The Transfer in the Invariant Theory of Modular Permutation Representations

Mara D. Neusel

PACIFIC JOURNAL OF MATHEMATICS

– TO APPEAR –

AMS CLASSIFICATION : 13A50 Invariant Theory
KEY WORDS : Polynomial Invariants of Finite Groups, Permutation Representation, Transfer, p-Regular Representation

Typeset by $\mathcal{LS}$TEX

SUMMARY : *This note investigates the image of the transfer homomorphism for permutation representations of finite groups over finite fields. One obtains a number of results showing that the image of the transfer* Im(Tr) *together with certain Chern classes generate the ring of invariants as an algebra. By a careful analysis of orbit sums one finds the surprising fact that the ideal* Im(Tr) *is a prime ideal for cyclic* p*-groups and determines an upper bound on its height.*

§1. Introduction

Let $\mathbb{F}$ be a finite field of $\mathrm{char}(\mathbb{F}) = p$. Let $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful representation of a finite group G. The group G acts via ρ on the n-dimensional vector space $V = \mathbb{F}^n$. This induces an action of G on the ring of polynomial functions $\mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[V]$, where $x_1, \ldots, x_n$ is the standard dual basis of V^*, via

$$gf(v) := f(\rho(g)^{-1} v) \quad \forall\, g \in G, f \in \mathbb{F}[x_1, \ldots, x_n]$$

Denote by $\mathbb{F}[V]^G$ the ring of polynomials invariant under the G-action. The transfer

$$\mathrm{Tr}^G : \mathbb{F}[V] \longrightarrow \mathbb{F}[V]^G;\ f \longmapsto \sum_{g \in G} gf$$

is a $\mathbb{F}[V]^G$-module homomorphism. It is surjective if and only if the characteristic of the ground field $\mathbb{F}$ does not divide the group order, i.e., in the nonmodular case, where it provides a tool for constructing the ring of invariants $\mathbb{F}[V]^G$. In the modular case very little is known about the image $\mathrm{Im}(\mathrm{Tr}^G)$, see [9] Section 11.5, [3], [5], [7], [8] and [10].

In this note we discuss the transfer for permutation representations. By a **permutation representation** $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ we understand a linear representation together with a basis $X = \{x_1, \ldots, x_n\}$ for $\mathbb{F}^n$, or its dual, refered to as the **permutation basis**, such that G permutes the elements of X. It turns out that the image of the transfer for cyclic p-groups is a prime ideal of height at most $n - k$, where k denotes the number of orbits of a permutation basis. In the special case of sums of copies of the regular representation of cyclic p-groups this upper bound on the height can be considerably improved. We generalize these results to arbitrary groups G with appropriate p-Sylow sub group. This is the contents of Section 2.

In Section 3 we consider sums of copies of the regular representation of arbitrary p-groups. It transpires that the transfer is surjective exactly in degrees prime to the characteristic.

This allows us in Section 4 to describe a generating set as an algebra of the ring of invariants of $\mathbb{Z}/p$ in any permutation representation, and also for the ring of invariants of a group with order $2p$ in its regular representation: both consist of the image of the transfer and certain Chern classes.

This applies to the regular representation of $\mathbb{Z}/4$ over a field of characteristic two, i.e., to one of Marie-José Bertin's famous examples and leads to a description of this ring of invariants, which appears in Section 5.

This work was done during my stay at Université de Toulouse Paul Sabatier in september 1996 and in february and march 1997. I would like to thank Claude Hayat-Legrand for the invitation and her hospitality. I would like to thank Manfred Göbel for many discussions. I am deeply indebt to Larry Smith for comments and suggestions on preliminary versions of this paper.

§2. Primality of the Image of the Transfer

In this section we show that the image of the transfer is a prime ideal for permutation representations. Moreover one can give an upper bound for the height. This generalizes results in [12].

Let $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a modular permutation representation of a finite group G permuting a basis $x_1, \ldots, x_n$ for the dual vector space V^*. Denote by

$$x^E = x_1^{E_1} \cdots x_n^{E_n} \in \mathbb{F}[x_1, \ldots, x_n]$$

a monomial, and by $[x^E] = \{x^{E'} \mid \exists\, g \in P \text{ with } gx^E = x^{E'}\}$ the set of its orbit elements. Then the orbit sums of monomials

$$o(x^E) = \sum_{x^{E'} \in [x^E]} x^{E'}$$

form an $\mathbb{F}$-basis for the ring $\mathbb{F}[V]^P$ of invariants, [9] Lemma 1.3.3 and Lemma 4.2.1.

If x^E is a monomial, then the orbit of x^E contains r elements for some $r \mid |G|$ and one says the orbit $[x^E]$, resp. the orbit sum $o(x^E)$, has length r. The following lemma provides a useful bound on the length of orbits of products.

LEMMA 2.1: *Let $\rho : P \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a modular permutation representation of a cyclic group P of order p^t. Let x^E and x^F be monomials in $\mathbb{F}[V]$ with orbit length r, resp. s. Then the orbit length of their product $x^E x^F$ is at most equal to* $\min(r, s)$.

PROOF: Denote by P_{x^E}, resp. P_{x^F} the isotropy groups of x^E, resp. x^F. Since the orbit length is r, resp. s, the order of these groups is given by

$$|P_{x^E}| = \frac{|P|}{r} \quad \text{and} \quad |P_{x^F}| = \frac{|P|}{s}.$$

The lattice of subgroups of P form a single chain, therefore for $r \geq s$

$$P_{x^E x^F} \supset P_{x^E} \cap P_{x^F} = P_{x^E}.$$

Hence

$$|P_{x^E x^F}| \geq |P_{x^E}| = \frac{|P|}{r},$$

and therefore

$$|o(x^E x^F)| \leq \frac{|P|}{|P_{x^E x^F}|} \leq r,$$

which was to be shown •

The following two examples show that the preceding lemma does not extend to arbitrary cyclic groups nor to non cyclic p-groups.

EXAMPLE 2.2 : Consider the regular representation of the cyclic group of order six $\rho : \mathbb{Z}/6 \hookrightarrow \mathrm{GL}(6, \mathbb{F})$ afforded by the matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Then the orbit sums

$$o(x_1x_3x_5) = x_1x_3x_5 + x_2x_4x_6 \quad \text{and} \quad o(x_1x_4) = x_1x_4 + x_2x_5 + x_3x_6$$

have length 2, resp. 3, but their product

$$o(x_1x_3x_5)o(x_1x_4) = o(x_1^2x_3x_4x_5) = \mathrm{Tr}(x_1^2x_3x_4x_5)$$

has orbit length 6.

EXAMPLE 2.3 : Consider the regular representation $\varrho : \mathbb{Z}/2 \times \mathbb{Z}/2 \hookrightarrow \mathrm{GL}(4, \mathbb{F})$ of the Klein 4-group, afforded by the matrices

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Then the orbit sums

$$o(x_1x_2) = x_1x_2 + x_3x_4 \quad \text{and} \quad o(x_1x_4) = x_1x_4 + x_2x_3$$

have orbit length 2, but their product

$$o(x_1x_2)o(x_1x_4) = o(x_1^2x_2x_4) = \mathrm{Tr}(x_1^2x_2x_4)$$

has orbit length 4.

THEOREM 2.4: *Let $\varrho : P \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a permutation representation of a cyclic p-group P of order p^t. Then the image of the transfer is a prime ideal in $\mathbb{F}[V]^P$ of height at most $n - k$, where k is the number of orbits of P acting on the basis $x_1, \ldots, x_n$ for V^*.*

PROOF: If x^E and x^F are monomials, and their orbits $[x^E]$, $[x^F]$ have lengths p^i, p^j resp., then the product of their orbit sums $o(x^E)o(x^F)$ contains the monomial $x^Ex^F = x^{E+F}$ which has orbit length at most $p^k = \min\{p^i, p^j\}$, i.e., $k = \min\{i, j\}$, by Lemma 2.1. The product $o(x^E)o(x^F)$ when expressed as a linear combination of orbit sums contains $o(x^{E+F})$ with coefficient 1. Moreover if $o(x^H)$ is an arbitrary orbit sum occurring in the expression of $o(x^E)o(x^F)$ as an $\mathbb{F}$-linear combination of orbit sums, then the orbit of x^H contains an element $x^{E'}x^{F'}$ where $x^{E'}$ is in the orbit of x^E and $x^{F'}$ is in the orbit of x^F. Therefore the orbit length of $o(x^H)$ is at most $p^k = \min\{p^i, p^j\}$ also. Let $f \in \mathbb{F}[V]^P$ and $|P| = p^t$, then one has

$$f = f_0 + f_1 + \cdots + f_t$$

where for $i = 0, \ldots, t$, and f_i is a linear combination of orbit sums $o(x^{E(i)})$ of length p^i. Note that the elements in the image of the transfer are precisely the linear combinations of the orbit sums of length $p^t = |P|$. Hence if $f \notin \mathrm{Im}(\mathrm{Tr}^P)$ then some f_i for $i < t$ must be nonzero. Suppose that $f, h \in \mathbb{F}[V]^P$ and $f, h \notin \mathrm{Im}(\mathrm{Tr}^P)$. Write

$$f = f_i + \cdots + f_t \text{ where } f_i \neq 0, \ i < t$$
$$h = h_j + \cdots + h_t \text{ where } h_j \neq 0, \ j < t.$$

We next show $fh \notin \mathrm{Im}(\mathrm{Tr}^P)$. Since $h_t \in \mathrm{Im}(\mathrm{Tr}^P)$

$$fh_t \in \mathrm{Im}(\mathrm{Tr}^P)$$

also. Hence if $f(h - h_t) = fh - fh_t \notin \mathrm{Im}(\mathrm{Tr}^P)$ then $fh \notin \mathrm{Im}(\mathrm{Tr}^P)$, so without loss of generality one may suppose

$$h = h_j + \cdots + h_{t-1}.$$

Likewise by symmetry one may suppose

$$f = f_i + \cdots + f_{t-1}.$$

The analysis of products of orbit sums of monomials above shows that f_rh_s can always be expressed as a linear combination of orbit sums of length at most $p^{\min\{r, s\}} = \min\{p^r, p^s\}$. In particular fh itself is a linear combination of orbit sums whose length is at most p^{t-1}. Since $\mathbb{F}[V]^P$ is a domain $fh \neq 0$ and therefore at least one of these orbit sums has a nonzero coefficient. $\mathrm{Im}(\mathrm{Tr}^P)$ is however the $\mathbb{F}$-linear span of the orbit sums of length p^t and therefore $fh \notin \mathrm{Im}(\mathrm{Tr}^P)$ as was to be shown.

In order to establish the upper bound[1] for the height, assume that $X = \{x_1, \ldots, x_n\}$, the basis set, consists of k orbits of P, say the orbits of $x_1, \ldots, x_k$. Then the k top orbit Chern classes $c_{\mathrm{top}}(x_1), \ldots, c_{\mathrm{top}}(x_k)$ are algebraically independent, hence generate a polynomial subalgebra $\mathbb{F}[c_{\mathrm{top}}(x_1), \ldots, c_{\mathrm{top}}(x_k)]$ of Krull dimension k in the ring of invariants. Since

$$\mathbb{F}[c_{\mathrm{top}}(x_1), \ldots, c_{\mathrm{top}}(x_k)] \cap \mathrm{Im}(\mathrm{Tr}^P) = 0$$

it follows that

$$\mathbb{F}[c_{\mathrm{top}}(x_1), \ldots, c_{\mathrm{top}}(x_k)] \hookrightarrow \mathbb{F}[V]^P/\mathrm{Im}(\mathrm{Tr}^P).$$

Therefore

$$\dim(\mathbb{F}[V]^P/\mathrm{Im}(\mathrm{Tr}^P)) \geq k,$$

i.e.,

$$\hbar t(\mathrm{Im}(\mathrm{Tr}^P)) \leq n - k$$

as claimed •

The preceding result was generalized to arbitrary cyclic permutation groups in [8], Corollary 5.2 and Corollary 6.2. However, we have even more:

COROLLARY 2.5: *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful representation of a finite group G with cyclic p-Sylow sub group $\mathrm{Syl}_p(G)$. If the restriction of ϱ to $\mathrm{Syl}_p(G)$ is a permutation representation, then the image of the transfer $\mathrm{Im}(\mathrm{Tr}^G)$ of G is prime of height at most $n - k$, where k is the number of orbits of $\mathrm{Syl}_p(G)$ acting on the basis $x_1, \ldots, x_n$ of V^*.*

PROOF: We have just proved that the image of the transfer of the p-Sylow subgroup is prime of height $n - k$. By Theorem 5.1 in [8] we have

$$\mathrm{Im}(\mathrm{Tr}^G) = \mathrm{Im}(\mathrm{Tr}^{\mathrm{Syl}_p(G)}) \cap \mathbb{F}[V]^G.$$

Therefore also $\mathrm{Im}(\mathrm{Tr}^G)$ is prime. It has the same height, because

$$\mathbb{F}[V]^G \hookrightarrow \mathbb{F}[V]^{\mathrm{Syl}_p(G)}$$

is an integral extension of integral domains, in particular we have the going-down property •

Theorem 2.4 can be considerably improved if we restrict to regular representations. For this we require a lemma.

LEMMA 2.6: *Let $\varrho : P \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be the regular representation of a p-group P of order p^t, so $n = p^t$. Then the Chern classes $c_p, \ldots, c_{p^t}$ of p-power degree are not contained in the image of the transfer.*

PROOF: The Chern class c_i is by definition the i-th elementary symmetric function in the orbit elements $x_1, \ldots, x_{p^t}$. Consider those of prime power degree, namely $c_p, \ldots, c_{p^t}$. Then c_{p^i} is the sum of all monomials

$$x_{k_1} \cdots x_{k_{p^i}},$$

where the k_j's are pairwise distinct. So, these monomials form a single Σ_{p^t}-orbit and possibly several P-orbits. The number of these monomials is $\binom{p^t}{p^i}$, which is not divisible[2] by the group order p^t. At least one of these orbits contains less than p^t elements. Hence c_{p^i} can be expressed as a linear combination of orbit sums where at least one is of length strictly less than $p^t = |P|$. Hence $c_{p^i} \notin \mathrm{Im}(\mathrm{Tr}^P)$ •

[1] This proof is adapted from [7], where this upper bound is shown to hold for arbitrary representations of p-groups.

[2] This may be verified by induction on i.

REMARK: If ϱ is a direct sum of k copies of the regular representation, i.e., $n = kp^t$, one gets analogously

$$c_{p^i}(x_j) \notin \mathrm{Im}(\mathrm{Tr}^P), \text{ for } j = 1, \ldots, k,$$

where the set of basis elements $X = \{x_1, \ldots, x_n\} = \bigsqcup_{i=1}^{k}[x_i]$ is the disjoint union of the k orbits of $x_1, \ldots, x_k$.

COROLLARY 2.7: *Let $\varrho : P \hookrightarrow GL(n, \mathbb{F})$ be the regular representation of a cyclic p-group P of order p^t, so $n = p^t$. Then the image of the transfer is a prime ideal of height at most $n - t = p^t - t$.*

PROOF: By Theorem 2.4 the image of the transfer is a prime ideal. Since ϱ is the regular representation, the set of basis elements $X = \{x_1, \ldots, x_n\}$ consists of exactly one orbit. By Lemma 2.6 the Chern classes of prime power degree, $c_p, \ldots, c_{p^t}$ are not contained in the image of the transfer. Since $c_p, \ldots, c_{p^t}$ are algebraically independent, they generate a polynomial subalgebra of the ring of invariants, which intersects with $\mathrm{Im}(\mathrm{Tr}^P)$ in the zero ideal. Hence

$$\hbar t\,(\mathrm{Im}(\mathrm{Tr}^P)) \leq n - \dim\,(\mathbb{F}[c_p, \ldots, c_{p^t}]) = n - t = p^t - t$$

as claimed •

REMARK: Under the weaker assumption that ϱ is a direct sum of k copies of the regular representation, i.e., $n = kp^t$, one gets

$$\hbar t(\mathrm{Im}(\mathrm{Tr}^P)) \leq n - tk = k(p^t - t).$$

The proof works analogously.

Like Theorem 2.4 also Corollary 2.7 has a generalization to groups with appropriate p-Sylow sub group.

COROLLARY 2.8: *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful representation of a finite group G with cyclic p-Sylow sub group $\mathrm{Syl}_p(G)$ of order $p^t(= n)$. If the restriction of ϱ to $\mathrm{Syl}_p(G)$ is the regular representation, then the image of the transfer $\mathrm{Im}(\mathrm{Tr}^G)$ of G is prime of height at most $n - t$.*

PROOF: •

§3. p-Regular Representations

DEFINITION: *A representation $G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ of a finite group G over a field of characteristic p is called* p**-regular** *if the restriction to a p-Sylow subgroup of G, $\mathrm{Syl}_p(G)$, is a direct sum of copies of the regular representation of $\mathrm{Syl}_p(G)$.*

The main result of this section follows from a simple lemma.

LEMMA 3.1: *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be the regular representation of a finite group G. Then for all subgroups $H < G$ the restriction*

$$\varrho\,|_H : H \hookrightarrow \mathrm{GL}(n, \mathbb{F})$$

is the direct sum of $|\ G : H\ |$ copies of the regular representation of H.

PROOF: If ϱ is the regular representation of G then the set $X = \{x_1, \ldots, x_n\}$ of basis element of V^* is a finite G-set with G acting freely. Hence for any subgroup $H < G$ the set X is the disjoint union of $|\ G : H\ |$ H-sets with, H acting freely on each copy •

REMARK: The above lemma remains true under the weaker assumption that ϱ is a direct sum of copies of the regular representation. The proof works unchanged.

THEOREM 3.2: *Let $P \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be the regular representation of a p-group of order p^t. Then the transfer is surjective in degree ℓ if and only if ℓ is prime to $p = \mathrm{char}(\mathbb{F})$.*

PROOF: Since ϱ is the regular representation, it is in particular a permutation representation. Hence any invariant polynomial f is a sum of orbitsums $o(x^E)$ of monomials $x^E = x_1^{e_1} \cdots x_n^{e_n} \in \mathbb{F}[x_1, \ldots, x_n]$. Let $f = \sum_\alpha o(x^{E_\alpha}) \in \mathbb{F}[V]^P$, $f \notin \mathrm{Im}(\mathrm{Tr}^P)$. Then at least one monomial x^{E_α} has orbit length less than the order of P, $|\, o(x^{E_\alpha})\, | < |\, P\, |$. This means that the isotropy group of x^{E_α} is nontrivial, hence there exists an element $g \in P$ such that

$$g x^{E_\alpha} = x^{E_\alpha}.$$

Denote by $< g > \subset P$ the cyclic subgroup generated by g. Then x^{E_α} is a product of top orbit Chern classes of the subgroup $< g >$

$$x^{E_\alpha} = \prod_{j=1}^{n} c_{\mathrm{top}}^{<g>}(x_j)^{\beta_j},$$

and its degree is

$$\deg(x^{E_\alpha}) = \sum_{j=1}^{n} (\deg(c_{\mathrm{top}}^{<g>}(x_j))\beta_j$$

By Lemma 3.1 $< g >$ acts on the standard basis $x_1, \ldots, x_n$ without fixed points. Therefore, p divides every summand on the right side, and hence $\deg(x^{E_\alpha})$.

In order to prove the reverse conclusion consider the p-th Chern class $c_p \in \mathbb{F}[V]^P$ of x_1. By Lemma 2.6 c_p is not in the image of the transfer. The same argument shows that no power of the p-th Chern class can be in the image of the transfer: an arbitrary power of the p-th Chern class, $c_p^{kp^s} = (c_p^k)^{p^s}$, where p does not divide k, is a sum of

$$\binom{\frac{p^t!}{p!(p^t-p)!} + k - 1}{k} = \frac{\left(\frac{p^t!}{p!(p^t-p)!} + k - 1\right)!}{k!\left(\frac{p^t!}{p!(p^t-p)!} - 1\right)!}$$

monomials. Since this is not divisible by the group order p^t, which may be verified by induction on k, $c_p^{kp^s}$ can be expressed as a linear combination of orbit sums where at least one is of length strictly less than $p^t = |P|$. Hence $c_p^{kp^s} \notin \mathrm{Im}(\mathrm{Tr}^P)$. Therefore in any degree ℓ which is divisible by p the transfer is not surjective, since it does not contain the appropriate power of c_p •

REMARK: The above theorem remains true under the weaker assumption that ϱ is a direct sum of copies of the regular representation. Apart from a more cumbersome notation the proof works unchanged.

COROLLARY 3.3: *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a p-regular representation of a finite group G. Then the transfer, Tr^G, is surjective in degrees prime to the characteristic.*

PROOF: Let $f \in \mathbb{F}[V]^G$ have degree not divisible by p. By Theorem 3.2 $f \in \mathbb{F}[V]^{\mathrm{Syl}_p(G)}$ is contained in the image of the transfer $\mathrm{Tr}^{\mathrm{Syl}_p(G)}$. Hence there exists a polynomial $\overline{f} \in \mathbb{F}[V]$, such that

$$\mathrm{Tr}^{\mathrm{Syl}_p(G)}(\overline{f}) = f.$$

Since the index d of a p-Sylow subgroup $\mathrm{Syl}_p(G)$ in G is prime to p we have

$$f = \frac{1}{d}\mathrm{Tr}^G_{\mathrm{Syl}_p(G)}(f) = \frac{1}{d}\mathrm{Tr}^G_{\mathrm{Syl}_p(G)}\mathrm{Tr}^{\mathrm{Syl}_p(G)}(\overline{f}) = \mathrm{Tr}^G_{\mathrm{Syl}_p(G)}\mathrm{Tr}^{\mathrm{Syl}_p(G)}\left(\frac{1}{d}\overline{f}\right),$$

i.e., $f \in \mathrm{Im}(\mathrm{Tr}^G)$ •

The following examples show that Theorem 3.2, resp. the remark following it, are not true under the weaker assumption that ρ is an arbitrary permutation representation.

EXAMPLE 3.4 : Consider the representation

$$\rho : \mathbb{Z}/4 \hookrightarrow \mathrm{GL}(6, \mathbb{F}_2)$$

of the cyclic group of order 4 over the field with 2 elements afforded by the matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

The orbitsum of the monomial x_5 is

$$o(x_5) = x_5 + x_6$$

and hence not in the image of the transfer even though it has degree prime to the characteristic.

EXAMPLE 3.5 : Consider the representation

$$\rho : \mathbb{Z}/2 \times \mathbb{Z}/2 \hookrightarrow \mathrm{GL}(4, \mathbb{F}_2)$$

of the Klein 4-group afforded by the matrices

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Then orbitsum of the monomial x_1 is

$$o(x_1) = x_1 + x_2$$

and hence not in the image of the transfer even though it has degree prime to the characteristic.

§4. The Ring of Invariants of Cyclic and Dihedral Groups

In this section we see that for the regular representation of groups of order $2p$ and for arbitrary permutation representations of $\mathbb{Z}/p$ the image of the transfer and certain orbit Chern classes generate the ring of invariants as an algebra over $\mathbb{F}$.

THEOREM 4.1: *Let $\rho : \mathbb{Z}/p \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a permutation representation of the cyclic group of order p. Then the ring of invariants $\mathbb{F}[V]^{\mathbb{Z}/p}$ is generated as an $\mathbb{F}$-algebra by the top orbit Chern classes $c_{\mathrm{top}}(x_i)$, $x_i \in \{x_1, \ldots, x_n\}$, and the image of the transfer.*

PROOF: Since ρ is a permutation representation the ring of invariants $\mathbb{F}[V]^{\mathbb{Z}/p}$ is generated by orbitsums of monomials, $o(x^E)$ for $x^E \in \mathbb{F}[V]$ a monomial. If the orbit length of x^E is p, then $o(x^E) \in \mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})$. If not, it is 1, and hence a product of top orbit Chern classes •

REMARK: Together with Manfred Göbel's degree bound for permutation representation, [6], the lemma above shows that in order to find the algebra generators of the ring of invariants one has to calculate the top orbit Chern classes (which have degree 1 or p), and the transfer up to degree $\max\{n, \frac{n(n-1)}{2}\}$.

Note that in the following theorem the case $p = 2$ is not excluded.

THEOREM 4.2: *Let $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be the regular representation of a group of order $2p$ $(= n)$, G not the Klein 4-group. Then the ring of invariants $\mathbb{F}[V]^G$ is generated by Chern classes of degree divisible by p and the image of the transfer.*

PROOF: Again ρ is a permutation representation and therefore $\mathbb{F}[V]^G$ is generated by orbitsums $o(x^E)$ of monomials $x^E \in \mathbb{F}[V]$.

CASE $\mid o(x^E) \mid = 2p$: Then $o(x^E) = \mathrm{Tr}^G(x^E)$, and there is nothing to show.

CASE $\mid o(x^E) \mid = 1$: Then $o(x^E) \notin \mathrm{Im}(\mathrm{Tr}^G)$, but the orbitsum $o(x^E)$ is a product of top orbit Chern classes

$$o(x^E) = \prod_{j=1}^{n} c_{\mathrm{top}}(x_j)^{\alpha_j}.$$

Its degree is divisible by p since ρ is the regular representation.

CASE $\mid o(x^E) \mid = p$ and $p \neq 2$: Then

$$\mathrm{Tr}^G(x^E) = 2o(x^E)$$

and hence $o(x^E)$ lies in the image of the transfer

$$o(x^E) = \mathrm{Tr}^G(\frac{1}{2}x^E).$$

CASE $\mid o(x^E) \mid = 2$: Then $x^E \in \mathbb{F}[V]^{\mathbb{Z}/p}$ for the[3] cyclic $\mathbb{Z}/p < G$. Hence x^E is a product of top orbit Chern classes of $\mathbb{Z}/p$

$$x^E = \prod_{j=1}^{n} c_{\mathrm{top}}^{\mathbb{Z}/p}(x_j)^{\alpha_j}.$$

By Lemma 3.1 the restriction of ρ to $\mathbb{Z}/p$ is the direct sum of two copies of the regular representation of $\mathbb{Z}/p$. Hence the basis $\{x_1, \ldots, x_n\}$ is the disjoint union of two nontrivial $\mathbb{Z}/p$-orbits. So, without loss of generality

$$x^E = c_{\mathrm{top}}^{\mathbb{Z}/p}(x_1)^{\alpha_1} c_{\mathrm{top}}^{\mathbb{Z}/p}(x_2)^{\alpha_2},$$

where $\alpha_1 \neq \alpha_2$ for otherwise x^E would be just a power of the top Chern class of G. Moreover for $\alpha_1 > \alpha_2$

$$x^E = c_{\mathrm{top}}^{G}(x_1) c_{\mathrm{top}}^{\mathbb{Z}/p}(x_1)^{\alpha_1 - \alpha_2}$$

Hence one can assume that $\alpha_2 = 0$. By [6] Theorem 5.8 the ring of invariants $\mathbb{F}[V]^G$ is generated by orbitsums of special monomials. Therefore $\alpha_1 = 1$ and

$$o(x^E) = c_{\mathrm{top}}^{\mathbb{Z}/p}(x_1) + c_{\mathrm{top}}^{\mathbb{Z}/p}(x_2).$$

[3] It is precisely here, where we need to assume that G is not $\mathbb{Z}/2 \times \mathbb{Z}/2$; recall Example 2.3.

Hence $o(x^E) = x_1^{e_1} \cdots x_n^{e_n}$ is the unique orbit of length two of a special monomial in degree p with $0 \le e_i \le 1$, $\forall\ i = 0, \ldots, n$. Therefore, since it is a summand of the p-th Chern class of G

$$c_p = o(x^E) + \mathrm{Tr}^G(f)$$

for some $f \in \mathbb{F}[V]$. It follows that $o(x^E)$ is in the subalgebra generated by the image of the transfer and the p-th Chern class •

REMARK: Again, together with Manfred Göbel's degree bound for permutation representation, [6], the lemma above shows that in order to find the algebra generators of the ring of invariants one has to calculate the orbit Chern classes of degree p and $2p$ and the transfer up to degree $p(2p-1)$.

EXAMPLE 4.3 : Consider the dihedral group of order 6

$$D_6 = \langle s,\ t \mid |s| = 2,\ |t| = 3,\ st = t^2 s\rangle.$$

Take its regular representation over a field of characteristic 3

$$\rho : D_6 \hookrightarrow \mathrm{GL}(6,\ \mathbb{F}),$$

afforded by the matrices

$$\rho(s) = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad \rho(t) = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Then the preceding theorem tells us that the ring of invariants if generated by the two Chern classes of degree divisible by 3, i.e., $c_3(x_1)$ and $c_6(x_1)$, and the image of the transfer map

$$\mathbb{F}[x_1, \ldots,\ x_6]^{D_6} = \mathbb{F}\langle c_3(x_1),\ c_6(x_1),\ \mathrm{Im}(\mathrm{Tr}^{D_6})\rangle,$$

where the $\langle - \rangle$-brackets emphasize that this is just the $\mathbb{F}$-algebra generated by the elements in the brackets, i.e., it is not a polynomial ring.

EXAMPLE 4.4 : Consider the $\mathbb{Z}/4$ representation of Example 3.4. The invariant orbitsum $o(x_1x_3x_5)$ is not in the subalgebra generated by the Chern classes and the image of the transfer. Hence for arbitrary permutation groups not even the weaker version (where the restriction to Chern classes of degree divisible by p is omitted) of Theorem 4.2 is valid.

EXAMPLE 4.5 : Recall the representation of the Klein 4-group from Example 3.5. The invariant orbitsum $o(x_1) = x_1 + x_2$ is not in the subalgebra generated by the Chern classes of degree divisible by 2 and the image of the transfer. However, since $\mathbb{F}[x_1, \ldots,\ x_4]^{\mathbb{Z}/2\times\mathbb{Z}/2} = \mathbb{F}[x_1 + x_2,\ x_1x_2,\ x_3 + x_4,\ x_3x_4]$, the ring of invariants is still generated by the image of the transfer and orbit Chern classes.

§5. Mme Bertin's $\mathbb{Z}/4$

In this section we apply Theorem 4.2 to obtain a description of the ring of invariants of one of Marie-José Bertin's famous examples, [2].

Consider the regular representation of the cyclic group of order 4 over a field $\mathbb{F}$ of characteristic 2

$$\rho : \mathbb{Z}/4 \hookrightarrow \mathrm{GL}(4, \mathbb{F})$$

afforded by the matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

This example was first studied by Marie-José Bertin. She showed in [2] that its ring of invariants is factorial but not Cohen-Macaulay, which was the first example of that type.[4]

THEOREM 5.1: *The ring of invariants, $\mathbb{F}[x_1, \ldots, x_4]^{\mathbb{Z}/4}$, of the regular representation of $\mathbb{Z}/4$ is generated as an algebra by the following eight polynomials*

$$\begin{aligned} c_1 &:= x_1 + x_2 + x_3 + x_4 \\ c_2 &:= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ c_3 &:= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\ c_4 &:= x_1x_2x_3x_4 \\ q &:= x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1 \\ k &:= x_1^2x_2 + x_2^2x_3 + x_3^2x_4 + x_4^2x_1 \\ l &:= x_1^3x_2 + x_2^3x_3 + x_3^3x_4 + x_4^3x_1 \\ m &:= x_1^3x_2^2 + x_2^3x_3^2 + x_3^3x_4^2 + x_4^3x_1^2 \end{aligned}$$

Note that each of these polynomials except c_2, c_4 is the transfer of one of its monomials. Moreover, c_1, c_2, c_3, c_4 are the four Chern classes of the only nontrivial orbit.

PROOF: By Theorem 4.2 the ring of invariants is generated by Chern classes whose degree is divisible by 2 and the image of the transfer. By [6] Corollary 5.9 the ring of invariants is generated by polynomials of degree ≤ 6. Hence calculating the image of the transfer up to degree 6 leads to the algebra generators given above •

REMARK: Since

$$c_2 = o(x_1x_2) + o(x_1x_3) = \mathrm{Tr}^{\mathbb{Z}/4}(x_1x_2) + o(x_1x_3)$$

resp.

$$|\ o(x_1x_2)\ | = 4 = |\ \mathbb{Z}/4\ | \quad \text{and} \quad |\ o(x_1x_3)\ | = 2 < |\ \mathbb{Z}/4\ |$$

this example illustrates also Lemma 2.6.

REMARK: Marie-José Bertin's relation, which shows that the ring of invariants is not Cohen-Macaulay reads as follows in this basis

$$T_5 := c_1(c_2q + c_1k + c_1c_3 + l) + (c_2 + q)k + c_3c_2 = 0.$$

Hence c_1, $c_2 + q$, c_3, c_4 form a system of parameters, but not a regular sequence. Theorem 5.1 shows that the canonical algebra homomorphism

$$\varphi : \mathbb{F}[c_1, c_2, c_3, c_4, q, k, l, m] \longrightarrow \mathbb{F}[x_1, \ldots, x_4]^{\mathbb{Z}/4}$$

[4] This example is also minimal, in the sense that for representations of degree ≤ 3 the ring of invariants is always Cohen-Macaulay, [11], no matter what the ground field is.

is surjective, and its kernel $\ker\varphi$ is the ideal of relations. Consider the following four polynomials[5] in $\ker(\varphi)$:

$$\begin{aligned}
R_1 &: c_1c_3q + c_1^2c_4 + c_1c_2c_3 + q^3 + c_3^2 + c_2^2q \\
R_3 &: c_1c_2c_3 + k^2 + c_2^2q + c_1^3c_3 + c_1qk + c_1^2q^2 + c_1^2c_4 + c_1^2c_2q \\
P_8 &: c_1^2k^2 + c_1c_4k + c_1^2c_2c_4 + l^2 + q^4 + c_3^2q + c_3m + c_4q^2 + c_2c_3k \\
P_{10} &: c_1^4c_2c_4 + c_1c_3c_4q + c_1^2c_4l + c_1^3c_3c_4 + c_2^2k^2 + m^2 + c_2c_3m + c_1c_4m + \\
&\quad + c_1c_3k^2 + c_3c_4k + c_3^2l + c_3^2c_4 + c_2c_4q^2 + c_2^2c_3k + c_1c_2c_4k + c_2c_3^2q + c_1c_2c_3l.
\end{aligned}$$

Then

$$\begin{aligned}
\mathbb{F}[c_1, c_2, c_3, c_4, q, k, l, m] &\supset (c_1, c_2, c_4, q, R_1, R_3, P_8, P_{10}) \\
&= (c_1, c_2, c_4, q, c_3^2, k^2, l^2 + c_3m, m^2)
\end{aligned}$$

Hence these eight polynomials form a system of parameters in $\mathbb{F}[c_1, c_2, c_3, c_4, q, k, l, m]$. By Macaulay's Theorem, see [4] Theorem 18.7 or [1] Theorem 3.3.2, every system of parameters in a Cohen-Macaulay algebra is a regular sequence. In particular the ideal

$$(R_1, R_3, P_8, P_{10}) \subset \mathbb{F}[c_1, c_2, c_3, c_4, q, k, l, m]$$

is regular of height 4. By Macaulay's Unmixedness Theorem, see [4] Corollary 18.14 or [1] Definition 3.3.1, an ideal I in a Cohen-Macaulay algebra, which is generated by $\mathit{ht}(I)$ elements, is height unmixed, i.e., our ideal (R_1, R_3, P_8, P_{10}) has no embedded prime ideals. Since the ring of invariants of a cyclic p-group is always a unique factorization domain, [9] Proposition 1.5.7, we have:

THEOREM 5.2: *The ring of invariants of the regular representation of the cyclic group of order four in characteristic two is given by*

$$\mathbb{F}[x_1, x_2, x_3, x_4]^{\mathbb{Z}/4} = \mathbb{F}[c_1, c_2, c_3, c_4, q, k, m, l]/\mathfrak{p}$$

where $\mathfrak{p}$ an isolated prime ideal of (R_1, R_3, P_8, P_{10}). Moreover $\mathfrak{p}$ has height 4 and is closed under the action of the Steenrod algebra •

REMARK: By Corollary 2.6 we know that the height of the image of the transfer is at most 2

$$\mathit{ht}\left(\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/4})\right) \le 2.$$

On the other hand we have that

$$\mathbb{F}[x_1, x_2, x_3, x_4]^{\mathbb{Z}/4}/\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/4}) = \mathbb{F}[c_2, c_4]$$

has Krull dimension 2. Therefore the height of the image of the transfer is precisely 2.

References

[1] Stanislaw Balcerzyk and Tadeusz Józefiak, *Commutative rings. Dimension, multiplicity and homological methods,* Mathematics and its Applications, PWN-Polish Scientific Publishers, Warsaw 1989.

[2] Marie-José Bertin, *Anneaux d'invariants d'anneaux de polynômes en caractéristique p,* C. R. Acad. Sc. Paris t. 264 (10 avril 1967), série A, 653-656.

[5] The two relations of degree 6, R_1, R_3, come out of the calculation of the image of the transfer in degree 6. The remaining ones come from the calculation of the Steenrod squares of T_5, R_1 and R_3. For an introduction to the Steenrod algebra and its use in invariant theory see [10].

[3] H. E. A. Campbell, I. P. Hughes, R. J. Shank and D. L. Wehlau, *Bases for rings of coinvariants,* Transformation Groups 1 (1996), 307-336.

[4] David Eisenbud, *Commutative algebra,* Graduate Texts in Mathematics 150, Springer Verlag, New York-Berlin-Heidelberg 1994.

[5] Mark Feshbach, *p-Subgroups of compact Lie groups and torsion of infinite height in* $H^*(BG;\mathbb{F}_p)$, Mich. Math. J. 29 (1982), 299-306.

[6] Manfred Göbel, *Computing bases for rings of permutation-invariant polynomials,* J. Symbolic Computation 19 (1995), 285-291.

[7] Kathrin Kuhnigk, *Transfer in Invariantenringen,* Diplomarbeit, Göttingen, 1998.

[8] R. James Shank and David L. Wehlau, *The Transfer in Modular Invariant Theory,* J. of Pure and Applied Algebra, to appear.

[9] Larry Smith, *Polynomial invariants of finite groups,* Research Notes in Mathematics, A. K. Peters Ltd., Wellesley, MA, 2nd corrected printing 1997.

[10] Larry Smith, $\mathcal{P}^*$*-invariant ideals in rings of invariants,* Forum Mathematicum 8 (1996), 319-342.

[11] Larry Smith, *Some rings of invariants that are Cohen-Macaulay,* Canadian Mathematical Bulletin 39 (1996), 238-240.

[12] Larry Smith, *Modular vector invariants of cyclic permutation representations,* Canadian Mathematical Bulletin, to appear.

Mara D. Neusel
Department of Mathematics
Notre Dame University
370 CCM
Notre Dame, IN 46556
USA

neusel.1@nd.edu