ACTA ARITHMETICA
XXXI (1976)

Equivalence classes of polynomials over finite fields

by

GARY L. MULLEN (Sharon, Pa.)

1. Introduction. The study of modular invariants of polynomials over a finite field was initiated by Jordan and Dickson in a series of papers ([4], [5], and [6]), where the transformations were restricted to the group of non-singular linear transformations. Later works on the subject considered various other specialized groups of linear transformations, see for example [3]. L. Carlitz in [1] enlarged the group of transformations under consideration to the full group of all permutations.

In this paper we treat the more general case where Ω may be taken to be an arbitrary group of permutations. Formulas, given in terms of the number of cycles of Ω, are obtained for the number of equivalence classes of a given order and in particular for the total number of classes induced by the group Ω. As a simple illustration of the type of results which we obtain, suppose Ω is the cyclic group of order four generated by the permutation $\varphi(x) = x^3+4x^2+2x$ over $K = \mathrm{GF}(5)$. If $\lambda(\Omega)$ denotes the number of classes induced by Ω then $\lambda(\Omega) = 825$, and moreover, Ω decomposes $K[x]$ into 25 classes of order one, 50 classes of order two, and 750 classes of order four.

Let $K = \mathrm{GF}(q)$ denote the finite field of order q where $q = p^n$ and K^r $(r \geqslant 1)$ represent the product of r copies of K. The ring of polynomials in r indeterminates over K will be denoted by $K[x_1, \ldots, x_r] = K[\bar{x}]$. Two polynomials $f, g \in K[\bar{x}]$ are equal if they are equal as functions. It is well known that every function of K^r into K can be represented as a polynomial in r indeterminates, each of which is of degree less than q. Since there are q^{q^r} such polynomials, they represent all such functions.

The group of all permutations of K^r will be denoted by Φ, which is clearly isomorphic to the symmetric group S_{q^r}. That Ω is an arbitrary subgroup of Φ will be denoted by $\Omega < \Phi$ and $|\Omega|$ will mean the order of Ω.

2. General theory. We begin with the following basic definition.

DEFINITION 2.1. Let $\Omega < \Phi$ and $f, g \in K[\bar{x}]$. Then f is *right equivalent* to g relative to Ω if there exists a $\varphi \in \Omega$ such that $f\varphi = g$.

The above relation is easily seen to be an equivalence relation on $K[\bar{x}]$ which reduces to that of Carlitz [1] when $\Omega = \Phi$. Since we will be dealing only with right equivalence, we will simply say that f is *equivalent* to g relative to Ω. A similar notion of left equivalence and applications to permutation polynomials will be discussed elsewhere.

The equivalence class relative to Ω of a polynomial f will be denoted by $f\Omega$ and $\mu(f, \Omega)$ will represent the order of the class of f while the number of equivalence classes induced by Ω will be denoted by $\lambda(\Omega)$.

DEFINITION 2.2. Let $\Omega < \Phi$ and $f \in K[\bar{x}]$. A permutation $\varphi \in \Omega$ is an *automorphism* of f relative to Ω if $f\varphi = f$.

Let $A(f, \Omega)$ and $\nu(f, \Omega)$ denote the group and number respectively of automorphisms of the polynomial f relative to Ω. It is easily seen that if $\Omega < \Phi$ then

$$A(f, \Omega) < A(f, \Phi) \quad \text{and} \quad A(f, \Omega) = A(f, \Phi) \cap \Omega.$$

If $A(f, \Omega)$ is normal in Ω then the class $f\Omega$ is a group under the operation $(f\varphi)(f\psi) = f(\varphi\psi)$. If $f\varphi = g$ for some $\varphi \in \Omega$ then $A(g, \Omega) = \varphi^{-1}A(f, \Omega)\varphi$ so that $\nu(g, \Omega) = \nu(f, \Omega)$. Thus the number of automorphisms depends only upon the class and not the particular polynomials in the class.

The following theorem, whose proof is immediate, generalizes the corresponding result of Carlitz ([1], Theorem 4.5).

THEOREM 2.1. *Let $f \in K[\bar{x}]$. Then for any group Ω*

$$\mu(f, \Omega)\nu(f, \Omega) = |\Omega|.$$

Suppose $K = \{a_1, \ldots, a_q\}$ and $f \in K[\bar{x}]$. Let

$$T_i = \{\bar{\beta} \in K^r \mid f(\bar{\beta}) = a_i\}, \quad i = 1, \ldots, q.$$

Upon reordering, we may assume that the non-empty T_i's are $T_1, \ldots, T_t$. Clearly t is the order of the range of f and $\pi_f = \{T_i \mid i = 1, \ldots, t\}$ is the *partition* of the polynomial f. Each polynomial determines a unique partition π_f of K^r. Moreover, if we are given a partition π of K^r of order t, then there are $q(q-1)\ldots(q-t+1)$ polynomials whose partition is π.

The following theorem provides a necessary and sufficient condition for the equivalence of two polynomials relative to a group Ω in terms of their respective partitions.

THEOREM 2.2. *Let $\Omega < \Phi$ and $f, g \in K[\bar{x}]$. Suppose that*

$$S_i = \{\bar{\beta} \in K^r \mid f(\bar{\beta}) = a_i\}, \quad i = 1, \ldots, q$$

and

$$T_i = \{\bar{\beta} \in K^r \mid g(\bar{\beta}) = a_i\}, \quad i = 1, \ldots, q.$$

Then f is equivalent to g relative to Ω if and only if there exists $\varphi \in \Omega$ such that $\varphi(T_i) \subseteq S_i$ for $i = 1, \ldots, q$.

Proof. Suppose there exists $\varphi \in \Omega$ such that $f\varphi = g$. Let $\bar{\beta} \in \varphi(T_i)$ for some i which implies that $\bar{\beta} = \varphi(\bar{\alpha})$ where $\bar{\alpha} \in T_i$. Thus $f(\bar{\beta}) = f\big(\varphi(\bar{\alpha})\big) = g(\bar{\alpha}) = a_i$ so that $\bar{\beta} \in S_i$ which proves the necessity.

Now let $\bar{\alpha} \in K^r$ so that $\bar{\alpha} \in T_i$ for some i which implies that $g(\bar{\alpha}) = a_i$. By hypothesis $\varphi(\bar{\alpha}) \in S_i$ for the same i. Thus $f\big(\varphi(\bar{\alpha})\big) = g(\bar{\alpha})$ and f is equivalent to g relative to Ω.

Following Carlitz, define $N_f(a)$ to be the number of solutions in K^r of the equation $f = a$. As a corollary we have the following result of Carlitz.

COROLLARY 2.3. *If $f, g \in K[\bar{x}]$ then f is equivalent to g relative to Φ if and only if $N_f(a) = N_g(a)$ for all $a \in K$.*

It might be suspected that if $\Omega < \Phi$, then

$$\mu(f, \Phi) = \mu(f, \Omega)[\Phi : \Omega]$$

for all f where $[\Phi : \Omega]$ denotes the index of Ω in Φ. That this is not the case in general may be seen from the simple example $f = a$ where $a \in K$.

We next determine conditions for a permutation to be an automorphism of a given polynomial. More precisely we have

LEMMA 2.4. *Suppose $f \in K[\bar{x}]$ and $\pi_f = \{T_i \mid i = 1, \ldots, t\}$ is the partition of f. Then a permutation φ is an automorphism of f if and only if $\varphi(T_i) \subseteq T_i$ for $i = 1, \ldots, t$.*

Proof. Let $f = g$ in Theorem 2.2.

If φ is a permutation of K^r then its cycle structure can be considered. We view the cycles of φ as sets whose elements are r-tupes of elements of K. When we list the cycles of a permutation as $\sigma_1, \ldots, \sigma_s$, we are assuming that the σ's are disjoint and are including those of length one. The cycles of a permutation induce a partition of K^r into disjoint subsets.

THEOREM 2.5. *Let φ be a permutation and $f \in K[\bar{x}]$ with partition $\pi_f = \{T_i \mid i = 1, \ldots, t\}$. Suppose that the cycles of φ are $\sigma_1, \ldots, \sigma_s$. Then φ is an automorphism of f if and only if for each $j = 1, \ldots, s$, $\sigma_j \subseteq T_i$ for some $i = 1, \ldots, t$, and, moreover, every T_i contains some σ_j.*

Proof. For sufficiency, by Lemma 2.4, it suffices to show that $\varphi(T_i) \subseteq T_i$ for $i = 1, \ldots, t$. Fix i and let $\varphi(\bar{\alpha}) \in \varphi(T_i)$ where $\bar{\alpha} \in T_i$. Since the σ's form a partition of K^r, we have $\bar{\alpha} \in \sigma_j$ for some $j = 1, \ldots, s$. But then $\varphi(\bar{\alpha}) \in \sigma_j$ so that $\varphi(\bar{\alpha}) \in T_i$.

For necessity, let σ_j be an arbitrary cycle of φ and suppose $\bar{\alpha} \in \sigma_j$. Then $\bar{\alpha} \in T_i$ for some i. Let $\bar{\beta} \neq \bar{\alpha} \in \sigma_j$. If no such $\bar{\beta}$ exists, the proof is complete. Since $\bar{\alpha}$ and $\bar{\beta}$ are in the same cycle of φ, we have $\bar{\beta} = \varphi^l(\bar{\alpha})$ for some positive integer l. By Lemma 2.4 $\varphi(\bar{\alpha}) \in T_i$ so that we have $\varphi^l(\bar{\alpha}) \in T_i$. The last statement of the theorem is obvious since if φ is an automorphism of f and $\bar{\alpha} \in T_i$, then the cycle containing $\bar{\alpha}$ is also in T_i.

One observes that φ is an automorphism of a polynomial f if and only if the cycles of φ are a refinement of the partition of f. We may generalize Theorem 2.5 slighty with

THEOREM 2.6. *Suppose $H < \Omega < \Phi$ and let $f \in K[\bar{x}]$. Then $H < A(f, \Omega)$ if and only if the cycles of each $\varphi \in H$ are a refinement of π_f.*

Suppose that a permutation φ has cycles $\sigma_1, \ldots, \sigma_s$. We now determine the number of partitions $\pi = \{T_i \mid i = 1, \ldots, t\}$ of order t such that the s cycles of φ are a refinement of π. Let $P(s, t)$ denote this number. If $s < t$, then clearly $P(s, t) = 0$ since in this case at least one T_i will fail to contain a σ_j. If $s \geqslant t$ then $P(s, t)$ is simply the number of ways of placing s different objects into t similar cells so that each cell contains at least one object. This number is the Stirling number of the second kind. Hence

$$P(s, t) = \begin{cases} \dfrac{1}{t!} \displaystyle\sum_{j=0}^{t-1} (-1)^j \binom{t}{j} (t-j)^s & \text{if} \quad s \geqslant t, \\ 0 & \text{if} \quad s < t. \end{cases}$$

THEOREM 2.7. *Suppose φ has s cycles. Then the number of polynomials for which φ is an automorphism is q^s.*

Proof. $P(s, t)$ counts the number of partitions π of order t for which the s cycles of φ are a refinement of π. The number of polynomials whose partition is π is given by $q(q-1) \ldots (q-t+1)$. Hence

$$\sum_{t=1}^{s} P(s, t) q(q-1) \ldots (q-t+1)$$

counts the number of polynomials f such that $f\varphi = f$.

On the other hand $P(s, t)$ counts the number of functions from a set of s elements whose range consists of t fixed elements where we do not distinguish order in the range. The t fixed elements can be chosen in $\binom{q}{t}$ ways from the field K. Thus $P(s, t)\binom{q}{t} t!$ counts the number of functions from a set of s elements to a set of q elements whose range has order t. Summing over all t counts the total number of functions from a set of s elements to a set of q elements. This number of functions is also given by q^s which completes the proof.

3. Cyclic groups. Suppose $\Omega = \langle \varphi \rangle$ is a cyclic group of order n. Let $H(t) = \langle \varphi^{n/t} \rangle$ denote the unique subgroup of Ω of order t where $t|n$. Let $s(t)$ represent the number of cycles of $\varphi^{n/t}$. Since any two generators of a cyclic group have the same number of cycles, we may call $s(t)$ the number of cycles of $H(t)$. Finally, let $M(t)$ denote the number of polynomials f such that $A(f, \Omega) = H(t)$ for each $t|n$.

Clearly $q^{s(t)}$ counts the number of polynomials f such that $H(t) < A(f, \Omega)$. However, some of the polynomials f counted above are such that $H(t) \lneq A(f, \Omega)$. There are precisely $\sum M(u)$ such polynomials where the sum is over all u for which $u|n$, $t|u$, and $t \neq u$. Thus we have proven

THEOREM 3.1. *For all t dividing n*

$$M(t) = q^{s(t)} - \sum M(u),$$

where the sum is over all u such that $u|n$, $t|u$, $t \neq u$.

COROLLARY 3.2. *For all $t|n$ there are $tM(t)/n$ classes of order n/t and*

$$\lambda(\Omega) = \frac{1}{n} \sum_{t|n} tM(t).$$

COROLLARY 3.3. *If $f \in K[\bar{x}]$ then $\nu(f, \Omega) = t$, or equivalently $\mu(f, \Omega) = n/t$, if and only if $H(t)$ is the largest subgroup of Ω for which the cycles of $H(t)$ are a refinement of π_f.*

Note. By the largest subgroup of Ω for which the cycles of $H(t)$ are a refinement of π_f we mean that if $H(t) < K$ and the cycles of K are a refinement of π_f then $H(t) = K$.

We now wish to determine when two groups induce equivalent decompositions of $K[\bar{x}]$.

DEFINITION 3.1. Let $\Omega_1, \Omega_2 < \Phi$. Suppose that Ω_1 and Ω_2 decompose $K[\bar{x}]$ into the equivalence classes $A_1, \ldots, A_{t_1}$ and $B_1, \ldots, B_{t_2}$ respectively. Then Ω_1 and Ω_2 induce *equivalent* decompositions of $K[\bar{x}]$ if $\{|A_i|\}$ is a permutation of $\{|B_i|\}$ where $|A|$ denotes the order of the set A. Otherwise, the decompositions are *inequivalent*.

THEOREM 3.4. *Suppose Ω_i $(i = 1, 2)$ are cyclic groups of order n and $H_i(t)$ denotes the unique subgroup of Ω_i of order t, where $t|n$. Then Ω_1 and Ω_2 induce equivalent decompositions of $K[\bar{x}]$ if and only if for each $t|n$, $H_1(t)$ and $H_2(t)$ have the same number of cycles.*

Proof. Follows from Theorem 3.1 and its corollaries.

One should observe from Theorem 3.4 that isomorphic subgroups need not induce equivalent decompositions of $K[\bar{x}]$. For example, if $r = 1$ and $|\Omega_i| = p$ a prime for $i = 1, 2$ where $2p \leqslant q$ then one can construct subgroups Ω_1 and Ω_2 which are isomorphic but which have different numbers of cycles and thus induce inequivalent decompositions of $K[\bar{x}]$.

4. Theory of cycles. We now define a notion of "cycles" for an arbitrary group of permutations which generalizes the idea of cycles for a single permutation. Let $\mathscr{P}$ denote the set of all partitions of K^r and suppose P_1 and P_2 are the partitions $A_1, \ldots, A_{s_1}$ and $B_1, \ldots, B_{s_2}$ respect-

ively. We say $P_1 \leqslant P_2$ if P_1 is a refinement of P_2, that is, if each A_i is a subset of some B_j. The relation $\leqslant$ is a partial order on $\mathscr{P}$. $P_3 \in \mathscr{P}$ is an *upper bound* of P_1 and P_2 if $P_1 \leqslant P_3$ and $P_2 \leqslant P_3$ while $P_4 \in \mathscr{P}$ is a *lower bound* of P_1 and P_2 if $P_4 \leqslant P_1$ and $P_4 \leqslant P_2$.

It is well known that $\mathscr{P}$ is a lattice relative to these definitions if we construct $\inf\{P_1, P_2\}$ and $\sup\{P_1, P_2\}$ as follows. Set $C_{ij} = A_i \cap B_j$. Then

$$\inf\{P_1, P_2\} = \{C_{ij} \mid C_{ij} \neq \emptyset\}.$$

To obtain $\sup\{P_1, P_2\}$, consider A_1 and take the union of A_1 and all B_j for which B_j contains an element of A_1. Using these B's we now take the union over all A_i for which A_i contains an element of some B_j. We continue to combine the A's and B's in this manner until we arrive at the first point for which $\bigcup A_i = \bigcup B_i$ and call this set D_1. If $D_1 \neq K^r$ we then start with some A_j not in D_1 and repeat the process until finally we obtain sets $D_1, \ldots, D_s$ such that $\bigcup_{i=1}^{s} D_i = K^r$. Then

$$\sup\{P_1, P_2\} = \{D_1, \ldots, D_s\}.$$

Let Ω be a fixed group of permutations. If $\varphi \in \Omega$ then the cycles of φ form a partition P_φ of K^r so that $P_\varphi \in \mathscr{P}$. Consider the collection $\{P_\varphi\}$ of all partitions of K^r as φ runs through the elements of Ω. Since $\mathscr{P}$ is a lattice, $\sup_{\varphi \in \Omega} P_\varphi$ is an element $P \in \mathscr{P}$. Let P denote the partition composed of the subsets $C_1, \ldots, C_s$. We may now make the

DEFINITION 4.1. Let Ω be a group of permutations. Then the sets $C_1, \ldots, C_s$ are the *cycles* of Ω and s is the *number* of cycles of Ω.

The next lemma shows that the above notion of cycles is a *bona fide* generalization of the notion of cycles of a single permutation.

LEMMA 4.1. *Let $\Omega = \langle \varphi \rangle$ and suppose φ has t cycles and $A_1, \ldots, A_s$ are the cycles of Ω from Definition 4.1. Then $s = t$, and, moreover, $A_1, \ldots, A_s$ are the cycles of φ.*

Proof. Let $\sigma_1, \ldots, \sigma_t$ denote the cycles of φ and let $\psi \in \Omega$ so that $\psi = \varphi^l$ for some positive integer l. Let $\delta_1, \ldots, \delta_\nu$ be the cycles of ψ and P_φ, P_ψ denote the partitions of K^r formed from the σ's and δ's respectively. For each $i = 1, \ldots, \nu$; $\delta_i \subseteq \sigma_j$ for some j since $\psi = \varphi^l$. Thus $\sup\{P_\varphi, P_\psi\} = P_\varphi$ and therefore $\sup_{\psi \in \Omega} P_\psi = P_\varphi$.

THEOREM 4.2. *Let π be a partition of K^r of order t. Suppose Ω has cycles $A_1, \ldots, A_s$. Then $A_1, \ldots, A_s$ are a refinement of π if and only if the cycles of each permutation in Ω are a refinement of π.*

Proof. Suppose $P = \sup_{\varphi \in \Omega} P_\varphi$ and $P \leqslant \pi$, then $P_\varphi \leqslant \pi$ for all $\varphi \in \Omega$. Conversely, if $P_\varphi \leqslant \pi$ for all $\varphi \in \Omega$ then $P \leqslant \pi$.

The above theorem will enable us to compute in terms of the number of cycles of an arbitrary group Ω, the number of polynomials f such that Ω leaves f fixed.

5. Abelian groups. Let Ω be a finite abelian group of type $A = (p_1^{r_1}, \ldots, p_k^{r_k})$ where $p_1, \ldots, p_k$ are primes with $p_1 \leqslant \ldots \leqslant p_k$ and $r_1, \ldots, r_k$ are positive integers with $r_i \geqslant r_{i+1}$ if $p_i = p_{i+1}$. In order to simplify the statement of results in this section we make the

DEFINITION 5.1. Let $A = (p_1^{r_1}, \ldots, p_k^{r_k})$ and $B = (q_1^{s_1}, \ldots, q_l^{s_l})$ be two types of finite abelian groups. Then A *equals* B if $k = l$; $p_i = q_i$ and $r_i = s_i$ for $i = 1, \ldots, l$. B is *less than* A (A is *greater than* B) if (1) $1 \leqslant l \leqslant k$; (2) Each distinct q occurs in the list of distinct p's; (3) There exists a 1-1 function ω from $\{1, \ldots, l\}$ into $\{1, \ldots, k\}$ such that for each $i = 1, \ldots, l$, $q_i^{s_i}$ divides $p_{\omega(i)}^{r_{\omega(i)}}$. B is *strictly less than* A (A is *strictly greater than* B) if B is less than A but not equal to A.

Thus an abelian group Ω of type A has a subgroup of type B if and only if B is less than A. Let $n(B)$ denote the number of subgroups of Ω of type B for each type B less than A. If Ω is an abelian p-group of type A then $n(B)$ is known for all B less than A, see for example [8]. Suppose the subgroups of Ω of type B are denoted by $H(i; B)$ and $s(i; B)$ represents the number of cycles of $H(i; B)$. Let $M(i; B)$ denote the number of polynomials f such that $H(i; B) = A(f, \Omega)$. If B is a type less than A then we may assume that $B = (q_1^{s_1}, \ldots, q_l^{s_l})$.

THEOREM 5.1. *If Ω is abelian of type A, then for each type B less than A*

$$M(i; B) = q^{s(i;B)} - \sum_{C} \sum_{j} M(j; C) \tag{5.1}$$

for $i = 1, \ldots, n(B)$ where the outer sum is over all types C strictly greater than B and less than A, while the inner sum is over those j for which $H(j; C)$ contains the given subgroup $H(i; B)$.

Proof. The proof of Theorem 3.1 may be extended to this case.

COROLLARY 5.2. *If Ω is abelian of type A then there are*

$$\Big(\prod_{i=1}^{l} q_i^{s_i} \Big/ \prod_{i=1}^{k} p_i^{r_i}\Big) \sum_{B} \sum_{i=1}^{n(B)} M(i; B) \tag{5.2}$$

classes of order $\prod_{i=1}^{k} p_i^{r_i} / \prod_{i=1}^{l} q_i^{s_i}$ and

$$\Big(q^{q^r} - \sum_{B} \sum_{i=1}^{n(B)} M(i; B)\Big) \Big/ \prod_{i=1}^{k} p_i^{r_i} \tag{5.3}$$

classes of order $\prod_{i=1}^{k} p_i^{r_i}$ where the outer sum in (5.2) is over all types $B = (q_1^{t_1}, \ldots$

$\ldots, \bar{q}_m^{t_m})$ *less than* A *for which* $\prod_{i=1}^{m} \bar{q}_i^{t_i} = \prod_{i=1}^{l} q_i^{s_i}$ *and the outer sum in* (5.3) *is over all types* B *less than* A.

Proof. For a fixed type $B = (q_1^{s_1}, \ldots, q_l^{s_l})$

$$\Big(\prod_{i=1}^{k} p_i^{r_i} \Big/ \prod_{i=1}^{l} q_i^{s_i}\Big) \sum_{i=1}^{n(B)} M(i; B)$$

counts the number of classes of order $\prod_{i=1}^{k} p_i^{r_i} / \prod_{i=1}^{l} q_i^{s_i}$ arising from polynomials whose automorphism group has type B. Suppose $B' = (\bar{q}_1^{t_1}, \ldots, \bar{q}_m^{t_m})$ is a type for which $\prod_{i=1}^{m} \bar{q}_i^{t_i} = \prod_{i=1}^{l} q_i^{s_i}$. If f is any polynomial whose automorphism group has this type B', then

$$\nu(f, \Omega) = \prod_{i=1}^{l} q_i^{s_i}$$

so that by Theorem 2.1

$$\mu(f, \Omega) = \prod_{i=1}^{k} p_i^{r_i} \Big/ \prod_{i=1}^{l} q_i^{s_i}$$

from which the result follows.

Corollary 5.3. *If* Ω *is abelian of type* A *then*

$$\lambda(\Omega) = \sum_{B} \Big(\prod_{i=1}^{l} q_i^{s_i} \Big/ \prod_{i=1}^{k} p_i^{r_i}\Big) \sum_{i=1}^{n(B)} M(i; B) + \Big(q^{q^r} - \sum_{B} \sum_{i=1}^{n(B)} M(i; B)\Big) \Big/ \prod_{i=1}^{k} p_i^{r_i}$$

where the two outer sums are over all types B *less than* A.

Corollary 5.4. *Let* $f \in K[\bar{x}]$ *and* Ω *be abelian of type* A. *Then*

$$\nu(f, \Omega) = \prod_{i=1}^{l} q_i^{s_i}$$

if and only if for some type $B = (q_1^{s_1}, \ldots, q_l^{s_l})$ *less than* A, $H(i; B)$ *for some* $i = 1, \ldots, n(B)$ *is the largest subgroup of* Ω *for which the cycles of* $H(i; B)$ *are a refinement of* π_f.

Let Ω_1 and Ω_2 denote abelian groups of type A. Define $H_j(i; B)$, $s_j(i; B)$, and $M_j(i; B)$ for $j = 1, 2$ as above. Then as a restatement of Corollary 5.2 we have

Corollary 5.5. Ω_1 *and* Ω_2 *induce equivalent decompositions of* $K[\bar{x}]$ *if and only if for each* d *dividing* $|\Omega_1|$, $\{s_1(i; B)\}$ *and* $\{s_2(i; B)\}$ *satisfy*

$$\sum_{B} \sum_{i=1}^{n(B)} M_1(i; B) = \sum_{B} \sum_{i=1}^{n(B)} M_2(i; B) \tag{5.4}$$

where the outer sums run over all types $B = (q_1^{s_1}, \ldots, q_l^{s_l})$ *less than* A *for which* $\prod_{i=1}^{l} q_i^{s_i} = d$ *and the* $M_j(i; B)$ *are given by* (5.1).

If Ω_1 and Ω_2 are cyclic of order n then the double sums in (5.4) reduce to a single term so that we have a generalization of Theorem 3.4.

6. Conjugate subgroups. In this section we show that conjugate subgroups of Φ induce equivalent decompositions of $K[\bar{x}]$. We first prove several very general results concerning an arbitrary group Ω. Let Ω be order n and suppose the subgroups of Ω are $H_1, \ldots, H_\nu$ of orders $d_1, \ldots, d_\nu$. Let s_i denote the number of cycles of H_i and suppose $M(i)$ represents the number of polynomials f such that $A(f, \Omega) = H_i$.

Theorem 6.1. *For each* $i = 1, \ldots, \nu$

$$M(i) = q^{s_i} - \sum_{j} M(j) \tag{6.1}$$

where the sum is over all j *such that* $H_i \lneqq H_j$.

Proof. q^{s_i} counts the number of polynomials f such that $H_i < A(f, \Omega)$. From this we subtract the number of f for which the containment is proper.

Corollary 6.2. *If* $d|n$ *then there are*

$$\frac{d}{n} \sum_{\substack{i \\ |H_i| = d}} M(i)$$

classes of order n/d *and*

$$\lambda(\Omega) = \frac{1}{n} \sum_{d|n} d \sum_{\substack{i \\ |H_i| = d}} M(i).$$

Corollary 6.3. *Let* $f \in K[\bar{x}]$ *and suppose* $d|n$. *Then* $\nu(f, \Omega) = d$ *if and only if for some* $i = 1, \ldots, \nu$ $|H_i| = d$ *and* H_i *is the largest subgroup of* Ω *for which the cycles of* H_i *are a refinement of* π_f.

Corollary 6.4. *Suppose* Ω_1 *and* Ω_2 *are of order* n *and* $\{s_i\}$ *and* $\{s_i'\}$ *represent the number of cycles of the various subgroups of* Ω_1 *and* Ω_2. *Then* Ω_1 *and* Ω_2 *induce equivalent decompositions of* $K[\bar{x}]$ *if and only if* $\{s_i\}$ *and* $\{s_i'\}$ *satisfy*

$$\sum M_1(i) = \sum M_2(i)$$

for each divisor d *of* n, *where the left and right sums run over all subgroups of order* d *of* Ω_1 *and* Ω_2 *respectively, and the* $M_j(i)$ $(j = 1, 2)$ *are given by* (6.1).

We now prove that conjugate subgroups of Φ induce equivalent decompositions of $K[\bar{x}]$. First we need a

LEMMA 6.5. *If Ω_1 and Ω_2 are conjugate subgroups of Φ, then Ω_1 and Ω_2 have the same number of cycles. Moreover, they have the same number of cycles of the same size.*

Proof. Let $\Omega_2 = \varphi^{-1}\Omega_1\varphi$ for some $\varphi \in \Phi$. Suppose $\varphi_1 \in \Omega_1$ has cycles $\sigma_1, \ldots, \sigma_s$. Then $\psi_1 = \varphi^{-1}\varphi_1\varphi$ has cycles $\delta_1, \ldots, \delta_s$ where $\delta_i = \{\varphi(\bar{\alpha}) \mid \bar{\alpha} \in \sigma_i\}$ so that $|\delta_i| = |\sigma_i|$ for $i = 1, \ldots, s$. Similarly, if the cycles of φ_2 are $\tau_1, \ldots, \tau_t$, then the cycles of $\psi_2 = \varphi^{-1}\varphi_2\varphi$ are $\gamma_i = \{\varphi(\bar{\alpha}) \mid \bar{\alpha} \in \tau_i\}$ so that $|\gamma_i| = |\tau_i|$ for $i = 1, \ldots, t$.

Let $P_{\varphi_1}, P_{\varphi_2}, P_{\psi_1}$, and P_{ψ_2} denote the partitions of K^r induced by the cycles of the permutations $\varphi_1, \varphi_2, \psi_1$, and ψ_2 respectively. When computing $\sup\{P_{\varphi_1}, P_{\varphi_2}\}$, suppose that σ_i collects $\tau_{i_1}, \ldots, \tau_{i_m}$. Then δ_i collects $\gamma_{i_1}, \ldots, \gamma_{i_m}$ when we compute $\sup\{P_{\psi_1}, P_{\psi_2}\}$. Since $|\sigma_i| = |\delta_i|$, δ_i cannot collect any more of the γ's.

One checks that $\tau_{i_j} = \tau_{i_k}$ $(j \neq k)$ if and only if $\gamma_{i_j} = \gamma_{i_k}$ $(j \neq k)$ so that the number of distinct elements collected by σ_i is the same as the number of distinct elements collected by δ_i. If τ_k is an arbitrary cycle of φ_2 collected by σ_i then one may easily verify that $\tau_k \subseteq \sigma_i$ if and only if $\gamma_k \subseteq \delta_i$. Thus if τ_k collects a σ different from σ_i, then γ_k collects a δ different from δ_i of the same size and conversely.

Suppose the cycle σ_1 is combined with the σ's and τ's to obtain a set A_1. Then, starting with δ_1 we form a set B_1 composed of δ's and γ's such that $|A_1| = |B_1|$. Continuing, we obtain sets $A_1, \ldots, A_s$ and $B_1, \ldots, B_s$ such that

$$\bigcup_{i=1}^{s} A_i = \bigcup_{i=1}^{s} B_i = K^r$$

where $|A_i| = |B_i|$ for $i = 1, \ldots, s$. Moreover, whatever σ's compose a set A_i the corresponding δ's compose B_i and conversely.

We continue this process until we obtain $\sup_{\varphi_1 \in \Omega_1} P_{\varphi_1}$ which gives the cycles of Ω_1, say $S_1, \ldots, S_v$. Similarly we get $\sup_{\psi_1 \in \Omega_2} P_{\psi_1}$ which gives the cycles of Ω_2, say $T_1, \ldots, T_v$ where $|S_i| = |T_i|$ for $i = 1, \ldots, v$ which completes the proof.

THEOREM 6.6. *If Ω_1 and Ω_2 are conjugate subgroups of Φ then Ω_1 and Ω_2 induce equivalent decompositions of $K[\bar{x}]$.*

Proof. Since the subgroups of Ω_2 are conjugate to those of Ω_1, applying the lemma to each subgroup of Ω_1, we see that the subgroups of Ω_1 have the same number of cycles as the corresponding subgroups of Ω_2 which together with Theorem 6.1 and its corollaries proves the theorem.

COROLLARY 6.7. *Any two p-Sylow subgroups of Φ induce equivalent decompositions of $K[\bar{x}]$.*

References

[1] L. Carlitz, *Invariantive theory of equations in a finite field*, Trans. Amer. Math. Soc. 75 (1953), pp. 405–427.

[2] S. R. Cavior, *Equivalence classes of sets of polynomials over a finite field*, Journ. Reine Angew. Math. 225 (1967), pp. 191–202.

[3] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover Publications, Inc., New York 1958.

[4] — *A theory of invariants*, Amer. J. Math. 31 (1909), pp. 337–354.

[5] — *General theory of modular invariants*, Trans. Amer. Math. Soc. 10 (1909), pp. 123–158.

[6] J. Dieudonne, *Oeuvres de Camille Jordan*, Gauthier-Villar et Co., Paris 1961.

[7] J. Riordan, *An Introduction to Combinatorial Analysis*, John Wiley & Sons, Inc., New York 1958.

[8] Y. Yeh, *On prime power abelian groups*, Bull. Amer. Math. Soc. 54 (1948), pp. 323–327.

Received on 29. 10. 1974 (636)