THE POLYNOMIAL FUNCTIONS ON FROBENIUS COMPLEMENTS

PETER MAYR

Institut für Algebra,
Johannes Kepler Universität Linz, Austria
peter.mayr@algebra.uni-linz.ac.at

Abstract. We determine the number of unary polynomial functions on all Frobenius complements and on all finite solvable groups all of whose abelian subgroups are cyclic.

1. Notation and results

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 $n \in \mathbb{N}_0$, $a_0, \ldots, a_n$ are in G, and $e_0, \ldots, e_{n-1}$ are integers (see [11], [15, Definition 4.4]). The set of all unary polynomial functions on G will be denoted by $P(G)$, the set of all functions from G into G by $M(G)$. For $f, g \in M(G)$, we define the product $f \cdot g$ by $f \cdot g\,(x) = f(x) \cdot g(x)$ for all $x \in G$. Then $(M(G),\cdot)$ is a group which is isomorphic to the direct product $(G^{|G|},\cdot)$. We note that $(P(G),\cdot)$ is the subgroup of $(M(G),\cdot)$ that is generated by the identity function and the constant functions on G.

Polynomial functions have been studied for several classes of groups, e.g. simple groups [8], symmetric groups [6, 7], linear groups [3, 14], and certain semidirect products of cyclic groups [13].

For a Frobenius group H with kernel A and complement G, E. Aichinger showed that

$$|P(H)| = |P(G)| \cdot |\{p|_A \mid p \in P(H) \text{ and } p(A) \subseteq A\}|^{|G|} \tag{1.1}$$

(see [1, Theorem 1.1]). Thus the problem of determining $|P(H)|$ is broken down into considering $P(G)$ and the restrictions of the polynomial functions to A. In [14] we described the latter for certain classes of groups H. In the present

Date: September 30, 2004.
AMS classification 08A40.
This work has been supported by grant P15691 of the Austrian Science Foundation (Fonds zur Förderung der wissenschaftlichen Forschung).

paper we resume the investigation of polynomial functions on Frobenius groups by determining $|P(G)|$ for every Frobenius complement G. We will use that every Frobenius complement G has a normal subgroup N such that all Sylow subgroups of N are cyclic and G/N is isomorphic to one of the following 6 groups:

$$1, \mathbb{Z}_2 \times \mathbb{Z}_2, A_4, S_4, A_5, S_5 \tag{1.2}$$

(see [4, Theorem 1.4]). Moreover, all abelian subgroups of G are cyclic. The formulae for $|P(G)|$ according to the classification in (1.2) will be given in Corollary 1.2, Theorem 1.3, and Theorem 1.5, respectively.

By [19, 6.1.11], every finite solvable group G all of whose abelian subgroups are cyclic has a normal subgroup N such that all Sylow subgroups of N are cyclic and G/N is isomorphic to one of the first 4 groups in (1.2). Hence Corollary 1.2 and Theorem 1.3 apply to those groups as well.

As a first step we determine the number of polynomial functions on coprime extensions of groups all of whose Sylow subgroups are cyclic.

Theorem 1.1. *Let G be a finite group, and let N be a normal subgroup of G such that all Sylow subgroups of N are cyclic. We assume that $|N|$ and $|G:N|$ are relatively prime. Let M_1 denote the set of Sylow subgroups of N', and let M_2 denote the set of Sylow subgroups of N/N'. Then we have*

$$|P(G)| = |P(G/N)| \cdot \prod_{P \in M_1} |P|^{2 \cdot |G:C_G(P)|} \cdot \prod_{P \in M_2} |P|^{2 \cdot |G/N' : C_{G/N'}(P)|}.$$

From Theorem 1.1 we obtain the number of polynomial functions on the groups G all of whose Sylow subgroups are cyclic. By [10, p.420, Satz 2.11], these are exactly the groups that satisfy the assumptions of the following Corollary 1.2.

Corollary 1.2. *Let $m, n, r \in \mathbb{N}$ such that $\gcd(m, n(r-1)) = 1$ and $r^n \equiv 1 \bmod m$. Let G be the group defined by*

$$G := \langle a, b \mid a^m = b^n = 1, a^b = a^r \rangle.$$

For a prime divisor p of m, let m_p denote the maximal power of p that divides m, and let t_p denote the multiplicative order of r modulo p. Then we have

$$|P(G)| = n^2 \cdot \prod_{p \mid m,\ p \text{ prime}} {m_p}^{2t_p}. \tag{1.3}$$

In [13, Theorem 3.11], the size of $P(G)$ for G as in Corollary 1.2 has been determined using a different approach. There we find the formula

$$|P(G)| = m^2 n^2 \cdot \prod_{i=2}^{n} {s_i}^2 \tag{1.4}$$

with s_i denoting the additive order of $(r-1)(r^2-1)\cdots(r^{i-1}-1)$ modulo m.

To see that (1.3) and (1.4) are equivalent, we show

$$\prod_{p|m,\ p \text{ prime}} {m_p}^{t_p} = m \cdot \prod_{i=2}^{n} s_i.$$

For a prime divisor p of m and an integer x, we write $\mu_p(x)$ for the maximal power of p that divides x. Then $\mu_p(m) = m_p$. Since s_i divides m for all $i \in \{2, \ldots, n\}$, it suffices to prove

$$ {m_p}^{t_p} = \mu_p(m \cdot \prod_{i=2}^{n} s_i) \tag{1.5}$$

for all prime divisors p of m. We note that $\mu_p(s_i)$ is the additive order of $(r-1)(r^2-1)\cdots(r^{i-1}-1)$ modulo m_p. Since p and $r^j - 1$ for $j \in \{1, \ldots, t_p - 1\}$ are relatively prime, we have $\mu_p(s_i) = m_p$ for all $i \in \{2, \ldots, t_p - 1\}$. As $r^{t_p} \equiv 1 \bmod p$, there is some integer d such that $r^{t_p} \equiv 1 + dp \bmod m_p$. By [10, p. 83, Hilfssatz 13.18], we have $(1+dp)^{m_p} \equiv 1 \bmod m_p$ and hence $r^{t_p m_p} \equiv 1 \bmod m_p$. Since $r^n \equiv 1 \bmod m_p$ and $\gcd(m_p, n) = 1$ by the assumptions on m, n, and r given in Corollary 1.2, we obtain $r^{t_p} \equiv 1 \bmod m_p$. Consequently, for $i > t_p$, we have $(r-1)(r^2-1)\cdots(r^{i-1}-1) \equiv 0 \bmod m_p$ and $\mu_p(s_i) = 1$. Hence

$$\mu_p(m) \cdot \prod_{i=2}^{n} \mu_p(s_i) = m_p \cdot \prod_{i=2}^{t_p} m_p = {m_p}^{t_p},$$

and (1.5) is proved. Thus the formulae in (1.3) and (1.4) give the same number indeed.

The following Theorem 1.3 in combination with Corollary 1.2 covers all solvable Frobenius complements.

Theorem 1.3. *Let G be a finite group all of whose abelian subgroups are cyclic, and let N be a normal subgroup of G.*

(1) *We assume that G/N is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Then we have a normal 2-complement K in G such that all Sylow subgroups of K are cyclic. Let M_1 and M_2 denote the set of Sylow subgroups of K' and of K/K', respectively. Then*

$$|P(G)| = \frac{|G:K|^4}{2^5} \cdot \prod_{P \in M_1} |P|^{2 \cdot |G : C_G(P)|} \cdot \prod_{P \in M_2} |P|^{2 \cdot |G/K' : C_{G/K'}(P)|}.$$

(2) *We assume that G/N is isomorphic to A_4. Then G has a normal Sylow 2-subgroup Q which is isomorphic to the quaternion group of order 8 such that all Sylow subgroups of G/Q are cyclic and*

$$|P(G)| = |P(G/Q)| \cdot 2^{25}.$$

(3) *We assume that G/N is isomorphic to S_4. Then G has a normal subgroup Q which is isomorphic to the quaternion group of order 8 such that all Sylow subgroups of G/Q are cyclic and*

$$|P(G)| = |P(G/Q)| \cdot 2^{60}.$$

We recall that the binary octahedral group G has a center $Z(G)$ of order 2 and that $G/Z(G)$ is isomorphic to S_4. The techniques used in the proof of Theorem 1.3 yield the following result on the binary octahedral group and other extensions of A_4 or S_4. We note that the numbers in Proposition 1.4 can be readily obtained from the GAP-package Sonata [2, 9].

Proposition 1.4.

(1) $|P(\mathrm{SL}(2,3))| = 3^2 \cdot 2^{25}$.
(2) $|P(\mathrm{GL}(2,3))| = 3^4 \cdot 2^{62}$.
(3) *Let G be the binary octahedral group. Then $|P(G)| = 3^4 \cdot 2^{62}$.*

Finally we consider the case that G is a non-solvable Frobenius complement. By [16, Theorem 18.6], G has a normal subgroup S that is isomorphic to the special linear group $\mathrm{SL}(2,5)$ such that all Sylow subgroups of G/S are cyclic. Hence $|P(G)|$ can be obtained from the next result together with Corollary 1.2.

Theorem 1.5. *Let G be a Frobenius complement with a normal subgroup S that is isomorphic to* $\mathrm{SL}(2,5)$.

(1) *If $|G:S|$ is odd, then $|P(G)| = |P(G/S)| \cdot 120^{60} \cdot 2$.*
(2) *If $|G:S|$ is even, then $|P(G)| = |P(G/S)| \cdot 120^{120}$.*

2. An auxiliary result

For a finite group G with a normal subgroup N, we define

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

By the homomorphism theorem, we then have

$$|P(G)| = |(N:G)_{P(G)}| \cdot |P(G/N)|. \tag{2.1}$$

Lemma 2.1. *Let G be a finite group, and let M, N be normal subgroups of G. We assume that M and N have relatively prime orders. Then we have*

$$|P(G)| = \frac{|P(G/M)| \cdot |P(G/N)|}{|P(G/(MN))|}.$$

Proof: Let $T := P(G)$. First we show that

$$(MN:G)_T = (M:G)_T \cdot (N:G)_T. \tag{2.2}$$

The inclusion "$\supseteq$" of (2.2) is obvious. In order to prove "$\subseteq$", we let $H := MN$ and consider the projections $\pi_M : H \to M$ and $\pi_N : H \to N$ that are defined by

$$\pi_M(xy) = x,\ \pi_N(xy) = y \text{ for all } x \in M, y \in N.$$

We show

$$\pi_M, \pi_N \in P(H). \tag{2.3}$$

Let k be an integer such that $k \equiv 1 \bmod |M|$ and $k \equiv 0 \bmod |N|$. For $x \in M$, $y \in N$, we then have $(xy)^k = x$. Hence π_M is a polynomial function on H. By $(xy)^{-k}xy = y$ for all $x \in M, y \in N$, we find $\pi_N \in P(H)$. Hence we have (2.3).

Let $f \in (H : G)_T$. By (2.3), the composed function $\pi_M \circ f$ is in $(M : G)_T$ and $\pi_N \circ f$ is in $(N : G)_T$. Together with $f(x) = \pi_M(f(x)) \cdot \pi_N(f(x))$ for all $x \in G$, this yields (2.2). By $(M : G)_T \cap (N : G)_T = (M \cap N : G)_T$ and $M \cap N = 1$, the product in (2.2) is direct.

By (2.1), we have $|P(G)| = |(H : G)_{P(G)}| \cdot |P(G/H)|$. Hence we obtain $|P(G)| = |(M : G)_{P(G)}| \cdot |(N : G)_{P(G)}| \cdot |P(G/H)|$. Multiplying this equation by $|P(G/M)| \cdot |P(G/N)|$ yields

$$|P(G)| \cdot |P(G/M)| \cdot |P(G/N)| = |P(G)|^2 \cdot |P(G/H)|.$$

From this, the result follows. □

3. Extensions of metacyclic groups

For proving Theorem 1.1, we will need the following result.

Lemma 3.1. *Let G be a finite group, and let P be a cyclic normal Sylow subgroup of G. Then we have:*

(1) $C_P(b) = 1$ *for all* $b \in G \setminus C_G(P)$;
(2) $|P(G)| = |P(G/P)| \cdot |P|^{2 \cdot |G:C_G(P)|}$.

Proof: For proving (1), we let $b \in G$ such that $C_P(b) \neq 1$. Then we have an element $a \in C_P(b)$ of prime order p. Since P is cyclic, we have $r \in \mathbb{N}$ such that $x^b = x^r$ for all $x \in P$. Hence $a^b = a$ yields $r \equiv 1 \bmod p$. Let $f \in \mathbb{N}$ such that $|P| = p^f$. Since $(1 + dp)^{p^{f-1}} \equiv 1 \bmod p^f$ for all $d \in \mathbb{N}$ by [10, p. 83, Hilfssatz 13.18], we have $b^{p^{f-1}} \in C_G(P)$. Then b is in $C_G(P)$ because p does not divide $|G : C_G(P)|$. Thus (1) is proved.

Next we show (2). By a theorem by Burnside [17, 10.1.8], we have a characteristic complement K for P in $C_G(P)$. Then K is normal in G. By Lemma 2.1, we have

$$|P(G)| = \frac{|P(G/P)| \cdot |P(G/K)|}{|P(G/(PK))|}. \tag{3.1}$$

If $PK = G$, then $|P(G/K)| = |P|^2$ and item (2) is immediate from (3.1). In the following we assume that $PK \neq G$. Then, by (1), G/K is a Frobenius

group with Frobenius kernel $A := PK/K$ and a Frobenius complement that is isomorphic to $G/C_G(P)$. Since every element of G/K acts on A via conjugation as an automorphism of the form $x \mapsto x^r$ for some integer r, we have

$$|\{q|_A \mid q \in P(G/K) \text{ and } q(A) \subseteq A\}| = |A| \cdot \exp(A).$$

Then [1, Theorem 4.1] (see also (1.1) above) yields

$$|P(G/K)| = |P(G/C_G(P))| \cdot |P|^{2 \cdot |G:C_G(P)|}. \tag{3.2}$$

By $C_G(P) = PK$, item (2) follows from (3.1) and (3.2). The lemma is proved. □

Proof of Theorem 1.1: Let G and N satisfy the assumptions of the theorem. First we consider the case that N is cyclic. We will use induction on the number of prime divisors of $|N|$. For $|N| = 1$ the theorem is trivially true. Now we assume $|N| > 1$. Let P be a non-trivial Sylow subgroup of N. For a subgroup U of G, we write $\bar{U} := (UP)/P$. By the homomorphism theorem, $\bar{G}$ and $\bar{N}$ satisfy the hypotheses of the theorem. Let M denote the set of Sylow subgroups of N. The Sylow subgroups of $\bar{N}$ are given by $\bar{Q}$ for $Q \in M$. By the induction assumption, we obtain

$$|P(G/P)| = |P(G/N)| \cdot \prod_{Q \in M \setminus \{P\}} |Q|^{2 \cdot |G:C_G(Q)|}. \tag{3.3}$$

Here we have used that G/N is isomorphic to $\bar{G}/\bar{N}$ and that $|\bar{G} : C_{\bar{G}}(\bar{Q})| = |G : C_G(Q)|$ for $Q \in M \setminus \{P\}$. From Lemma 3.1 (2) and (3.3), we obtain

$$|P(G)| = |P(G/N)| \cdot \prod_{Q \in M} |Q|^{2 \cdot |G:C_G(Q)|}. \tag{3.4}$$

Hence the theorem is proved for the case that N is cyclic.

Next we assume that N is not cyclic. By [10, p.420, Satz 2.11], we have that N' is cyclic and $\gcd(|N'|, |N : N'|) = 1$. Hence G and N' satisfy the hypotheses of the theorem. By (3.4), we have

$$|P(G)| = |P(G/N')| \cdot \prod_{Q \in M_1} |Q|^{2 \cdot |G:C_G(Q)|} \tag{3.5}$$

with M_1 the set of Sylow subgroups of N'. Let M_2 denote the set of Sylow subgroups of the cyclic group N/N'. Then (3.4) yields

$$|P(G/N')| = |P(G/N)| \cdot \prod_{Q \in M_2} |Q|^{2 \cdot |G/N:C_{G/N}(Q)|}. \tag{3.6}$$

Now the result follows from (3.5) and (3.6). □

Proof of Corollary 1.2: Let $N := \langle a \rangle$. For every Sylow p-subgroup P of N, we have $C_G(P) = C_G(\{x \in P \mid x^p = 1\})$ by Lemma 3.1 (1). For t_p the smallest

positive integer such that $r^{t_p} \equiv 1 \bmod p$, we then have $|G : C_G(P)| = t_p$. We note that $|P| = m_p$. From Theorem 1.1 we obtain

$$|P(G)| = |P(G/N)| \cdot \prod_{p|m,\ p \text{ prime}} {m_p}^{2t_p}.$$

Since G/N is cyclic of order n, we have $|P(G/N)| = n^2$ and the result follows. □

4. Extensions of the quaternion group

We will need the concept of *length* of a polynomial that was introduced by S. D. Scott in [18]. Let p be a polynomial (in the variety of all groups) in the variable x over the finite group G (cf. [11, p. 27]). We write p in the form $a_0\mathsf{x}^{e_0}a_1\mathsf{x}^{e_1}\cdots a_{n-1}\mathsf{x}^{e_{n-1}}a_n$, and define its *Scott length* $\lambda(\mathsf{p})$ (cf. [18, p. 251]) by

$$\lambda(\mathsf{p}) := \sum_{i=0}^{n-1} e_i.$$

For a polynomial p over G, let $\overline{\mathsf{p}}$ be the polynomial function induced by p on G. The *Scott length of the group* G, denoted by $\lambda(G)$, is the smallest positive integer n such that there is a polynomial p with $\lambda(\mathsf{p}) = n$ and $\overline{\mathsf{p}}(x) = 1$ for all $x \in G$.

Let q be a polynomial with $\overline{\mathsf{q}}(x) = 1$ for all $x \in G$. Then by [18, Proposition 1.1], its Scott length is a multiple of $\lambda(G)$. Hence the Scott length of a finite group divides the exponent of the group. We have $\lambda(G) = \exp(G)$ for abelian G. We note that for every normal subgroup N of G the length $\lambda(G/N)$ divides $\lambda(G)$. In particular $\exp(G/G')$ divides $\lambda(G)$.

For the proof of Theorem 1.3 and Proposition 1.4, we will use the following criterion to decide whether a given function is polynomial.

Lemma 4.1. *Let G be a finite group, let Q be a normal subgroup of G such that Q is a quaternion group of order 8, and let $Z := Q'$. We assume that G/Z is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, A_4, or S_4. Let $\lambda := \lambda(G/Z)$ be the Scott length of G/Z. Then the following are equivalent for each function $f : G \to Z$:*

(1) *The function f is in $P(G)$;*
(2) *There exists an integer μ such that*

$$f(x \cdot z) = f(x) \cdot z^{\lambda\mu} \text{ for all } x \in G,\ z \in Z.$$

The assumptions of this lemma are satisfied for the quaternion group of order 8, $\mathrm{SL}(2,3)$, $\mathrm{GL}(2,3)$, and the binary octahedral group. We note that $\lambda(\mathbb{Z}_2 \times \mathbb{Z}_2) = 2$, $\lambda(A_4) = 3$, and $\lambda(S_4) = 2$ (see the proof of Lemma 4.2 below).

Proof of Lemma 4.1: Since Z is characteristic in Q, we have that Z is normal in G. Together with $|Z| = 2$, this yields that Z is central in G. Hence the implication (1) ⇒ (2) is immediate.

It remains to prove (2) $\Rightarrow$ (1). To this end, we will show the existence of certain interpolation functions in $(Z : G)_{P(G)}$. By the definition of λ, we have a function $i \in P(G)$ such that

$$i(G) \subseteq Z \text{ and } i(z) = z^\lambda \text{ for all } z \in Z. \tag{4.1}$$

By assumption, $Q = G$ or Q/Z is the unique minimal normal subgroup of G/Z and $C_{G/Z}(Q/Z) = Q/Z$. Hence, by [5, Theorem 4.1 (2)], we have $e \in P(G)$ such that

$$e(q) \in qZ \text{ for all } q \in Q \text{ and } e(G \setminus Q) \subseteq Z. \tag{4.2}$$

We choose a to be an element of order 4 in Q. Then $c := a^2$ generates Z. We define $p \in P(Q)$ by

$$p(x) = x \cdot x^a \text{ for all } x \in Q.$$

Then p satisfies

$$p(aZ) = \{c\} \text{ and } p(Q \setminus aZ) = \{1\}. \tag{4.3}$$

For $t \in G$, we define $p_t \in P(G)$ by

$$p_t(x) = p(e(at^{-1}x)) \text{ for all } x \in G.$$

From (4.2) and (4.3), we obtain that

$$p_t(tZ) = \{c\} \text{ and } p_t(G \setminus tZ) = \{1\}. \tag{4.4}$$

We are ready for the interpolation argument. Let $f : G \to Z$ be a function that satisfies (2) with $\mu \in \mathbb{Z}$. We consider the function g on G that is defined by

$$g(x) = f(x) \cdot i(x)^{-\mu} \text{ for all } x \in G.$$

Then $g(G) \subseteq Z$ and $g(xz) = g(x)$ for all $x \in G, z \in Z$ by (4.1). Since g is constant on each coset of Z in G, it is the product of certain functions p_t for $t \in G$ by (4.4). Hence $g \in P(G)$. By $i \in P(G)$, this implies $f \in P(G)$. The lemma is proved. □

The number of polynomial functions on the quaternion group of order 8 follows easily. For results on the generalized quaternion groups we have to refer to [12].

Lemma 4.2. *Let G be a finite group, let Q be a normal subgroup of G such that Q is a quaternion group of order 8, and let $Z := Q'$. Then we have:*

1. *$P(Q) = 2^7$.*
2. *If G/Z is isomorphic to A_4, then $P(G) = 3^2 \cdot 2^{25}$.*
3. *If G/Z is isomorphic to S_4, then $P(G) = 3^4 \cdot 2^{62}$.*

Proof: The group Q/Q' is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and has Scott length 2. By Lemma 4.1, a function $f : Q \to Q'$ is in $P(Q)$ if and only if f is constant on all cosets of Q' in Q. Hence

$$|(Q' : Q)_{P(Q)}| = 2^4.$$

By $|P(Q/Q')| = 2^3$ and (2.1), we obtain (1).

For proving (2), we first show

$$\lambda(A_4) = 3. \tag{4.5}$$

We define the polynomial $\mathsf{q} = \mathsf{x}^{-3} \cdot (\mathsf{x}^3)^{(1,2,3)} \cdot (\mathsf{x}^3)^{(1,3,2)}$ over A_4. Then $\overline{\mathsf{q}}(x) = 1$ for all $x \in A_4$. By [18, Proposition 1.1], $\lambda(A_4)$ divides the Scott length of q, which is 3. Since $\exp(A_4/{A_4}')$ divides $\lambda(A_4)$, we have (4.5).

For G such that G/Z is isomorphic to A_4, Lemma 4.1 yields

$$|(Q' : G)_{P(G)}| = 2^{12} \cdot 2. \tag{4.6}$$

Together with $|P(A_4)| = 2^{12} \cdot 3^2$ (see [14, Example 5.20] or [5, Example 2]), we obtain (2).

For (3), we show

$$\lambda(S_4) = 2. \tag{4.7}$$

The polynomial $\mathsf{q} = (\mathsf{x}^2 \cdot (\mathsf{x}^2)^{(1,2)})^2 \cdot \mathsf{x}^6 \cdot (\mathsf{x}^{-6})^{(1,2,3)} \cdot (\mathsf{x}^{-6})^{(1,3,2)}$ over S_4 satisfies $\overline{\mathsf{q}}(x) = 1$ for all $x \in S_4$. Since $\lambda(\mathsf{q}) = 2$ and $\lambda(S_4) > 1$, we have (4.7).

We assume that G/Z is isomorphic to S_4. By Lemma 4.1, we obtain

$$|(Q' : G)_{P(G)}| = 2^{24}.$$

Together with $|P(S_4)| = 2^{38} \cdot 3^4$ (see [5, Example 3]), this yields (3). □

Proof of Proposition 1.4: Since $\mathrm{SL}(2,3)$ satisfies the assumptions of Lemma 4.2 (2), we have assertion (1) of the proposition. Both $\mathrm{GL}(2,3)$ and the binary octahedral group satisfy the assumptions of Lemma 4.2 (3). Hence we have (2) and (3). □

5. Frobenius complements

Proof of Theorem 1.3: Let G be a finite group, and let N be a normal subgroup of G. We assume that all abelian subgroups of G are cyclic and that G/N is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, A_4, or S_4. Then every non-trivial Sylow p-subgroup of G has exactly one subgroup of order p. By [17, 5.3.6], the Sylow 2-subgroups of G are generalized quaternion groups and the Sylow p-subgroups of G for p odd are cyclic. We note that all Sylow subgroups of N are cyclic.

First we consider the case that G/N is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. By [17, 10.1.9], N has a normal 2-complement K, that is, N has a normal subgroup K such that $|K|$ is odd and $|N : K|$ is a power of 2. Then K is a normal 2-complement in G. Let Q be a Sylow 2-subgroup of G. With M_1 and M_2 denoting the set of Sylow subgroups of K' and of K/K', respectively, Theorem 1.1 yields

$$|P(G)| = |P(Q)| \cdot \prod_{P \in M_1} |P|^{2 \cdot |G : C_G(P)|} \cdot \prod_{P \in M_2} |P|^{2 \cdot |G/N' : C_{G/N'}(P)|}. \tag{5.1}$$

In [12] (see also Lemma 4.2 (1) above) the number of polynomial functions on the generalized quaternion group Q is given as

$$|P(Q)| = 2^{4t-5} \text{ for } |Q| = 2^t. \tag{5.2}$$

Now the formula given in Theorem 1.3 (1) follows from (5.1) and (5.2).

Next we assume that G/N is isomorphic to A_4. Let Q be a Sylow 2-subgroup of G. Since the non-trivial elements of $(QN)/N$ are permuted transitively under conjugation by elements in G/N, we have that

$$Q \text{ is a quaternion group of order 8 and } Q \subseteq G'. \tag{5.3}$$

We show that

$$Q \text{ is the unique Sylow } 2-\text{subgroup in } G. \tag{5.4}$$

For $U \leq G$, we write $\bar{U} := (UN')/N'$. Since $\bar{N}$ is a cyclic normal subgroup of $\bar{G}$, it is centralized by $\bar{G}'$. Then $\bar{Q} \subseteq C_{\bar{G}}(\bar{N})$ by (5.3). Hence

$$QN' \text{ is normal in } QN. \tag{5.5}$$

Because N' is cyclic, it is centralized by G'. Thus $Q \subseteq C_G(N')$ and, by (5.5), Q is normal in QN. Since $|G : QN| = 3$, we then obtain (5.4). All Sylow subgroups of G/Q are cyclic.

As in case (1), we note that N has a normal 2-complement K. Then $QK = QN$. By Lemma 2.1, we have

$$|P(G)| = \frac{|P(G/Q)| \cdot |P(G/K)|}{|P(G/(QK))|}.$$

Since QK has index 3 in G, we find $|P(G/(QK))| = 3^2$. The quotient G/K satisfies the assumptions of Lemma 4.2 (2). Hence we have $|P(G/K)| = 3^2 \cdot 2^{25}$, and the result in item (2) follows.

We now consider the case that G/N is isomorphic to S_4. Then G has a normal subgroup H of index 2 such that H/N is isomorphic to A_4. By (2), we have a unique Sylow 2-subgroup Q in H, and Q is isomorphic to the quaternion group of order 8. Hence Q is normal in G, and all Sylow subgroups of G/Q are cyclic.

Let K be the normal 2-complement in N. Then K is normal in G. The quotient G/K satisfies the assumptions of Lemma 4.2 (3). Hence we have $P(G/K) = 3^4 \cdot 2^{62}$. Since $G/(QK)$ is isomorphic to S_3, Corollary 1.2 yields $|P(G/(QK))| = 2^2 \cdot 3^4$. By Lemma 2.1, we obtain the formula given in (3). The proof of the theorem is complete. □

Proof of Theorem 1.5: Let G be a Frobenius complement, and let S be a normal subgroup of G such that S is isomorphic to $\mathrm{SL}(2, 5)$.

First we assume that G/S has odd order. Then S has a direct complement M in G and $\gcd(|S|, |M|) = 1$ by [16, Theorem 18.6]. Hence $|P(G)| = |P(S)| \cdot |P(M)|$

by Lemma 2.1. By [3, Corollary 2.2], we have $|P(\mathrm{SL}(2,5))| = 120^{60} \cdot 2$. Thus Theorem 1.5 (1) is proved.

Next we assume that G/S has even order. By [16, Theorem 18.6], we have a normal subgroup M of G such that $\gcd(|S|, |M|) = 1$ and $|G : SM| = 2$. Lemma 2.1 yields

$$|P(G)| = \frac{|P(G/S)| \cdot |P(G/M)|}{4}. \tag{5.6}$$

It remains to determine $|P(G/M)|$. We note that M has a complement H in G with $S \subseteq H$ by the Schur-Zassenhaus Theorem [17, 9.1.2]. We show that H satisfies the assumptions of [3, Theorem 2.1]. To this end, we prove that S and $Z := Z(S)$ are the only non-trivial, proper normal subgroups of H.

Seeking a contradiction, we let N be a proper normal subgroup of H such that $N \not\subseteq S$. Then we have $NS = H$ by $|H : S| = 2$. Thus

$$H/N \cong S/(N \cap S). \tag{5.7}$$

Since S is quasisimple, we have $N \cap S \subseteq Z$. Thus $|N \cap S| \leq 2$ and, by (5.7), $|N| \in \{2, 4\}$. In any case, NZ has order 4 and $H/(NZ)$ is isomorphic to S/Z, that is to A_5. Then NZ is a central subgroup of order 4 in H. This contradicts the fact that the Sylow 2-subgroups of H are generalized quaternion groups of order 16 by [17, 10.5.6 (ii)]. Thus all proper normal subgroups of H are contained in S.

The normal subgroups of S are $1, Z$, and S. By $Z = Z(H)$ and $S = H'$, all of them are normal in H, and H has property (A) (see [3, p. 5629]). Then [3, Theorem 2.1] yields

$$|P(H)| = |S|^{|H:Z|} \cdot \mathrm{lcm}(\exp H/S, \exp Z) \cdot |H : S|.$$

Thus $|P(H)| = 120^{120} \cdot 4$. Since G/M is isomorphic to H, Theorem 1.5 (2) follows from (5.6). □

References

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

[2] E. Aichinger, F. Binder, J. Ecker, P. Mayr, and C. Nöbauer. *SONATA - system of near-rings and their applications, GAP package, Version 2*, 2003. (`http://www.algebra.uni-linz.ac.at/Sonata/`).

[3] E. Aichinger and P. Mayr. Polynomial functions and endomorphism near-rings on certain linear groups. *Communications in Algebra*, 31(11):5627–5651, 2003.

[4] R. Brown. Frobenius groups and classical maximal orders. *Mem. Amer. Math. Soc.*, 151(717), 2001.

[5] Y. Fong and K. Kaarli. Unary polynomials on a class of groups. *Acta Sci. Math. (Szeged)*, 61(1-4):139–154, 1995.

[6] Y. Fong and J. D. P. Meldrum. The endomorphism near-rings of the symmetric groups of degree at least five. *J. Austral. Math. Soc. Ser. A*, 30(1):37–49, 1980/81.
[7] Y. Fong and J. D. P. Meldrum. The endomorphism near-ring of the symmetric group of degree four. *Tamkang J. Math.*, 12(2):193–203, 1981.
[8] A. Fröhlich. The near-ring generated by the inner automorphisms of a finite simple group. *J. London Math. Soc.*, 33:95–107, 1958.
[9] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.3*, 2002. (`http://www.gap-system.org`).
[10] B. Huppert. *Endliche Gruppen. I.* Springer-Verlag, Berlin, 1967.
[11] H. Lausch and W. Nöbauer. *Algebra of polynomials*. North-Holland, Amsterdam, London; American Elsevier Publishing Company, New York, 1973.
[12] J. J. Malone. Generalised quaternion groups and distributively generated near-rings. *Proc. Edinburgh Math. Soc. (2)*, 18:235–238, 1973.
[13] J. J. Malone and G. Mason. ZS-metacyclic groups and their endomorphism near-rings. *Monatsh. Math.*, 118(3-4):249–265, 1994.
[14] P. Mayr. *Polynomial functions on classical groups and Frobenius groups*. PhD thesis, Johannes Kepler University Linz, 2004. Available at `http://www.algebra.uni-linz.ac.at/~stein/thesis.pdf`.
[15] R. N. McKenzie, G. F. McNulty, and W. F. Taylor. *Algebras, lattices, varieties, Volume I.* Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, California, 1987.
[16] D. Passman. *Permutation groups*. W. A. Benjamin, Inc., New York-Amsterdam, 1968.
[17] D. J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.
[18] S. D. Scott. The arithmetic of polynomial maps over a group and the structure of certain permutational polynomial groups. I. *Monatsh. Math.*, 73:250–267, 1969.
[19] J. A. Wolf. *Spaces of constant curvature*. McGraw-Hill Book Co., New York, 1967.