Proceedings of the Edinburgh Mathematical Society (2012) **55**, 355–367
DOI:10.1017/S0013091508001107

INVARIANTS OF HYPERPLANE GROUPS AND VANISHING IDEALS OF FINITE SETS OF POINTS

H. E. A. CAMPBELL AND JIANJUN CHUAI

Department of Mathematics and Statistics, University of New Brunswick, Fredericton, New Brunswick E3B 5A3, Canada (eddy@unb.ca; jchuai@unb.ca)

(Received 31 October 2008)

Abstract We define a hyperplane group to be a finite group generated by reflections fixing a single hyperplane pointwise. Landweber and Stong proved that the invariant ring of a hyperplane group is again a polynomial ring in any characteristic. Recently, Hartmann and Shepler gave a constructive proof of this result. By their algorithm, one can always construct generators that are additive. In this paper, we study hyperplane groups of order a power of a prime p in characteristic p and give a slightly different construction of the generators than Hartmann and Shepler. We then show that such generators have a particular form. Furthermore, we show that if the group is defined by a finite additive subgroup $W \subseteq \mathbb{F}^n$, the vanishing ideal of W is generated by polynomials obtained from a set of generators of the invariant ring that are additive. Finally, we give a shorter proof of the fact that the module of the invariant differential 1-forms is free in our situation.

Keywords: hyperplane group; invariant ring; vanishing ideal; invariant differential 1-form

2010 *Mathematics subject classification:* Primary 13A50; 14R99

1. Introduction

Given a finite-dimensional representation of a finite group G on a vector space V over a field $\mathbb{F}$ of characteristic $p \geqslant 0$, we say that a non-identity element $\sigma \in G$ is a reflection if σ fixes a hyperplane of V pointwise. We say that G is a reflection group if G is generated by reflections. The action of G on V induces an action of G on the hom-dual V^* of V via the rule

$$\sigma(x)(v) = x(\sigma^{-1}(v))$$

for $\sigma \in G$, $x \in V^*$ and $v \in V$. When $\mathbb{F}$ is infinite, we note that the symmetric algebra of V^* can be identified with the coordinate ring, $\mathbb{F}[V]$, of V. However, we shall use the notation $\mathbb{F}[V]$ to denote the symmetric algebra of V^* over any field $\mathbb{F}$. The action of G on V^* can be extended to the symmetric algebra of V^* via the rules $\sigma(f \cdot f') = \sigma(f) \cdot \sigma(f')$ and $\sigma(f + f') = \sigma(f) + \sigma(f')$. The ring of functions left invariant by the action of G is denoted by $\mathbb{F}[V]^G$ and the study of this invariant ring is centuries old. We recommend [**1**, **3**, **11**] as general references for the invariant theory of finite groups.

The invariant ring $\mathbb{F}[V]^G$ is much better understood in the non-modular case (i.e. when the characteristic p of the field does not divide the order $|G|$ of the group G). In this case, it is a famous result [**2**,**9**,**10**] that $\mathbb{F}[V]^G$ is again a polynomial algebra if and only if G is a reflection group. The best known example is provided by the usual representation of the symmetric group which is generated by its transpositions $x \leftrightarrow y$ fixing the hyperplane determined by $x - y$. In fact, the usual representation of the symmetric group has a polynomial ring of invariants independently of the characteristic of the field. However, it remains a most important problem of modular invariant theory to characterize those groups G with an invariant ring which is again polynomial. It is known that G must be a reflection group, but it is also known that this is not a sufficient condition [**9**].

In this paper, we shall study a special family of modular reflection groups that are known to have polynomial invariant rings. A reflection group G is said to be a hyperplane group if each element of G fixes the same hyperplane pointwise. To our knowledge, these groups were first defined and studied by Landweber and Stong in [**7**]. They proved that such groups always have polynomial invariant rings.

In what follows, we take V to be a vector space of dimension $n+1$ over a field $\mathbb{F}$ of characteristic $p > 0$ with basis $\{e, e_1, \dots, e_n\}$, we take U to be the hyperplane of V spanned by $\{e_1, \dots, e_n\}$ and we take G to be a (finite) hyperplane group fixing U pointwise. We suppose now that $\{x, x_1, \dots, x_n\}$ is the hom-dual basis of $\{e, e_1, \dots, e_n\}$. Then U is defined by $x = 0$ and the induced action of G on V^* is of the form

$$\sigma(x) = a_\sigma x, \qquad \sigma(x_i) = x_i + a_{i,\sigma} x \quad \text{for } 1 \leqslant i \leqslant n,$$

where $\sigma \in G$, $a_\sigma, a_{i,\sigma} \in \mathbb{F}$ and $a_\sigma \neq 0$. Namely, under the basis $\{x, x_1, \dots, x_n\}$, the matrix of σ takes the following form:

$$\begin{pmatrix} a_\sigma & a_{1,\sigma} & \cdots & a_{n,\sigma} \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

We recall that over any field k of characteristic $p > 0$, a polynomial $f(y) \in k[y]$ is said to be additive in y if

$$f(y+z) = f(y) + f(z)$$

in $k[y,z]$. We note that f is additive in y if and only if each of its terms is of the form $a_i y^{p^i}$ for $a_i \in k$ and $i \geqslant 0$. A polynomial in $\mathbb{F}[x, x_1, \dots, x_n]$ is said to be additive in $x_1, \dots, x_n$ if

$$f(x, x_1 + y_1, \dots, x_n + y_n) = f(x, x_1, \dots, x_n) + f(x, y_1, \dots, y_n)$$

in $\mathbb{F}[x, x_1, \dots, x_n, y_1, \dots, y_n]$. For example, $x_1^p - x^{p-1}x_1 \in k[x, x_1]$ is additive in x_1. It is not hard to see that a homogeneous polynomial $f(x, x_1, \dots, x_n) \in \mathbb{F}[V]$ is additive in $x_1, \dots, x_n$, if and only if

$$f(x, x_1, \dots, x_n) = f(x, x_1, 0, \dots, 0) + f(x, 0, x_2, 0, \dots, 0) + \cdots + f(x, 0, \dots, 0, x_n),$$

and each homogeneous polynomial $f(x, 0, \dots, 0, x_i, 0, \dots, 0)$ is additive in x_i.

Recently, Hartmann and Shepler [**5**] examined the Jacobians associated to hyperplane groups and gave a constructive proof of the result of [**7**] just cited. More precisely, they proved that, for the hyperplane group G,

$$\mathbb{F}[V]^G = \mathbb{F}[x^s, f_1, \dots, f_n],$$

where $s > 0$ is some integer (in fact, s is the order of the image of θ defined below) and each f_i is homogeneous and additive in $x_1, \dots, x_n$.

We note that to prove that $\mathbb{F}[V]^G$ is polynomial we need only to prove that $\mathbb{F}[V]^H$ is polynomial, where H is the kernel of the group homomorphism

$$\theta : G \to \mathbb{F}^*, \quad \sigma \to a_\sigma.$$

This can be seen as follows. The image of θ is a cyclic subgroup of $\mathbb{F}^*$ of order coprime to p. Let s be the order of this cyclic subgroup and define

$$\mathbb{F}[V]^G_{\theta^i} = \{f \in \mathbb{F}[V] \mid \sigma(f) = \theta(\sigma)^i f \text{ for all } \sigma \in G\},$$

often referred to as the semi-invariants associated to the group character θ^i. Then we have

$$\mathbb{F}[V]^H = \bigoplus_{i=0}^{s-1} \mathbb{F}[V]^G_{\theta^i}.$$

Since G is generated by reflections, each $\mathbb{F}[V]^G_{\theta^i}$ is free of rank 1 over $\mathbb{F}[V]^G$ [**8**]. It follows that $\mathbb{F}[V]^H$ is free over $\mathbb{F}[V]^G$. So, $\mathbb{F}[V]^G$ is a polynomial ring if $\mathbb{F}[V]^H$ is [**11**, Corollary 6.7.13].

So, we shall assume $G = H$ in what follows. It is then clear that G is an elementary abelian p-group (in particular, $\det(\sigma) = 1$ for any $\sigma \in G$) and that $x \in (V^*)^G$.

Let $\mathcal{G}$ denote the collection of all the finite hyperplane groups on V that fix U pointwise and fix x, and let $\mathcal{W}$ denote the collection of all finite additive subgroups of $\mathbb{F}^n$. It is easy to see that there exists a one-to-one correspondence between $\mathcal{G}$ and $\mathcal{W}$. We have that, for any $G \in \mathcal{G}$, the set

$$\{(a_{1,\sigma}, a_{2,\sigma}, \dots, a_{n,\sigma}) \mid \sigma \in G\}$$

(using the notation established above) is a finite additive subgroup of $\mathbb{F}^n$. And if W is a finite additive subgroup of $\mathbb{F}^n$, then each $w = (a_1, a_2, \dots, a_n) \in W$ defines an invertible linear transformation σ_w of V^* by the rule

$$\sigma_w(x) = x, \qquad \sigma_w(x_i) = x_i + a_i x \quad \text{for } 1 \leqslant i \leqslant n.$$

Then $G = \{\sigma_w \mid w \in W\} \in \mathcal{G}$. Now any group in $\mathcal{G}$ is an elementary abelian p-group, and a finite additive subgroup of $\mathbb{F}^n$ is also an elementary abelian p-group. So the one-to-one correspondence described above is an isomorphism of vector spaces over $\mathbb{F}_p$.

We now view $x_1, \dots, x_n$ as the dual basis to the standard basis of $\mathbb{F}^n$ and view the polynomial algebra $A = \mathbb{F}[x_1, \dots, x_n]$ as the symmetric algebra of $(\mathbb{F}^n)^*$. For any subset $T \subset \mathbb{F}^n$, the vanishing ideal of T is defined to be

$$I(T) = \{f \in A \mid f(t) = 0 \text{ for all } t \in T\}.$$

The well-known Hilbert Basis Theorem tells us that $I(T)$ is always finitely generated. Furthermore, if T is finite, then $I(T)$ is generated by n elements [**12**, Theorem 4.2.4].

In the next section, we give a slightly different approach from [**5**] to prove that $\mathbb{F}[V]^G = \mathbb{F}[x, f_1, \dots, x_n]$ for any G in $\mathcal{G}$, where each $f_i = f_i(x, x_1, \dots, x_n)$ is homogeneous and additive in $x_1, \dots, x_n$. Furthermore, we prove that if G is defined by $W \subseteq \mathbb{F}^n$, then $I(W)$ is generated by $f_1(1, x_1, \dots, x_n), \dots, f_n(1, x_1, \dots, x_n)$. We also give a proof of the fact that the $\mathbb{F}[V]^G$-module of invariant differential 1-forms, $(\Omega^1)^G$, is free in our situation.

2. Main result

We continue to use the notation established in the introduction: $\mathbb{F}[V] = \mathbb{F}[x, x_1, \dots, x_n]$, and G is a hyperplane group fixing x and the hyperplane $x = 0$ pointwise. As above, we view $A = \mathbb{F}[x_1, \dots, x_n]$ as the coordinate ring of $\mathbb{F}^n$. In the proof of the main theorem below, we shall need the following well-known result.

Let $f, f_1, \dots, f_n \in \mathbb{F}[V]^G$ be a homogeneous system of parameters of degrees $|f|, |f_1|, \dots, |f_n|$, respectively. Then $\mathbb{F}[V]^G = \mathbb{F}[f, f_1, \dots, f_n]$ if and only if

$$|f| \cdot |f_1| \cdots |f_n| = |G| \tag{2.1}$$

(see [**6**, Proposition 16]).

It is easy to see that $\mathbb{F}[V]^G = (\mathbb{F}[V]^H)^{G/H}$ for any normal subgroup H of G. Suppose we are given a normal subgroup H of G such that G is generated by H and a single element σ so that G/H is generated by (the image of) σ. For $f \in \mathbb{F}[V]$, we define $\Delta(f) = \sigma(f) - f$. Then Δ is a *twisted* derivation: $\Delta(ff') = \Delta(f)f' + \sigma(f)\Delta(f')$, and we note that $\Delta\colon \mathbb{F}[V]^H \to \mathbb{F}[V]^H$ is a map of $\mathbb{F}[V]^G$ modules.

In this situation, we shall construct invariants in two ways. Note that the $N_\sigma(f)$ in the next lemma is just the relative norm of f.

Lemma 2.1. *Let H be a normal subgroup of G and assume $G = \langle H, \sigma \rangle$.*

(i) *Suppose $f \in \mathbb{F}[V]^H$ and assume $\Delta(f) \in \mathbb{F}[V]^G$. Then*

$$N_\sigma(f) = N(f) = f^p - \Delta(f)^{p-1} f \in \mathbb{F}[V]^G.$$

(ii) *Suppose $f, f' \in \mathbb{F}[V]^H$ with $\Delta(f') \mid \Delta(f)$ and $\Delta(f)/\Delta(f') \in \mathbb{F}[V]^G$. Then*

$$\mathcal{R}_\sigma(f, f') = \mathcal{R}(f, f') = f - \frac{\Delta(f)}{\Delta(f')} f' \in \mathbb{F}[V]^G.$$

Proof. This is done by direct computation. □

Remark 2.2. For any pair $f, f' \in \mathbb{F}[V]^H$ with $\Delta(f'), \Delta(f) \in \mathbb{F}[V]^G$, we may construct a G-invariant

$$\Delta(f')f - \Delta(f)f'$$

of degree at most $|f| + |f'|$.

https://doi.org/10.1017/S0013091508001107 Published online by Cambridge University Press

Now we give the main result of the paper.

Theorem 2.3. *Let $\mathbb{F}[V] = \mathbb{F}[x, x_1, \dots, x_n]$ and let G be a non-trivial finite hyperplane group on V fixing x and the hyperplane $x = 0$ pointwise. We have the following.*

(i) *$\mathbb{F}[V]^G$ is a polynomial ring and there exist polynomials $f_1, \dots, f_n \in \mathbb{F}[V]^G$ such that $\mathbb{F}[V]^G = \mathbb{F}[x, f_1, \dots, f_n]$, where each f_i is homogeneous and additive in $x_1, \dots, x_n$ [**5**].*

(ii) *If $\mathbb{F}[V]^G = \mathbb{F}[x, f_1, \dots, f_n]$, where all f_i are homogeneous and additive in $x_1, \dots, x_n$, then each f_i is of the form*

$$f_i = \sum_{j=0}^{d_i} \sum_{k=1}^{n} a_{ijk} x^{p^{d_i} - p^{d_i - j}} x_k^{p^{d_i - j}},$$

where $a_{ijk} \in \mathbb{F}$. Furthermore, if $\mathbb{F}$ is a perfect field, then with a suitable choice of the coordinate functions each f_i has the following form

$$f_i = x_i^{p^{d_i}} + \sum_{j=1}^{d_i} \sum_{k=1}^{n} c_{ijk} x^{p^{d_i} - p^{d_i - j}} x_k^{p^{d_i - j}},$$

where $c_{ijk} \in \mathbb{F}$.

(iii) *If G is defined by the additive subgroup $W \subset \mathbb{F}^n$ and $\mathbb{F}[V]^G = \mathbb{F}[x, f_1, \dots, f_n]$, where each $f_i = f_i(x, x_1, \dots, x_n)$ is homogeneous and additive in $x_1, \dots, x_n$, then the vanishing ideal $I(W)$ is generated by $\hat{f}_1, \dots, \hat{f}_n$, where*

$$\hat{f}_i = f_i(1, x_1, \dots, x_n).$$

Proof. We shall give a slightly different proof of the first statement from the one that appears in [**5**].

As noted above, we have that G is an elementary abelian p-group. So we assume that G has rank $r > 0$ and generated by $\sigma_1, \sigma_2, \dots, \sigma_r$ for some $r > 0$. So we shall induct on r to show (i). Let us assume $\{\sigma_1, \dots, \sigma_r\}$ is a basis for G over $\mathbb{F}_p$.

Assume that $r = 1$ and that $\sigma = \sigma_1$ corresponds to $(a_1, \dots, a_n)$. We may assume that $a_1 \neq 0$. We note that $\Delta_\sigma(x_1) \mid \Delta_\sigma(x_i)$ for all $2 \leqslant i \leqslant n$. So $\mathcal{R}_\sigma(x_1, x_i) = x_i - a_1^{-1} a_i x_1$ is G-invariant by the lemma. We may conclude that

$$\mathbb{F}[V]^G = \mathbb{F}[x, x_1^p - a_1^{p-1} x^{p-1} x_1, x_2 - a_1^{-1} a_2 x_1, \dots, x_n - a_1^{-1} a_n x_1].$$

So the result is true for $r = 1$. Now assume $r > 1$ and define H to be the group generated by $\sigma_1, \dots, \sigma_{r-1}$ and assume by induction that

$$\mathbb{F}[V]^H = \mathbb{F}[x, f_1, \dots, f_n]$$

is polynomial, where the f_i are homogeneous and additive in $x_1, \dots, x_n$. Using (2.1), we have

$$|f_1| \cdot |f_2| \cdots |f_n| = |H| = p^{r-1},$$

where $|f_i| = \deg f_i$. Let $\sigma = \sigma_r$ correspond to $(a_1, \dots, a_n)$ and arrange the f_i such that

$$|f_1| \leqslant |f_2| \leqslant \cdots \leqslant |f_n|.$$

We take i to be the smallest integer such that $\sigma(f_i) \neq f_i$. Then, for each j we have

$$\sigma f_j(x, x_1 \dots, x_n) = f_j(x, x_1 \dots, x_n) + f_j(x, a_1 x, \dots, a_n x) = f_j + b_j x^{|f_j|},$$

where $b_j \in \mathbb{F}$. Thus, we have $b_j = 0$ for $1 \leqslant j < i$ and $b_i \neq 0$.

Using Lemma 2.1, we take

$$N(f_i) = f_i^p - b_i^{p-1} x^{|f_i|(p-1)} f_i,$$

and for $j > i$ we take

$$\mathcal{R}(f_i, f_j) = f_j - b_i^{-1} b_j x^{|f_j| - |f_i|} f_i.$$

Then these homogeneous polynomials are G-invariant and, since

$$\{x, f_1, \dots, f_{i-1}, N(f_i), \mathcal{R}(f_i, f_{i+1}), \dots, \mathcal{R}(f_i, f_n)\}$$

is a homogeneous system of parameters for $\mathbb{F}[V]^G$ and the product of their degrees is $p \cdot |H| = |G|$, we have (using (2.1)) that

$$\mathbb{F}[V]^G = \mathbb{F}[x, f_1, \dots, f_{i-1}, N(f_i), \mathcal{R}(f_i, f_{i+1}), \dots, \mathcal{R}(f_i, f_n)]$$

is a polynomial ring. Furthermore, each of these polynomials is additive in $x_1, \dots, x_n$, completing the proof of (i).

For (ii), assume $\mathbb{F}[V]^G = \mathbb{F}[x, f_1, \dots, f_n]$ is a polynomial ring, where each f_i is homogeneous and additive in $x_1, \dots, x_n$. Now, the polynomial

$$f_i(x, 0, \dots, 0, x_j, 0, \dots, 0)$$

is homogeneous and additive in x_j for $1 \leqslant i, j \leqslant n$. Thus, each f_i must be of the form

$$f_i = \sum_{j=0}^{d_i} \sum_{k=1}^{n} a_{ijk} x^{p^{d_i} - p^{d_i - j}} x_k^{p^{d_i - j}},$$

where $a_{ijk} \in \mathbb{F}$ and $p^{d_i} = |f_i|$.

Furthermore, since $\{x, f_1, \dots, f_n\}$ is a homogeneous system of parameters for $\mathbb{F}[V]$,

$$\{f_1(0, x_1, \dots, x_n), \dots, f_n(0, x_1, \dots, x_n)\}$$

is a homogeneous system of parameters for $A = \mathbb{F}[x_1, \dots, x_n]$. We also have

$$f_i(0, x_1, \dots, x_n) = \sum_{k=1}^{n} a_{i0k} x_k^{p^{d_i}}.$$

Since $\mathbb{F}$ is perfect, there exists a $b_{ik} \in \mathbb{F}$ such that $a_{i0k} = b_{ik}^{p^{d_i}}$ for each pair (i,k). Thus,

$$f_i(0, x_1, \dots, x_n) = \left(\sum_{k=1}^{n} b_{ik} x_k \right)^{p^{d_i}}.$$

Hence,

$$\left\{ y_i = \sum_{k=1}^{n} b_{ik} x_k \;\middle|\; 1 \leqslant i \leqslant n \right\}$$

is also a homogeneous system of parameters for $\mathbb{F}[x_1, \dots, x_n]$. In other words, $\{y_1, \dots, y_n\}$ is a basis of the vector space $\langle x_1, \dots, x_n \rangle$. Thus, we have

$$\mathbb{F}[V] = \mathbb{F}[x, y_1, \dots, y_n],$$
$$\Delta_\sigma(y_i) \in \mathbb{F}x \quad \text{for } 1 \leqslant i \leqslant n,\ \sigma \in G,$$

and each f_i can be written in the form

$$f_i(x, x_1, \dots, x_n) = y_i^{p^{d_i}} + \sum_{j=1}^{d_i} \sum_{k=1}^{n} c_{ijk} x^{p^{d_i} - p^{d_i - j}} y_k^{p^{d_i - j}},$$

with $c_{ijk} \in \mathbb{F}$. So (ii) follows.

We now prove (iii), i.e. that

$$I(W) = (\hat{f}_1, \dots, \hat{f}_n),$$

where $\hat{f}_i = f_i(1, x_1, \dots, x_n)$. First of all, for any $\sigma \in G$ corresponding to $(a_1, \dots, a_n)$, we have

$$0 = \Delta_\sigma(f_i) = f_i(x, a_1 x, \dots, a_n x) = f_i(1, a_1, \dots, a_n) x^{p^{d_i}}.$$

Thus,

$$\hat{f}_i(a_1, \dots, a_n) = f_i(1, a_1, \dots, a_n) = 0,$$

and therefore

$$(\hat{f}_1, \dots, \hat{f}_n) \subseteq I(W).$$

Next, we prove the claim that

$$\dim_{\mathbb{F}} A/(\hat{f}_1, \dots, \hat{f}_n) \leqslant |G|.$$

First, we assume that $\mathbb{F}$ is perfect. Then, from (ii), we may assume that each f_i is of the form

$$f_i = x_i^{p^{d_i}} + \sum_{j=1}^{d_i} \sum_{k=1}^{n} c_{ijk} x^{p^{d_i} - p^{d_i - j}} x_k^{p^{d_i - j}},$$

and thus

$$\hat{f}_i = x_i^{p^{d_i}} + \sum_{j=1}^{d_i} \sum_{k=1}^{n} c_{ijk} x_k^{p^{d_i-j}},$$

where $c_{ijk} \in \mathbb{F}$. Then we see that, as a vector space over $\mathbb{F}$, $A/(\hat{f}_1, \ldots, \hat{f}_n)$ is spanned by the residue classes of the monomials

$$x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n},$$

where $0 \leqslant e_i < p^{d_i}$. So,

$$\dim_{\mathbb{F}} A/(\hat{f}_1, \ldots, \hat{f}_n) \leqslant \prod_{i=1}^{n} p^{d_i} = |G|.$$

Thus, the claim is true for $\mathbb{F}$ a perfect field.

Now assume that $\mathbb{F}$ is arbitrary. Let $\bar{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$ (thus, in particular, $\bar{\mathbb{F}}$ is perfect) and let $\bar{V} = \bar{\mathbb{F}} \otimes_{\mathbb{F}} V$. Then

$$\bar{\mathbb{F}}[\bar{V}] = \bar{\mathbb{F}} \otimes_{\mathbb{F}} \mathbb{F}[V]$$

and

$$\bar{\mathbb{F}}[\bar{V}]^G = \bar{\mathbb{F}} \otimes_{\mathbb{F}} \mathbb{F}[V]^G.$$

So, if we let $X = 1 \otimes x$ and $X_i = 1 \otimes x_i$ for $1 \leqslant i \leqslant n$, then

$$\bar{\mathbb{F}}[\bar{V}] = \bar{\mathbb{F}}[X, X_1, \ldots, X_n]$$

and

$$\bar{\mathbb{F}}[\bar{V}]^G = \bar{\mathbb{F}}[X, F_1, \ldots, F_n],$$

where $F_i = f_i(X, X_1, \ldots, X_n)$ for $1 \leqslant i \leqslant n$. Thus, since $\bar{\mathbb{F}}$ is perfect, for $\bar{A} := \bar{\mathbb{F}}[X_1, \ldots, X_n]$ and $\hat{F}_i = f_i(1, X_1, \ldots, X_n)$,

$$\dim_{\bar{\mathbb{F}}} \bar{A}/(\hat{F}_1, \ldots, \hat{F}_n) \leqslant |G|.$$

Moreover, from the natural exact sequence

$$0 \to \bar{\mathbb{F}} \otimes_{\mathbb{F}} (\hat{f}_1, \ldots, \hat{f}_n)A \to \bar{\mathbb{F}} \otimes_{\mathbb{F}} A \to \bar{\mathbb{F}} \otimes_{\mathbb{F}} A/(\hat{f}_1, \ldots, \hat{f}_n) \to 0$$

we see that

$$\bar{A}/(\hat{F}_1, \ldots, \hat{F}_n) \cong \bar{\mathbb{F}} \otimes_{\mathbb{F}} A/(\hat{f}_1, \ldots, \hat{f}_n).$$

It follows that

$$\dim_{\mathbb{F}} A/(\hat{f}_1, \ldots, \hat{f}_n) = \dim_{\bar{\mathbb{F}}} \bar{A}/(\hat{F}_1, \ldots, \hat{F}_n) \leqslant |G|.$$

This proves the claim.

https://doi.org/10.1017/S0013091508001107 Published online by Cambridge University Press

Furthermore, by the Chinese Remainder Theorem, we have

$$A/I(W) \simeq \bigoplus_{w\in W} A/\mathfrak{m}_w \simeq \mathbb{F}^{|G|},$$

where $\mathfrak{m}_w = I(\{w\})$. So,

$$\dim_{\mathbb{F}} A/I(W) = |G|.$$

Now, from the fact that $(\hat{f}_1, \dots, \hat{f}_n) \subseteq I(W)$, as shown earlier, we have that

$$\dim_{\mathbb{F}} A/I(W) \leqslant \dim_{\mathbb{F}} A/(\hat{f}_1, \dots, \hat{f}_n).$$

Thus,

$$|G| = \dim_{\mathbb{F}} A/I(W) \leqslant \dim_{\mathbb{F}} A/(\hat{f}_1, \dots, \hat{f}_n) \leqslant |G|,$$

and so

$$I(W) = (\hat{f}_1, \dots, \hat{f}_n).$$

This completes the proof of the theorem. □

Note that every f_i in the theorem is a polynomial, each of whose monomials only involves x and another variable. So $\hat{f}_i$ is a linear combination of p-powers of the variables $x_1, x_2, \dots, x_n$. Thus, we have the following.

Corollary 2.4. *Let $\mathbb{F}$ be a field of characteristic $p > 0$ and let $W \subseteq \mathbb{F}^n$ be a finite additive subgroup. Then the vanishing ideal $I(W)$ can be generated by n polynomials, each of which is a linear combination of p-powers of the variables.*

We remark that the proof of Theorem 2.3 (i) gives an algorithm for constructing a generating set for the invariant ring. This algorithm differs slightly from the one given in [**5**]. In fact, in [**5**], the polynomials

$$f_j' = f_j - (b_j/(b_i^{|f_j|/|f_i|}))f_i^{|f_j|/|f_i|}, \quad j > i,$$

were constructed instead of the polynomials $\mathcal{R}(f_i, f_j)$ constructed here.

Also, Hartmann and Shepler studied invariant differential forms of reflection groups in [**4**]. In particular, they proved the following result.

Theorem 2.5. *Let $\mathbb{F} = \mathbb{F}_q$ be a finite field and let G be any hyperplane group on V. Then the $\mathbb{F}[V]^G$-module of invariant differential 1-forms,*

$$(\Omega^1)^G = (\mathbb{F}[V] \otimes_{\mathbb{F}} V^*)^G,$$

is free.

They proved the above theorem by constructing linearly independent generators for $(\Omega^1)^G$ over $\mathbb{F}[V]^G$ from the generators of the polynomial ring $\mathbb{F}[V]^G$ produced by their algorithm. In our situation, we can prove the following.

Theorem 2.6. *Let the situation be as in Theorem 2.3 and assume*

$$\mathbb{F}[V]^G = \mathbb{F}[x, f_1, \dots, f_n],$$

where

$$f_i = \sum_{j=0}^{d_i} \sum_{k=1}^{n} a_{ijk} x^{p^{d_i} - p^{d_i - j}} x_k^{p^{d_i - j}}$$

for $1 \leqslant i \leqslant n$. *And, as in [**4**], assume* $p \neq 2$. *Then* $(\Omega^1)^G$ *is a free* $\mathbb{F}[V]^G$*-module. In fact, if* $d_1 = \cdots = d_{r-1} = 0$ *and* $d_i > 0$ *for* $i \geqslant r$, *then* $\mathrm{d}f_i / x^{p^{d_i} - 2} \in (\Omega^1)^G$ *for each* $i \geqslant r$, *and the invariant differential* 1*-forms*

$$\mathrm{d}x, \mathrm{d}f_1, \dots, \mathrm{d}f_{r-1}, \mathrm{d}f_r / x^{p^{d_r} - 2}, \dots, \mathrm{d}f_n / x^{p^{d_n} - 2}$$

constitute a basis for $(\Omega^1)^G$ *over* $\mathbb{F}[V]^G$.

Proof. Without loss of generality, we shall assume $f_i = x_i$ for $1 \leqslant i \leqslant r - 1$. Also, we shall use the notation from [**4**]. In our situation, $Q_{\det} = 1$, $Q(\hat{\mathcal{A}}) = x^{n-r+1}$ and $\mathrm{vol} = \mathrm{d}x \wedge \mathrm{d}x_1 \wedge \cdots \wedge \mathrm{d}x_n$. Note that, for $i \geqslant r$,

$$\begin{aligned}
\mathrm{d}f_i &= \mathrm{d}\biggl(\sum_{k=1}^{n} a_{id_ik} x^{p^{d_i} - 1} x_k \biggr) \\
&= \biggl(-\sum_{k=1}^{n} a_{id_ik} x^{p^{d_i} - 2} x_k \biggr) \mathrm{d}x + \sum_{k=1}^{n} a_{id_ik} x^{p^{d_i} - 1} \, \mathrm{d}x_k \\
&= x^{p^{d_i} - 2} \biggl(\biggl(-\sum_{k=1}^{n} a_{id_ik} x_k \biggr) \mathrm{d}x + \sum_{k=1}^{n} a_{id_ik} x \, \mathrm{d}x_k \biggr).
\end{aligned}$$

So, $\mathrm{d}f_i / x^{p^{d_i} - 2}$ is an invariant differential 1-form for each $i \geqslant r$. Furthermore,

$$\begin{aligned}
\mathrm{d}x \wedge \mathrm{d}x_1 \wedge \cdots \wedge \mathrm{d}x_{r-1} \wedge \mathrm{d}f_r / x^{p^{d_r} - 2} \wedge \cdots \wedge \mathrm{d}f_n / x^{p^{d_n} - 2} &= a x^{n-r+1} \, \mathrm{d}x \wedge \mathrm{d}x_1 \wedge \cdots \wedge \mathrm{d}x_n \\
&= a Q(\hat{\mathcal{A}}) Q_{\det} \, \mathrm{vol},
\end{aligned}$$

where $a \in \mathbb{F}$ is the determinant of the $(n - r + 1) \times (n - r + 1)$ matrix

$$\begin{pmatrix} a_{rd_rr} & \cdots & a_{rd_rn} \\ \vdots & \ddots & \vdots \\ a_{nd_nr} & \cdots & a_{nd_nn} \end{pmatrix}.$$

We have that $a \neq 0$, since $\mathrm{d}x, \mathrm{d}x_1, \dots, \mathrm{d}x_{r-1}, \mathrm{d}f_r, \dots, \mathrm{d}f_n$ are linearly independent over $\mathbb{F}(V)^G$, and thus

$$\mathrm{d}x \wedge \mathrm{d}x_1 \wedge \cdots \wedge \mathrm{d}x_{r-1} \wedge \mathrm{d}f_r / x^{p^{d_r} - 2} \wedge \cdots \wedge \mathrm{d}f_n / x^{p^{d_n} - 2} \neq 0.$$

So, by [**4**, Theorem 7], $(\Omega^1)^G$ is free over $\mathbb{F}[V]^G$ with

$$\mathrm{d}x, \mathrm{d}x_1, \dots, \mathrm{d}x_{r-1}, \mathrm{d}f_r / x^{p^{d_r} - 2}, \dots, \mathrm{d}f_n / x^{p^{d_n} - 2}$$

as a basis. □

3. Examples

We now give some examples to show how to use the method given in the proof of Theorem 2.3 to construct generators for $\mathbb{F}[V]^G$ and $I(W)$. First, we note that if $W \subseteq \mathbb{F}_p^n$ is an additive subgroup, then, after a suitable coordinate transformation,

$$W = \{(c_1, \dots, c_r, 0, \dots, 0) \mid c_i \in \mathbb{F}_p\}.$$

Thus,

$$\mathbb{F}[V]^G = \mathbb{F}[x, x_1^p - x^{p-1}x_1, \dots, x_r^p - x^{p-1}x_r, x_{r+1}, \dots, x_n],$$

and thus

$$I(W) = (x_1^p - x_1, \dots, x_r^p - x_r, x_{r+1}, \dots, x_n).$$

So, we shall consider examples in which $\mathbb{F} \neq \mathbb{F}_p$.

Example 3.1. We assume $\mathbb{F} \neq \mathbb{F}_p$ and take $u \in \mathbb{F} \setminus \mathbb{F}_p$. Consider the finite set

$$W = \{(a + bu, b + au) \mid a, b \in \mathbb{F}_p\} \subset \mathbb{F}^2.$$

Then W is an additive group of order p^2 generated by the basis elements $(1, u)$, $(u, 1)$. We denote by σ_1, σ_2 the algebra automorphisms they define on $\mathbb{F}[V] = \mathbb{F}[x, x_1, x_2]$ respectively. Let G_1 denote the hyperplane group generated by σ_1 and let G denote the hyperplane group G generated by σ_1 and σ_2. We have

$$\mathbb{F}[V]^{G_1} = \mathbb{F}[x, x_1^p - x^{p-1}x_1, x_2 - ux_1]$$

and

$$\mathbb{F}[V]^G = \mathbb{F}[V]^{G_2} = \mathbb{F}[x, f_1, f_2],$$

where

$$\begin{aligned} f_1 &= x_1^p - x^{p-1}x_1 - \frac{u^p - u}{1 - u^2}x^{p-1}(x_2 - ux_1) \\ &= x_1^p + \frac{u^{p+1} - 1}{1 - u^2}x^{p-1}x_1 - \frac{u^p - u}{1 - u^2}x^{p-1}x_2 \end{aligned}$$

and

$$\begin{aligned} f_2 &= (x_2 - ux_1)^p - (1 - u^2)^{p-1}x^{p-1}(x_2 - ux_1) \\ &= x_2^p - u^p x_1^p - (1 - u^2)^{p-1}x^{p-1}x_2 + u(1 - u^2)^{p-1}x^{p-1}x_1. \end{aligned}$$

Thus, $I(W) = (\hat{f}_1, \hat{f}_2)$, where

$$\hat{f}_1 = x_1^p + \frac{u^{p+1} - 1}{1 - u^2}x_1 - \frac{u^p - u}{1 - u^2}x_2$$

and

$$\hat{f}_2 = x_2^p - u^p x_1^p - (1 - u^2)^{p-1}x_2 + u(1 - u^2)^{p-1}x_1.$$

Example 3.2. Let $\mathbb{F} = \mathbb{F}_p(u)$, where u is transcendental over $\mathbb{F}_p$ (thus $\mathbb{F}$ is not perfect, as u is not a pth power in $\mathbb{F}$). Let

$$W = \{(a + cu, b + cu^2) \mid a, b, c \in \mathbb{F}_p\}$$

and let G be the group defined by W. Then G is generated by σ_1, σ_2 and σ_3, where σ_1, σ_2 and σ_3 correspond to $(1, 0)$, $(0, 1)$ and (u, u^2), respectively. We denote by G_1 the group generated by σ_1 and by G_2 the group generated by σ_1 and σ_2. Then we have

$$\mathbb{F}[V]^{G_1} = \mathbb{F}[x, x_1^p - x^{p-1}x_1, x_2],$$
$$\mathbb{F}[V]^{G_2} = \mathbb{F}[x, x_1^p - x^{p-1}x_1, x_2^p - x^{p-1}x_2]$$

and

$$\mathbb{F}[V]^G = \mathbb{F}[x, f_1, f_2],$$

where

$$f_1 = (x_1^p - x^{p-1}x_1)^p - (u^p - u)^{p-1}x^{p(p-1)}(x_1^p - x^{p-1}x_1)$$

and

$$f_2 = (x_2^p - x^{p-1}x_2) - (u^p + u)(x_1^p - x^{p-1}x_1).$$

Thus, $I(W) = (\hat{f}_1, \hat{f}_2)$, where

$$\hat{f}_1 = (x_1^p - x_1)^p - (u^p - u)^{p-1}(x_1^p - x_1)$$

and

$$\hat{f}_2 = (x_2^p - x_2) - (u^p + u)(x_1^p - x_1).$$

We note that Example 3.2 shows that if $\mathbb{F}$ is not perfect, the method given in the proof of Theorem 2.3 may fail to produce a generating set with each f_i having the form

$$f_i = x_i^{p^{d_i}} + \sum_{j=1}^{d_i}\sum_{k=1}^{n} c_{ijk} x^{p^{d_i} - p^{d_i - j}} x_k^{p^{d_i - j}},$$

where $c_{ijk} \in \mathbb{F}$. In fact, in Example 3.2,

$$f_2 = (x_2^p - (u^p + u)x_1^p) - x^{p-1}x_2 + (u^p + u)x^{p-1}x_1,$$

and clearly $x_2^p - (u^p + u)x_1^p$ is not the pth power of a linear form, as required in part (ii) of the theorem.

Acknowledgements. This research was partly supported by the NSERC. We thank the anonymous referee for helpful comments and suggestions.

References

1. D. J. Benson, *Polynomial invariants of finite groups* (Cambridge University Press, 1993).
2. C. Chevalley, Invariants of finite groups generated by reflections, *Am. J. Math.* **77** (1955), 778–782.
3. H. Derksen and G. Kemper, *Computational invariant theory*, Encyclopaedia of Mathematical Sciences, Volume 130 (Springer, 2002).
4. J. Hartmann and A. Shepler, Reflection groups and differential forms, *Math. Res. Lett.* **14** (2007), 955–971.
5. J. Hartmann and A. Shepler, Jacobians of reflection groups, *Trans. Am. Math. Soc.* **360** (2008), 123–133.
6. G. Kemper, Calculating invariant rings of finite groups over arbitrary fields, *J. Symb. Computat.* **21**(3) (1996), 351–366.
7. P. S. Landweber and R. E. Stong, The depth of rings of invariants over finite fields, in *Proc. New York Number Theory Seminar*, Lecture Notes in Mathematics, Volume 1240 (Springer, 1987).
8. H. Nakajima, Relative invariants of finite groups, *J. Alg.* **79** (1982), 218–234.
9. J.-P. Serre, Groupes finis d'automorphismes d'anneaux locaux réguliers, in *Colloque d'Algèbre (Paris, 1967)*, Exposé 8, pp. 1–11 (Ecole Normale Supérieure de Jeunes Filles, Secrétariat Matheématique, Paris, 1968).
10. G. C. Shephard and J. A. Todd, Finite unitary reflection groups, *Can. J. Math.* **6** (1954), 274–304.
11. L. Smith, *Polynomial invariants of finite groups*, Research Notes in Mathematics, Volume 6 (A. K. Peters, Boca Raton, FL, 1995).
12. W. V. Vasconcelos, *Computational methods in commutative algebra and algebraic geometry*, Algorithms and Computation in Mathematics, Volume 2 (Springer, 1998).

https://doi.org/10.1017/S0013091508001107 Published online by Cambridge University Press