INVARIANTS OF FINITE GROUPS GENERATED BY REFLECTIONS.*

By Claude Chevalley.

1. An invertible linear transformation of a finite dimensional vector space V over a field K will be called a *reflection* if it is of order two and leaves a hyperplane pointwise fixed. A group G of linear transformations of V is a *finite reflection group* if it is a finite group generated by reflections. The operations of G extend to automorphisms of the symmetric algebra S of V by the rule $g(P)(x) = P(g^{-1}(x))$, $(P \varepsilon S, x \varepsilon V)$, and an element $P \varepsilon S$ such that $g(P) = P$ for all $g \varepsilon G$ is said to be *an invariant of* G. Our main purpose in this note is to prove the theorem:

(A) *Let G be a finite reflection group in a n-dimensional vector-space V over a field K of characteristic zero. Then the K-algebra J of invariants of G is generated by n algebraically independent homogeneous elements* (*and the unit*).

A vector space A is *graded* by subspaces A^i, (i positive integer), if it is the direct sum of the A^i. The degree d^0P of $P \varepsilon A$ is the smallest integer j such that $P \varepsilon \sum_{i \leqq j} A^i$; the elements of A^i are the homogeneous elements of degree i. When the A^i are finite dimensional, the Poincaré series of A in the indeterminate t is defined as

$$P_t(A) = \sum_{i \geqq 0} \dim. A^i \cdot t^i.$$

In particular S is graded in the obvious way and $P_t(S) = (1-t)^{-n}$. Let F be the ideal generated by the homogeneous elements of strictly positive degrees in J. Then the grading of S induces a grading of the quotient space S/F. Since F is invariant under G, the operations of G in S induce automorphisms of S/F. We shall also prove:

(B) *Let $I_1, \cdots, I_n$ be a minimal system of homogeneous generators of J and let m_i be the degree of I_i, $(1 \leqq i \leqq n)$. Then*

$$P_t(S/F) = (1-t)^{-n} \cdot \prod_{i=1}^{i=n} (1-t^{m_i}).$$

* Received June 9, 1955.

The product of the m_i is equal to the order of G and to the dimension of S/F. The natural representation of G in S/F is equivalent to the regular representation.

2. Two lemmas. In this paragraph, the characteristic p of the infinite groundfield K is allowed to be $\neq 0$ and G denotes a finite reflection group in V whose order N is prime to p.[1] To any element $P \varepsilon S$ we can then associate its average over G:

$$M(P) = 1/N \sum_{g \varepsilon G} g(P).$$

LEMMA 1. *Let $U_1, \cdots, U_m$ be invariants of G such that U_1 does not belong to the ideal generated in J by $U_2, \cdots, U_m$. Let P_i, $(1 \leqq i \leqq m)$, be homogeneous elements of S satisfying a relation $\sum_1^m P_i \cdot U_i = 0$. Then $P_1 \varepsilon F$.*

If $d^0 P_1 = 0$, then it follows from the assumption and from the relation

$$M(P_1) \cdot U_1 + \cdots + M(P_m) \cdot U_m = 0$$

that $P_1 = M(P_1) = 0$. Assume now $d^0 P_1 > 0$ and the lemma to be true for all relations $\sum_1^m Q_i \cdot U_i = 0$ with homogeneous Q_i and $d^0 Q_1 < d^0 P_1$. Let s be a reflection of G leaving pointwise fixed a hyperplane with equation $L = 0$. Then $s(P_i) - P_i = L \cdot Q_i$, $(Q_i \varepsilon S,\ i = 1, \cdots, m)$, and

$$Q_1 \cdot U_1 + \cdots + Q_m \cdot U_m = 0$$

whence, by induction, $Q_1 \varepsilon F$ or, otherwise said, $s(P_1) \equiv P_1 \bmod. F$; the group G being generated by reflections, we have then $g(P_1) \equiv P_1 \bmod. F$ for any $g \varepsilon G$, whence $P_1 \equiv M(P_1) \bmod. F$; since P_1 is homogeneous of strictly positive degree, the same is true for $M(P_1)$; therefore $M(P_1) \varepsilon F$ and $P_1 \varepsilon F$.

LEMMA 2. *Assume K to be a perfect field. Let I_i, $(1 \leqq i \leqq m)$, be homogeneous invariants which form an ideal basis of F,[2] with $m_i = d^0 I_i$ prime to p for $i \leqq r$. Then $I_1, \cdots, I_r$ are algebraically independent.*

Let us suppose the lemma to be false and let $H(I_1, \cdots, I_r) = 0$ be a non trivial relation of minimal degree between $I_1, \cdots, I_r$ where $H(y_1, \cdots, y_r)$

---

[1] In this paper, we are primarily interested in the case $p = 0$, but Lemma 2 will be used in a forthcoming paper of A. Borel, to appear in Jour. Math. Pur. Appl.

[2] This always exists since by the classical theorem for invariants of a finite group, J is a finitely generated K-algebra.

is a polynomial in r letters y_i. We may assume that there exists an integer h such that for any monomial $y_1^{k_1}\cdot\cdots\cdot y_r^{k_r}$ of H we have

$$k_1\cdot m_1+\cdots+k_r\cdot m_r=h.$$

The partial derivatives $\partial H/\partial y_i$ are not all zero, because otherwise (for $p\neq 0$, the only case for which it is not obvious), K being perfect, H would be the p-th power of a polynomial H^*, and $H^*(I_1,\cdots,I_r)=0$ would be a non trivial relation of strictly smaller degree. Set

$$H_i=\partial H/\partial y_i\,(I_1,\cdots,I_r), \qquad (1\leqq i\leqq r);$$

then $H_1,\cdots,H_r$ are in J and not all zero; after a possible permutation of indices, we may assume that they belong to the ideal generated in J by the first s of them, but that none of $H_1,\cdots,H_s$ belongs to the ideal generated by the other ones in J. Set

$$H_{s+j}=\sum_{j=1}^{i=s}V_{j,i}H_i.$$

Let x_k, $(1\leqq k\leqq n)$, be coordinates in V. Since

$$\sum_{i=1}^{i=r}H_i\cdot(\partial I_i/\partial x_k)=0, \qquad (1\leqq k\leqq n),$$

we have by Lemma 1

$$\partial I_i/\partial x_k+\sum_{j=1}^{j=r-s}V_{j,i}(\partial I_{s+j}/\partial x_k)\,\varepsilon\,F, \qquad (1\leqq i\leqq s;1\leqq k\leqq n)$$

(the left hand sides are homogeneous in the x_k by the above remark on the monomials of H). Multiplying this relation by x_k and adding the relations thus obtained, we get

$$m_iI_i+\sum_{j=1}^{j=r-s}V_{j,i}m_{s+j}I_{s+j}=\sum_{l=1}^{l=m}A_{i,l}I_l, \qquad (1\leqq i\leqq s).$$

where the $A_{i,l}$ are forms belonging to the ideal generated by $x_1,\cdots,x_n$. For reasons of homogeneity, we have $A_{i,l}=0$ if I_l is not of strictly lower degree than I_i; m_i being prime to p for $i\leqq r$, we see that I_i belongs to the ideal generated by the other I_j, which is a contradiction. Thus $I_1,\cdots,I_r$ are algebraically independent.

3. Proofs of Theorems (A) and (B). We assume again the ground-field to be of characteristic zero and denote as in Lemma 2 by $I_1,\cdots,I_m$ homogeneous invariants of G forming an ideal basis of F. By Lemma 2 they are algebraically independent, whence also $m \leqq n$. Using averages over G, it is readily seen by induction on the degree that the unit and the I_i generate J and thus, to finish the proof of (A), there remains to show that $m \geqq n$.

Let $x_1, \cdots, x_n$ be coordinates in V and let $K(x)$ be the field of rational functions in the x_i. It is acted upon in a natural way by G and we denote by L the subfield of elements invariant under G. Then $K(x)$ is a Galois extension of L, with Galois group G and L has also transcendence degree n over K. On the other hand, G being *finite*, every invariant in $K(x)$ is classically the quotient of two invariant polynomials; thus $L = K(J)$ is generated by the I_i, and $m \geqq n$.

LEMMA 3. *Let $P_1, \cdots, P_s$ be homogeneous elements of S whose residue classes* mod F *are linearly independent over K in S/F. Then $P_1, \cdots, P_s$ are linearly independent over $K(J)$.*

Let $V_1 \cdot P_1 + \cdots + V_s \cdot P_s = 0$ be a relation with $V_i \varepsilon K(J)$, $(1 \leqq i \leqq s)$. We have to prove that $V_i = 0$ for all i and it is enough to consider the case where the V_i are homogeneous elements of J such that $d^0 V_i + d^0 P_i$ is equal to a constant h independent of i.

By the degree of the monomial $I_1^{k_1} \cdots I_n^{k_n}$ we mean its degree as element of S, i.e. $k_1 m_1 + \cdots + k_n m_n$. Let S_j, $(j = 1, 2, \cdots)$, be the different monomials in the I_i arranged by increasing degrees, with $S_1 = 1$. We have

$$V_i = \sum_{j \geqq 0} k_{ij} S_j, \qquad (k_{ij} \varepsilon K, k_{ij} = 0 \text{ for } d^0 V_i \neq d^0 S_j, \ (1 \leqq i \leqq n)),$$

and our relation may be written

$$\sum_{j \geqq 0} W_j \cdot S_j = 0, \qquad (W_j = \sum_{i=1}^{i=s} k_{ij} P_i),$$

where W_j is homogeneous, of degree equal to $h - d^0 S_j$. Assume that $k_{ij} = 0$ for $1 \leqq i \leqq s$ and $j < t$. Since by Theorem A the monomial S_t does not belong to the ideal generated in J by the S_j with $j > t$, we have by Lemma 1 $W_t \varepsilon F$ and the hypothesis gives then $k_{it} = 0$ for $i = 1, \cdots, s$. This proves by induction on j that $k_{ij} = 0$ for all i, j, and the lemma.

We now come to the proof of (B). The field $K(x)$ being a normal extension of $K(J)$ with Galois group G, has degree N over $K(J)$, hence the dimension of S/F over K is finite. Let $A_1, \cdots, A_q$ be homogeneous polynomials whose residue classes mod F form a basis of S/F. By induction on the degree we see that every $P \varepsilon S$ may be expressed as linear combination

11

of the A_i with coefficients in J, and this expression is unique in view of Lemma 3. Hence

$$P_t(S) = P_t(S/F) \cdot P_t(J);$$

but $P_t(S) = (1-t)^{-n}$ and Theorem A gives $P_t(J) = \prod_1^n (1-t^{m_i})^{-1}$, whence the first assertion of (B). We may also write

$$P_t(S/F) = \prod_{i=1}^{i=n} (1+t+t^2+\cdots+t^{m_i-1})$$

and, setting $t=1$, we get $\dim. S/F = m_1 \cdot \cdots \cdot m_n$. Since every element of $K(x)$ may be written as the quotient of a polynomial by an invariant polynomial, it also follows from the above and Lemma 3 that the A_i form a basis of $K(x)$ over $K(J)$, whence $N = \dim. S/F$.

We have for $g \varepsilon G$

$$g(A_i) = \sum_{j=1}^{j=N} a_{ij}(g) A_j, \qquad (i=1,\cdots,N),$$

where the $a_{ij}(g)$ are homogeneous elements of J and where $a_{ii}(g) \varepsilon K$ by homogeneity. The matrices $(a_{ij}(g))$ describe the natural representation of G in $K(x)$, considered as vector space over $K(J)$. If we reduce the coefficients mod F we get the natural representation of G in S/F, considered as vector space over K; this reduction does not affect the diagonal coefficients, hence both representations have the same character and are equivalent. But G is the Galois group of the normal extension $K(x)$ of $K(J)$, so that the former representation is equivalent to the regular representation, which proves the last statement of (B).

COLUMBIA UNIVERSITY.