivial and ϕ is fixed-point-free. Using Theorem 2 we get that

$$|P(G)| = 3^2 \cdot 7^{3(1+2+3)} = 3^2 \cdot 7^{18}.$$

Example 4

Let $G = A \rtimes B$ where $A = \mathbb{Z}_{23}^3$, $B = \mathbb{Z}_7$, and let

$$\phi = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 14 \\ 0 & 1 & 13 \end{pmatrix}.$$

Since the characteristic polynomial of ϕ is $x^3 + 10x^2 + 9x + 22$, i.e. irreducible cubic, A is simple S-module and $S \cong \mathrm{GF}(23^3)$. So the center of G is trivial and ϕ is fixed-point-free. Using Theorem 2 we get that

$$|P(G)| = 7^2 \cdot 23^{7(3+3)} = 7^2 \cdot 23^{42}.$$

Thank you!