ACTA ET COMMENTATIONES UNIVERSITATIS TARTUENSIS DE MATHEMATICA
Volume 17, Number 1, June 2013
Available online at www.math.ut.ee/acta/

Unary polynomials on a class of semidirect products of finite groups

Kalle Kaarli and Peeter Puusemp

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, $p \neq q$.

1. Introduction

Given a (universal) algebra A, an n-ary *polynomial function* on A is a mapping $A^n \to A$ that can be presented as a composition of fundamental operations of A, projection maps and constant maps. In the present paper we consider only unary polynomial functions. Therefore, from now on, when we talk about polynomial functions we always mean unary polynomial functions. Also, often we refer to polynomial functions just as to polynomials. The set of all polynomial functions on an algebra A will be denoted by $P(A)$.

Clearly, polynomial functions on a commutative ring R with identity are the usual polynomials, that is, the functions $f : R \to R$ that can be defined by the formula

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

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

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 $x \in A$.

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

Received June 11, 2012.
2010 *Mathematics Subject Classification.* Primary 20D40; Secondary 08A40.
Key words and phrases. Polynomial function, finite group, semidirect product of groups.
This work was supported by Estonian Science Foundation Grant 8394 and Estonian Targeted Financing Project SF0180039s08.
http://dx.doi.org/10.12697/ACUTM.2013.17.07

for each $x \in G$

$$f(x) = a_1 + e_1 x + a_2 + e_2 x + \ldots + a_s + e_s x + a_{s+1}. \tag{1.1}$$

The groups we consider are written additively, although they need not be abelian. This is a general practice in theory of polynomial functions on groups. It comes from the fact that multiplicative notation is already occupied in the natural near-ring structure of the set $P(G)$.

Obviously, in formula (1.1) it suffices to take $e_i \in \{-1, 1\}$. If, moreover, the group G is finite then we may take all e_i equal to 1. This is because in a finite group the additive inverse of any element a is equal to its multiple ma where $m > 0$. This implies that in case of a finite group G any function $f \in P(G)$ has the form

$$f(x) = (a_1 + x - a_1) + (a_2 + x - a_2) + \ldots + (a_{s-1} + x - a_{s-1}) + a_s\,, \tag{1.2}$$

where $a_1, \ldots, a_s \in G$. In other words, polynomial functions of finite groups are precisely the sums of finitely many inner automorphisms and a constant.

As described in [1] the size of $P(G)$ is known for all groups with $|G| \leq 100$, all finite simple groups, all finite abelian groups, the symmetric groups S_n, dihedral and generalized dihedral groups, generalized quaternion groups, dicyclic groups, certain subdirectly irreducible groups (including the non-abelian groups of order qp), and the general linear groups. The aim of the present paper 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 1. 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

$$(a_1, b_1) + (a_2, b_2) = (a_1 + \alpha(b_1)(a_2), b_1 + b_2). \tag{1.3}$$

We shall identify every $a \in A$ with $(a, 0) \in G$ and every $b \in B$ with $(0, b) \in G$. After such identification A is a normal subgroup of G ($A \trianglelefteq G$), B is a subgroup of G ($B \leq G$) and

$$b + a - b = \alpha(b)(a) \tag{1.4}$$

for all $a \in A$, $b \in B$.

Clearly, the natural homomorphism $G \to G/A$ induces the surjective group homomorphism $\Phi : P(G) \to P(G/A)$ whose kernel K consists of all polynomials $p \in P(G)$ such that $p(G) \subseteq A$. It follows that the problem of describing polynomials of G reduces, to great extent, to characterizing polynomials of G/A and polynomials of G belonging to K. Indeed, if we know the polynomials of G/A then we may pick for each of them a polynomial $f \in P(G)$ that induces it modulo A. In other words, we may choose a transversal T of

cosets of K in $P(G)$. Now every polynomial of G has a unique representation in the form of a sum $f+g$, where $f \in T$, $g \in K$.

Let $|B| = q$, $B = \{0 = b_0, \dots, b_{q-1}\}$ and $K_i = \{p|_{b_i+A} \,|\, p \in K\}$, $i = 0, 1, \dots, q-1$. Obviously, every $p \in K$ determines a q-tuple $(p|_{b_0+A}, \dots, p|_{b_{q-1}+A})$. Hence, we have a one-to-one mapping

$$\Psi : K \to K_0 \times \cdots \times K_{q-1}\,, \quad \Psi(p) = (p|_{b_0+A}, \dots, p|_{b_{q-1}+A})\,.$$

In what follows we shall use a result of Aichinger [1].

Theorem 1 (E. Aichinger)**.** *Let $G = A \rtimes_\alpha B$ and let Ψ be the mapping defined above. Assume that the homomorphism α is one-to-one and all automorphisms $\alpha(b)$, $b \neq 1$, are fixed-point-free. Then the mapping Ψ is bijective.*

This is a special case of Lemma 2.2 in [1]. Note that the assumptions of that lemma are satisfied. Indeed, since α is one-to-one and B is a group of prime order, the centralizer of A in B is the zero subgroup.

Furthermore, it is easy to see that 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 (actually a group isomorphism). It follows that under assumptions of Theorem 1, in order to describe 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:

$$|P(G)| = |P(G/A)| \cdot |K_0|^{|B|}\,. \tag{1.5}$$

2. 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, $|\alpha(B)| > 1$. The case $|\alpha(B)| = 1$ is uninteresting because in that case the group G would be abelian.

Since B is a cyclic group of prime order q and α is non-trivial, the image $\alpha(B)$ is a cyclic group of order q, too. Thus,

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

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 $\mathrm{GF}(p)$-representation of the group $\mathbb{Z}_q$. Since $(q, p) = 1$, Maschke's Theorem [2, p. 216] implies that α is completely reducible. This means that the S-module A is the direct sum of irreducible S-submodules A_i, $i = 1, \dots, k$. Let ϕ_i be the restriction of ϕ to A_i, $i = 1, \dots, k$. Also, let $\tilde{A}_j$, $j = 1, \dots, l$, be the 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 that 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 (1.3)

that C is the center of the group G. If there is no i with $\phi_i = 1$, we put $C = \{0\}$ and $D = A$.

Next proposition describes normal subgroups of G.

Proposition 1. *The group G is the direct sum 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 contained in D or equal to $D \rtimes B$.*

Proof. It is easy to check that $D \rtimes B$ is a normal subgroup of G and obviously $C + (D \rtimes B) = G, C \cap (D \rtimes B) = \{0\}$. Let X be an arbitrary normal subgroup of G. Assume first that $X \subseteq A$. The multiplication law (1.3) easily implies that X is an S-submodule of A. Hence, $X = X_1 + \cdots + X_l$, where $X_i = X \cap \tilde{A}_i$, $i = 1, \ldots, l$. Then obviously $X_1 \subseteq C$ and $X_2 + \cdots + X_l \subseteq D$.

Let now $X \not\subseteq A$. Then there exists $a + b \in X$ with $a \in A, 0 \neq b \in B$. Since b is a generator of B, we may assume $b = 1$. Now we show that $D \subseteq X$. Since D is a sum of minimal S-submodules, it suffices to show that every minimal S-submodule of D is contained in X. Take any of the minimal submodules $A_j \subseteq D$ and $a_1 \in A_j$, such that $\phi_j(a_1) \neq a_1$. This is possible, because otherwise we would have $\phi_j = 1$ which would imply $A_j \subseteq C$. Then (1.4) implies

$$\phi(a_1) - a_1 + a + b = b + a_1 - b - a_1 + a + b = -a_1 + (a + b) + a_1 \in X\,,$$

hence also $0 \neq \phi(a_1) - a_1 \in X$. Since A_j is a minimal S-submodule of A, we conclude $A_j \subseteq X$. Next we show that $B \subseteq X$, thus also $D \rtimes B \subseteq X$. Take again $a + b \in X$, where $a \in A$ and $0 \neq b \in B$. Since $D \subseteq X$, we may assume that $a \in C$, hence $0 \neq pb = p(a + b) \in X$ which implies $B \subseteq X$. Now clearly $X = Y + (D \rtimes B)$, where $Y = X \cap C$. □

3. Polynomial functions on the group G

We have proved that the group G is the direct sum of normal subgroups C and $D \rtimes B$. Therefore 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 $p(x) = p|_C(y) + p|_{D \rtimes B}(z)$. Actually we can say more. Namely, due to the result of Kaarli and Mayr [3], Proposition 1 implies that χ is surjective.

Remark. We thank the reviewer who has pointed out that the surjectivity of χ can be derived also from a result of Scott [4]. Indeed, Proposition 1 implies that the only homomorphic image of $D \rtimes B$ with non-trivial center is B. Now, since $|B| = q \neq p$, the surjectivity of χ follows from Theorem 3.4 and Corollary to Theorem 2.1 of [4].

Hence the problem of characterization of polynomials of G reduces to the same problem for groups C and $D \rtimes B$. Moreover, since for the abelian group C the problem is trivial, we have to deal only with group $D \rtimes B$. Equivalently,

we may assume that $C = \{0\}$, that is, $\phi_i \neq 1$ for every $i = 1, \dots, k$. In this situation Theorem 1 applies. Indeed, since α is one-to-one, it suffices to observe that $\alpha(b)$ is fixed-point-free for every $0 \neq b \in B$. But this is the case because $\phi = \alpha(1)$ is fixed-point-free and every $0 \neq b \in B$ generates B.

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 $K_0 = \{p|_A \,|\, p \in P(G), p(A) \subseteq A\}$.

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,*

$$|K_0| = |S| \cdot |A| \,. \tag{3.1}$$

Proof. This is an easy consequence of the general form of group polynomials (1.2) and the formula (1.4). Clearly, it suffices to show that $\{f \in K_0 \,|\, f(0) = 0\} = S$. By definition, S consists of all functions on A that can be expressed as unary ring polynomials in ϕ. Since formula (1.4) implies $\phi \in K_0$, we have the inclusion $S \subseteq \{f \in K_0 \,|\, f(0) = 0\}$. For the opposite inclusion, due to formula (1.2), we have to prove that the restriction of every inner automorphisms of G to A is contained in S. Let γ be the inner automorphism of G determined by $a + b$, where $a \in A$, $b \in B$. Since A is an abelian normal subgroup of G, the restriction $\gamma|_A$ coincides with the restriction to A of the inner automorphism of G, determined by b. Since B is a cyclic group of order q with generator 1 and $\alpha(1) = \phi$, formula (1.4) implies $\gamma|_A = \phi^k$, where $0 \leq k < q$. This proves the lemma. □

Finally, we calculate the size of the ring S in terms of the S-module A. Since A is a faithful completely reducible S-module, the ring S is classically semisimple. Since S is commutative, it must be a direct sum of Galois fields. It follows from the basic ring theory that these direct summands S_j are in one-to-one correspondence with the homogeneous components $\tilde{A}_j$, $j = 1, \dots, l$. More precisely, every S_j is isomorphic to the so-called bicentralizer of any A_i contained in $\tilde{A}_j$, $j = 1, \dots, l$. This means that $S_j \simeq \operatorname{End}_{F_i} A_i$, where $F_i = \operatorname{End}_S A_i$. Obviously, A_i is a vector space over F_i. Since S_j is commutative, the dimension of this space must be 1. Thus, if the dimension of A_i over $\mathbb{Z}_p$ is m_i, then $F_i \simeq \mathrm{GF}(p^{m_i})$ and also $S_j \simeq \mathrm{GF}(p^{m_i})$.

In conclusion we have the following theorem.

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 $\operatorname{End} A$ generated by $\alpha(1)$ and let $A_1, \dots, A_l$ be a complete list of pairwise non-isomorphic irreducible*

S-submodules of A. Denote $|A_i| = p^{m_i}$, $i = 1, \dots, l$. *Then*

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

Proof. Using formulas (1.5) and (3.1), we have

$$\begin{aligned} |P(G)| &= |P(B)| \cdot |K| = q^2 \cdot |K_0|^q = q^2 \cdot (|S| \cdot |A|)^q \\ &= q^2 \cdot (|S_1| \cdots |S_l| \cdot |A|)^q = q^2 \cdot (p^{m_1} \cdots p^{m_l} \cdot p^n)^q \\ &= q^2 p^{(m_1+\cdots+m_l+n)q}\,. \end{aligned}$$

□

4. Examples

To conclude, we consider some examples with different action of $\phi = \alpha(1)$ on A.

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 the S-module A splits into direct sum of three irreducible submodules A_1, A_2 and A_3, all of which are additively isomorphic to $\mathbb{Z}_5$. Since the automorphism ϕ acts trivially on A_1 and A_2, and non-trivially on A_3, we have two homogeneous components: $\tilde{A}_1 = A_1 + A_2 = C$, $\tilde{A}_2 = A_3 = D$. Hence, $G = C \times (D \rtimes B)$ and $P(G)$ is isomorphic to $P(C) \times P(D \rtimes B)$. Obviously, $|P(C)| = p^3$. In order to calculate the size of $P(D \rtimes B)$, observe that $\psi = \phi|_D = \big(4\big)$. Clearly, the ring T generated by ψ in $\operatorname{End} A$ is isomorphic to GF(5). Thus, using Theorem 2 we get

$$\begin{aligned} |P(G)| &= |P(C)||P(D \rtimes B)| = |P(C)| \cdot |P(B)| \cdot (|T| \cdot |D|)^2 \\ &= 5^3 \cdot 2^2 \cdot (5 \cdot 5)^2 = 2^2 \cdot 5^7\,. \end{aligned}$$

Example 2. Let $G = A \rtimes B$, where $A = \mathbb{Z}_5^3$, $B = \mathbb{Z}_2$, and let

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

This example is similar to the previous one. Again A is a direct sum of three irreducible submodules A_1, A_2 and A_3 and again we have two homogeneous components. The difference is that now $\tilde{A}_1 = A_1 = C$, $\tilde{A}_2 = A_2 + A_3 = D$. Further, $|P(C)| = 5^2$, $|D| = 5$ and $|T| = 5$. Consequently,

$$|P(G)| = |P(C)||P(D \rtimes B)| = 5^2 \cdot 2^2 \cdot (5^2 \cdot 5)^2 = 2^2 \cdot 5^8.$$

Example 3. Let $G = A \rtimes B$, where $A = \mathbb{Z}_{19}^4$, $B = \mathbb{Z}_5$, and let

$$\phi = \begin{pmatrix} 0 & 18 & 0 & 0 \\ 1 & 14 & 0 & 0 \\ 0 & 0 & 0 & 18 \\ 0 & 0 & 1 & 4 \end{pmatrix}.$$

Since the characteristic polynomial of ϕ is

$$x^4 + x^3 + x^2 + x + 1 = (x^2 + 5x + 1)(x^2 + 15x + 1),$$

i.e., the product of distinct monic irreducible polynomials of degree 2 over GF(19), the S-module A splits into the direct sum of two non-isomorphic irreducible submodules A_1 and A_2. Hence the homogeneous components of A are $\tilde{A}_1 = A_1$ and $\tilde{A}_2 = A_2$. It is easy to see that the both A_1 and A_2 are additively isomorphic to $\mathbb{Z}_{19}^2$, and the both S_1 and S_2 are isomorphic to $\mathrm{GF}(19^2)$. So the center of G is trivial and ϕ is fixed-point-free. Using Theorem 2 we get that

$$|P(G)| = 5^2 \cdot 19^{5(2+2+4)} = 5^2 \cdot 19^{40}.$$

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., an irreducible cubic, A is a 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

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

References

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

[2] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, New York, 1996.

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

[4] S. D. Scott, *The arithmetic of polynomial maps over a group and the structure of certain permutational polynomial groups. I*, Monatsh. Math. **73** (1969), 250–267.

Institute of Mathematics, University of Tartu, 50090 Tartu, Estonia
E-mail address: kaarli@ut.ee
E-mail address: peeter.puusemp@ut.ee