where the combination of the $\pm$ signs is the same as in the representation of $L(m+b)$. The rest of the argument is already as in the proof of the Theorem 3. For O-estimates see [2].

If we have a region defined by a system of algebraic inequalities then the order of the error term is usually determined by a single piece of the boundary, that is by just one of the inequalities. In this sense, we will not be getting much new.

Let us also mention that all estimates still hold if we restrict ourselves to lattice points with square-free (or cube-free etc.) coordinates as considered by Lursmanašvili or Podsypanin.

Note added in proof by the editor. Similar results have been obtained by B. Novák. However he has notified the editors that his paper *Remarks on Jarník Ω-method in lattice point theory*, announced in J. Number Theory 8(1976), p. 39, will not appear.

References

[1] B. Diviš, *Lattice point theory of irrational ellipsoids with an arbitrary center*, Mh. Math. 83(1977), pp. 279–307.

[2] — *Lattice point theory in polyhedra*, to appear.

[3] — *Mean value estimates in lattice point theory*, Mh. Math. 84(1977), pp. 21–28.

[4] V. Jarník, *Über Gitterpunkte in mehrdimensionalen Ellipsoiden*, Math. Ann. 100 (1928), pp. 699–721; Tôhoku Math. J. 30(1929), pp. 354–371.

[5] — *Bemerkungen zu Landauschen Methoden in der Gitterpunktlehre*, Abh. aus Zahlentheorie und Analysis zur Erinnerung an E. Landau, Berlin 1968, pp. 139–156.

[6] B. Novák, *Mean value theorems in the theory of lattice points with weight II*, Comm. Math. Univ. Carol. 11 (1970), pp. 53–81.

[7] — *Über eine Methode der Ω-Abschätzungen*, Czech. Math. J. 21 (1971), pp. 257–279.

Received on 29. 7. 1976 (862)

ACTA ARITHMETICA
XXXV (1979)

Weak equivalence of functions over a finite field

by

GARY L. MULLEN (Sharon, Pa.)

1. Introduction. In a series of papers [1], [3], and [8], L. Carlitz, S. Cavior, and the author studied right equivalence of functions over a finite field. In [3] and [7] S. Cavior and the author studied properties of left equivalence of functions over a finite field, while in [3] Cavior considered the notion of weak equivalence.

In this paper we study a form of weak equivalence which generalizes all of the above types of equivalence of functions over a finite field. Even though we restrict our study to functions of one variable, it will be clear that our results are readily extendable to several variables and in fact, may be extended to functions from one finite set to another.

In Section 1 we are concerned with preliminaries while in Section 2 we present the general theory of weak equivalence. In Section 3 the theory of weak equivalence is applied in the case where the groups of permutations are cyclic. In Section 4, as a special case of weak equivalence, we present an application to similarity of functions over a finite field as considered by Cavior in [3]. Finally in Section 5 we give several applications of weak equivalence to permutation polynomials over a finite field.

Let $K = \mathrm{GF}(q)$ denote the finite field of order q where $q = p^n$. Let $K[x]$ represent the ring of polynomials over K. Two polynomials $f, g \in K[x]$ are equal if they are equal as functions. By the Lagrange Interpolation Formula ([5], p. 55), each function from K into K can be expressed uniquely as a polynomial of degree less than q so that $K[x]$ consists of exactly q^q functions. The group of all permutations of K will be denoted by Φ so that Φ is isomorphic to S_q, the symmetric group of order $q!$. That Ω is an arbitrary subgroup of Φ will be denoted by $\Omega < \Phi$, $|\Omega|$ will denote the order of Ω, and $[\Phi\colon \Omega]$ will represent the index of Ω in Φ.

2. General theory. We begin with

DEFINITION 2.1. Let $\Omega_1, \Omega_2 < \Phi$ and $f, g \in K[x]$. Then f is *weakly equivalent* to g relative to Ω_1 and Ω_2 if there exists $\varphi_1 \in \Omega_1$ and $\varphi_2 \in \Omega_2$ such that $\varphi_1 f \varphi_2 = g$.

We now list several special cases of the above definition.

Case 1: $\Omega_1 = \{\text{id.}\}$, $\Omega_2 = \Phi$ right equivalence of Carlitz in [1];

Case 2: $\Omega_1 = \{\text{id.}\}$, $\Omega_2 < \Phi$ right equivalence of the author in [8];

Case 3: $\Omega_1 = \Phi$, $\Omega_2 = \{\text{id.}\}$ left equivalence of Cavior in [3];

Case 4: $\Omega_1 < \Phi$, $\Omega_2 = \{\text{id.}\}$ left equivalence of the author in [7];

Case 5: $\Omega_1 = \Phi$, $\Omega_2 = \Phi$ weak equivalence of Cavior in [3].

The above relation is an equivalence relation on $K[x]$. Let $\Omega_1 f \Omega_2$ and $\mu(f, \Omega_1, \Omega_2)$ denote the equivalence class of f and the number of elements in the class of f relative to Ω_1 and Ω_2. Further, let $\lambda(\Omega_1, \Omega_2)$ denote the number of equivalence classes induced by the groups Ω_1 and Ω_2.

One can easily observe that if $f \in K[x]$ and $f\Omega_2 = \{f = f_1, f_2, \ldots, f_n\}$ where $f\Omega_2$ is the right equivalence class of f relative to Ω_2 as defined in [8], then

$$\Omega_1 f \Omega_2 = \Omega_1 f_1 \cup \ldots \cup \Omega_1 f_n \tag{2.1}$$

where $\Omega_1 f_i$ is the left equivalence class of f_i relative to Ω_1 as defined in [7]. Similarly we have

$$\Omega_1 f \Omega_2 = g_1 \Omega_2 \cup \ldots \cup g_m \Omega_2 \tag{2.2}$$

where $\Omega_1 f = \{f = g_1, g_2, \ldots, g_m\}$ is the left equivalence class of f relative to Ω_1 and $g_i\Omega_2$ is the right equivalence class of g_i relative to Ω_2. Hence every weak equivalence class can be decomposed into a union of disjoint left or right equivalence classes. For further details regarding left and right equivalence classes, see [7] and [8].

If $K = \{\alpha_1, \ldots, \alpha_q\}$ and $f \in K[x]$ let $S_i = \{\gamma \in K |\ f(\gamma) = \alpha_i\}$ for $i = 1, \ldots, q$. Assume that the non-empty S_i's are $S_1, \ldots, S_t$ where t is the order of the range of f. Then $\pi_f = \{S_i |\ i = 1, \ldots, t\}$ is the *partition* of f and t is the *order* of π_f. We now state several necessary and sufficient conditions for the weak equivalence of two functions in terms of their respective partitions. Using an argument similar to that given by Cavior in [3] we have the following generalization of Theorem 5.1 of [3].

THEOREM 2.1. *Let $\Omega_1, \Omega_2 < \Phi$ and $f, g \in K[x]$. Let*

$$\pi_f = \{S_i |\ i = 1, \ldots, t\}; \quad f(S_i) = \gamma_i, \quad i = 1, \ldots, t,$$

$$\pi_g = \{T_i |\ i = 1, \ldots, r\}; \quad g(T_i) = \delta_i, \quad i = 1, \ldots, r.$$

Then f is weakly equivalent to g relative to Ω_1 and Ω_2 if and only if $\{|S_i| \mid i = 1, \ldots, t\}$ is a permutation of $\{|T_i| \mid i = 1, \ldots, r\}$ and there exists $\varphi_1 \in \Omega_1, \varphi_2 \in \Omega_2$ such that $\varphi_2(T_i) = S_i$ $(i = 1, \ldots, t)$ and $\varphi_1(\gamma_i) = \delta_i$ $(i = 1, \ldots, t)$.

Using Theorem 2.1 of [7] we may state

THEOREM 2.2. *Let $\Omega_1, \Omega_2 < \Phi$ and $f, g \in K[x]$. Then f is weakly equivalent to g relative to Ω_1 and Ω_2 if and only if there exists $\varphi_1 \in \Omega_1$, $\varphi_2 \in \Omega_2$ such that $\pi_{f\varphi_2} = \pi_g = \{S_i |\ i = 1, \ldots, t\}$ and $\varphi_1(\gamma_i) = \delta_i$ where $f\varphi_2(S_i) = \gamma_i$ and $g(S_i) = \delta_i$ for $i = 1, \ldots, t$.*

Using Theorem 2.2 of [8] we may state

THEOREM 2.3. *Let $\Omega_1, \Omega_2 < \Phi$ and $f, g \in K[x]$. Suppose that $\pi_g = \{T_i |\ i = 1, \ldots, t\}$. Then f is weakly equivalent to g relative to Ω_1 and Ω_2 if and only if there exists $\varphi_1 \in \Omega_1$, $\varphi_2 \in \Omega_2$ such that $\varphi_2(T_i) = S_i$ for $i = 1, \ldots, t$ where $\pi_{\varphi_1 f} = \{S_i |\ i = 1, \ldots, t\}$.*

DEFINITION 2.2. Let $\Omega_1, \Omega_2 < \Phi$ and $f \in K[x]$. If $\varphi_1 \in \Omega_1$ and $\varphi_2 \in \Omega_2$ then the pair (φ_1, φ_2) is a *weak automorphism* of f relative to Ω_1 and Ω_2 if $\varphi_1 f \varphi_2 = f$.

The set of weak automorphisms of a function f relative to Ω_1 and Ω_2 forms a group $A(f, \Omega_1, \Omega_2)$ of order $\nu(f, \Omega_1, \Omega_2)$ under the operation $(\psi_1, \psi_2)(\varphi_1, \varphi_2) = (\psi_1\varphi_1, \psi_2\varphi_2)$. Clearly if $\Omega_1, \Omega_2 < \Phi$ then $A(f, \Omega_1, \Omega_2) < A(f, \Phi, \Phi)$ and

$$A(f, \Omega_1, \Omega_2) = A(f, \Phi, \Phi) \cap (\Omega_1 \times \Omega_2).$$

If $\varphi_1 f \varphi_2 = g$ for some $\varphi_1 \in \Omega_1, \varphi_2 \in \Omega_2$ then

$$A(g, \Omega_1, \Omega_2) = (\varphi_1, \varphi_2^{-1}) A(f, \Omega_1, \Omega_2)(\varphi_1^{-1}, \varphi_2) \tag{2.3}$$

so that $\nu(g, \Omega_1, \Omega_2) = \nu(f, \Omega_1, \Omega_2)$. Thus the number of weak automorphisms of a function depends only upon the class and not on the particular functions in the class.

The following theorem, whose proof we omit, generalizes the corresponding results of Carlitz, Cavior, and the author.

THEOREM 2.4. *Let $\Omega_1, \Omega_2 < \Phi$ and $f \in K[x]$. Then*

$$\mu(f, \Omega_1, \Omega_2)\nu(f, \Omega_1, \Omega_2) = |\Omega_1||\Omega_2|. \tag{2.4}$$

We now state a result which generalizes Lemma 2.3 of [7], Lemma 2.4 of [8], and gives a necessary and sufficient condition under which a pair (φ_1, φ_2) is a weak automorphism of a function f.

THEOREM 2.5. *Let $f \in K[x]$. If $\varphi_1 \in \Omega_1$, $\varphi_2 \in \Omega_2$ then $\varphi_1 f \varphi_2 = f$ if and only if $\pi_f \varphi_2 = \pi_f = \{S_i |\ i = 1, \ldots, t\}$ and $\varphi_1(\gamma_i) = \delta_i$ where $f\varphi_2(S_i) = \gamma_i$ and $f(S_i) = \delta_i$.*

Thus $\varphi_1 f \varphi_2 = f$ if and only if for each $i = 1, \ldots, t$, $\varphi_2(S_i) = S_{j_i}$ and $\varphi_1(\gamma_i) = \delta_i$. Theorem 2.5 will prove to be very useful in determining the number of functions f such that $\varphi_1 f \varphi_2 = f$. It will be seen that the number of such f depends only upon the cycle structure of φ_1 and φ_2. In order to count the number of such f, we will count the number of partitions π with the property that $\pi\varphi_2 = \pi$. The number of such partitions will depend only upon the lengths of the cycles of φ_2. For each such partition π we will then determine the number of functions f arising from π with

the property that $\varphi_1(\gamma_i) = \delta_i$. The number of such f will depend only upon the number of cycles of φ_1 of various lengths.

If $\varphi_1 \in \Omega_1, \varphi_2 \in \Omega_2$ and $\varphi_1 f = f\varphi_2 = f$ then $\varphi_1 f \varphi_2 = f$. That the converse is not true in general may be seen by the following example where $K = \mathrm{GF}(3)$, $\varphi_1(x) = \varphi_2(x) = 2x$, and $f(x) = x$. We now determine the number $N(\varphi_1, \varphi_2)$ of functions f such $\varphi_1 f \varphi_2 = \varphi_1 f = f\varphi_2 = f$.

THEOREM 2.6. *If φ_1 has $m(1)$ cycles of length one and φ_2 has s cycles then*

$$N(\varphi_1, \varphi_2) = [m(1)]^s. \tag{2.5}$$

Proof. By Theorem 2.5 of [8], $f\varphi_2 = f$ if and only if the cycles of φ_2 refine the partition π_f. By Lemma 2.3 of [7], $\varphi_1 f = f$ if and only if $\varphi_1(a) = a$ for all $a \in R_f$, the range of f. If $S(s, t)$ denotes the Stirling number of the second kind, then $S(s, t)$ counts the number of partitions π of order t for which the s cycles of φ_2 refine π. Let F_{φ_1} represent the set of fixed points of φ_1 and set $m = m(1)$. Then for each partition π of order t there are $m(m-1)\dots(m-t+1)$ functions f whose partition is π and for which $R_f \subseteq F_{\varphi_1}$. Summing over all $t = 1, \dots, m$ we get

$$N(\varphi_1, \varphi_2) = \sum_{t=1}^{m} S(s, t) m(m-1)\dots(m-t+1).$$

If $s > m$ then $m(m-1)\dots(m-t+1) = 0$ for $t > m$. If $m > s$ then $S(s, t) = 0$ when $t > s$. Hence

$$N(\varphi_1, \varphi_2) = \sum_{t=1}^{s} S(s, t) m(m-1)\dots(m-t+1) = [m(1)]^s$$

by an elementary combinatorial argument.

We note that if $\varphi_1 = \mathrm{id.}$, then $m(1) = q$ so that $N(\mathrm{id.}, \varphi_2) = q^s$ as in Theorem 2.7 of [8]. If $\varphi_2 = \mathrm{id.}$, then $s = q$ so that $N(\varphi_1, \mathrm{id.}) = [m(1)]^q$ as in Theorem 2.4 of [7] when $r = 1$.

If φ_1 and φ_2 are fixed permutations, we now determine the number of functions f such that $\varphi_1 f \varphi_2 = f$ where $\varphi_1 f \neq f$ and $f\varphi_2 \neq f$. By Theorems 2.5 and 2.6 we must count the number of partitions $\pi = \{T_i \mid i = 1, \dots, t\}$ such that $\{T_i\varphi_2\}$ is a permutation of $\{T_i\}$ with the property that for at least one i, $T_i\varphi_2 = T_j$ where $j \neq i$.

We first prove the following

LEMMA 2.7. *Let π be a partition of K such that $\pi\varphi_2 = \pi$. If $T \in \pi$ and T intersects a cycle σ of φ_2, then T must intersect σ in a number of elements which divides the length of σ.*

Proof. Let m be the smallest positive integer such that $T\varphi_2^m = T$. Suppose $T \cap \sigma = \{a_{i_1}, \dots, a_{i_l}\}$ where $i_1 < \dots < i_l$ so that $a_{i_j}\varphi_2^m = a_{i_{j+1}}$. Let $a \in \sigma$ and suppose $a_{i_1}\varphi_2^n = a$. Let $n = mq_1 + r$ where $0 \leqslant r < m$.

Since $T\varphi_2^m = T$ we see that $a \in T\varphi_2^r$. The sets $T, T\varphi_2, \dots, T\varphi_2^{m-1}$ are pairwise disjoint and they have the same number of elements. Thus $ml = k$ so that $l|k$ where k is the length of σ. This completes the proof of the lemma.

We have shown that if π is a partition such that $\pi\varphi_2 = \pi$ and $T \in \pi$ intersects two or more cycles of φ_2, then T must intersect each cycle in a number of elements which divides the length of the cycle. Further, if $T_1, \dots, T_d$ partition a cycle σ of length k, then the T's are cyclic in the sense that $T_i = T_1\varphi_2^{i-1}$ and the T's form a cyclic partition of length $d = k/l$.

Suppose φ_2 has s cycles. Let $P(s)$ represent the number of partitions of s. Each summand p_i of a partition of s will be used to construct partitions which overlap into various cycles. For example, if $s = p_1 + \dots + p_g$ then for each $i = 1, \dots, g$ the summand p_i will be used to construct partitions which overlap into some p_i cycles. If these cycles are $\sigma_{i_1}, \dots, \sigma_{ip_i}$ of lengths $k_{i1}, \dots, k_{ip_i}$ then $(k_{i1}, \dots, k_{ip_i})$ will determine the type of overlap which occurs. If $p_i = 1$ then we will construct partitions which intersect just the cycle σ_{i1}.

Let $B(s; p_1, \dots, p_g)$ denote the number of ways that s distinct cycles can be divided into g distinguishable classes containing $p_1, \dots, p_g$ cycles where $s = p_1 + \dots + p_g$. By an elementary combinatorial argument we may prove

$$B(s; p_1, \dots, p_g) = \frac{s!}{p_1! p_2! \dots p_g!}. \tag{2.6}$$

If some of the p_i's are equal then (2.6) is to be interpreted as follows. Suppose $p_{i_1}, \dots, p_{i_h}$ are distinct and that for $j = 1, \dots, h$, c_j denotes the number of times that p_{i_j} occurs. Then (2.6) becomes

$$\frac{s!}{\prod_{j=1}^{h} (p_{i_j}!)^{c_j}\, p_{i_j}}. \tag{2.7}$$

Let $p_1 + \dots + p_g$ be a partition of s. For each $i = 1, \dots, g$ let $\sigma_{i1}, \dots, \sigma_{ip_i}$ be the p_i cycles of lengths $k_{i1}, \dots, k_{ip_i}$ under consideration. We determine the number $\beta_i(k_{i1}, \dots, k_{ip_i})$ of partitions π of $\sigma_{i1} \cup \dots \cup \sigma_{ip_i}$ with the property that φ_2 permutes the subsets of π. To this end let $\tau(n)$ denote the number of divisors of n.

LEMMA 2.8. *If $p_i = 1$ and σ_{i1} is of length k_{i1} then*

$$\beta_i(k_{i1}) = \tau(k_{i1}). \tag{2.8}$$

Proof. By Lemma 2.7, we know that if a set T intersects σ_{i1}, it must do so in l_{i1} elements where $l_{i1}|k_{i1}$. Let $d = k_{i1}/l_{i1}$ and suppose $\sigma_{i1} = (a_1, \dots, a_{k_{i1}})$. We construct a partition of σ_{i1} containing d subsets each of order l_{i1}. Define

$$
\begin{aligned}
T_1 &= \{a_1, a_{d+1}, \ldots, a_{k_{i1}-d+1}\},\\
T_2 &= \{a_2, a_{d+2}, \ldots, a_{k_{i1}-d+2}\},\\
&\cdots\cdots\cdots\cdots\cdots\\
T_d &= \{a_d, a_{2d}, \ldots, a_{k_{i1}}\}.
\end{aligned} \tag{2.9}
$$

Clearly $T_1, \ldots, T_d$ have the same number of elements, $T_i \cap T_j = \emptyset$ if $i \neq j$, $T_{i+1} = T_i\varphi_2$ for $i = 1, \ldots, d-1$ and $T_d\varphi_2 = T_1$. Thus the partition $\{T_1, \ldots, T_d\}$ has the property that φ_2 permutes the T's. Conversely if $\{S_1, \ldots, S_m\}$ partitions σ_{i1} and is such that for each $i = 1, \ldots, m$, $S_i\varphi_2 = S_{j_i}$ then $\{S_1, \ldots, S_m\}$ must be of the form (2.9) for some l_{i1} dividing k_{i1}. Since there are $\tau(k_{i1})$ divisors of k_{i1}, the proof is complete.

LEMMA 2.9. *Suppose $p_i > 1$ and $\sigma_{i1}, \ldots, \sigma_{ip_i}$ are of lengths $k_{i1}, \ldots, k_{ip_i}$ where $(k_{i1}, \ldots, k_{ip_i}) = 1$. Then*

$$\beta_i(k_{i1}, \ldots, k_{ip_i}) = \tau(k_{i1}) \ldots \tau(k_{ip_i}) + 1. \tag{2.10}$$

Proof. Let π be a partition of $\sigma_{i1} \cup \ldots \cup \sigma_{ip_i}$ with the property that $\pi\varphi_2 = \pi$. Suppose $T \in \pi$ intersects all of the cycles $\sigma_{i1}, \ldots, \sigma_{ip_i}$. Let m be the smallest positive integer such that $T\varphi_2^m = T$. From Lemma 2.7 we see that $ml_{ij} = k_{ij}$ for $j = 1, \ldots, p_i$ where l_{ij} denotes the number of elements from σ_{ij} in T. Thus $m|k_{ij}$ for all j so that $l_{ij} = k_{ij}$. Hence the only set which intersects all of the σ's is $T = \sigma_{i1} \cup \ldots \cup \sigma_{ip_i}$. The remaining partitions are such that each subset intersects a single σ_{ij}. By Lemma 2.8 there are $\tau(k_{ij})$ partitions of σ_{ij} for $j = 1, \ldots, p_i$ from which (2.10) follows.

Note. In the proof of Lemma 2.9, we need not consider the case where a set intersects less than p_i cycles because that case will be taken care of by a different partition of s.

LEMMA 2.10. *Suppose $p_i > 1$ and $\sigma_{i1}, \ldots, \sigma_{ip_i}$ are of lengths $k_{i1}, \ldots, k_{ip_i}$ where $(k_{i1}, \ldots, k_{ip_i}) > 1$. Then*

$$\beta_i(k_{i1}, \ldots, k_{ip_i}) = \sum_{\substack{l_{i1}+\ldots+l_{ip_i} | k_{i1}+\ldots+k_{ip_i} \\ l_{ij} | k_{ij}}} \frac{k_{i1} \ldots k_{ip_i}}{l_{i1} \ldots l_{ip_i}} \frac{(l_{i1}+\ldots+l_{ip_i})}{(k_{i1}+\ldots+k_{ip_i})}. \tag{2.11}$$

Proof. Let π be a partition of $\sigma_{i1} \cup \ldots \cup \sigma_{ip_i}$ with the property that $\pi\varphi_2 = \pi$. Suppose $T \in \pi$ intersects σ_{ij} in l_{ij} elements for $j = 1, \ldots, p_i$ where $l_{ij} | k_{ij}$. Let m be the smallest positive integer such that $T\varphi_2^m = T$. The sets $T, T\varphi_2, \ldots, T\varphi_2^{m-1}$ are pairwise disjoint and they each have $l_{i1}+\ldots+l_{ip_i}$ elements. Hence $m(l_{i1}+\ldots+l_{ip_i}) = k_{i1}+\ldots+k_{ip_i}$ so that $(l_{i1}+\ldots+l_{ip_i}) | (k_{i1}+\ldots+k_{ip_i})$.

There are $(k_{i1} \ldots k_{ip_i})/(l_{i1} \ldots l_{ip_i})$ ways to construct T since from each σ_{ij} there are k_{ij}/l_{ij} ways to choose the desired l_{ij} elements. Once T is chosen, the remaining sets are uniquely determined. Since the numbering of the sets is immaterial, we divide by the number of sets which is

$(k_{i1}+\ldots+k_{ip_i})/(l_{i1}+\ldots+l_{ip_i})$. Summing over all $l_{i1}+\ldots+l_{ip_i}$ where $l_{ij} | k_{ij}$ for $j = 1, \ldots, p_i$ yields (2.11).

THEOREM 2.11. *Let $s = p_1+\ldots+p_g$. For $i = 1, \ldots, g$ consider the p_i cycles $\sigma_{i1}, \ldots, \sigma_{ip_i}$ of lengths $k_{i1}, \ldots, k_{ip_i}$. The total number of partitions π of K such that π arises from this partition of s and π has the property that $\pi\varphi_2 = \pi$ is given by*

$$\prod_{i=1}^{g} \beta_i(k_{i1}, \ldots, k_{ip_i}) - 1 - a \prod_{\substack{1 \leq i \leq g \\ 1 \leq j \leq p_i}} \tau(k_{ij}) \tag{2.12}$$

where

$$a = \begin{cases} 0 & \text{if all } p_i = 1 \text{ or for some } i,\ p_i > 1 \text{ and } (k_{i1}, \ldots, k_{ip_i}) > 1, \\ 1 & \text{if for all } i = 1, \ldots, g,\ (k_{i1}, \ldots, k_{ip_i}) = 1. \end{cases} \tag{2.13}$$

Proof. The product

$$\prod_{i=1}^{g} \beta_i(k_{i1}, \ldots, k_{ip_i}) \tag{2.14}$$

counts the number of partitions π such that $\pi\varphi_2 = \pi$ which arise from the given partition of s. There is one partition π counted in (2.14) which arises when for all i and j, $l_{ij} = k_{ij}$. This partition π has the property that the cycles of φ_2 refine π and is thus already counted by Theorem 2.6.

If all $p_i = 1$ or for some i, $p_i > 1$ and $(k_{i1}, \ldots, k_{ip_i}) > 1$ then we let $a = 0$ since in this case each partition arising from (2.14) will have been counted exactly once. Suppose that for all $i = 1, \ldots, g$, $(k_{i1}, \ldots, k_{ip_i}) = 1$. Let π be a partition with the property that each set in π intersects a single cycle σ. Any such partition π will have been counted in the partition of s when all $p_i = 1$ since in that case each set in the partition intersects just one cycle σ. There are

$$\prod_{\substack{1 \leq i \leq g \\ 1 \leq j \leq p_i}} \tau(k_{ij}) \tag{2.15}$$

such partitions π. Hence we take $a = 1$ and the proof is complete.

We now determine the number $N(\varphi_2)$ of partitions $\pi = \{T_i | \ i = 1, \ldots, t\}$ of K with the property that $\pi\varphi_2 = \pi$ and for some i, $T_i\varphi_2 = T_j$ where $j \neq i$.

THEOREM 2.12. *Suppose φ_2 has s cycles. Then*

$$N(\varphi_2) = \sum_{p_1+\ldots+p_g=s} \sum \Big(\prod_{i=1}^{g} \beta_i(k_{i1}, \ldots, k_{ip_i}) - 1 - a \prod_{\substack{1 \leq i \leq g \\ 1 \leq j \leq p_i}} \tau(k_{ij}) \Big) \tag{2.16}$$

where the outer sum is over all $P(s)$ partitions $p_1+\ldots+p_g$ of s, the inner sum is over all $(s!)/p_1! \ldots p_g!$ ways that s cycles can be divided into g dis-

tinguishable classes containing $p_1, \dots, p_g$ *cycles where* $p_1 + \dots + p_g = s$, *a is given by* (2.13), *and the* k_{ij}*'s are lengths of the cycles of* φ_2.

Proof. We sum (2.12) over all

$$\frac{s!}{p_1! \dots p_g!} \tag{2.17}$$

ways that s cycles can be divided into g distinguishable classes containing $p_1, \dots, p_g$ cycles where $p_1 + \dots + p_g = s$. If the p_i's are not distinct then (2.17) is to be interpreted as follows. Suppose $p_{i_1}, \dots, p_{i_h}$ are distinct and that for $j = 1, \dots, h$, c_j denotes the number of times that p_{i_j} occurs. Then (2.17) becomes

$$\frac{s!}{\prod_{j=1}^{h} (p_{i_j}!)^{c_j} p_{i_j}}. \tag{2.18}$$

Summing over all $P(s)$ partitions of s completes the proof.

We note that if $\varphi_2 = \mathrm{id}.$ then $N(\varphi_2)$ should be zero since φ_2 fixes every subset in a partition. If $\varphi_2 = \mathrm{id}.$, then all $k_{ij} = 1$ so that (2.12) becomes zero and thus $N(\varphi_2) = 0$ by (2.16).

THEOREM 2.13. *Suppose* φ_2 *has* s *cycles. Then the number of partitions* π *with the property that* $\pi\varphi_2 = \pi$ *is given by*

$$\sum_{t=1}^{s} S(s, t) + N(\varphi_2) \tag{2.19}$$

where $S(s, t)$ *is the Stirling number of the second kind and* $N(\varphi_2)$ *is given by* (2.16).

Proof. $S(s, t)$ counts the number of partitions π of order t for which the s cycles of φ_2 refine π. Each such partition π has the property that if $T \in \pi$ then $T\varphi_2 = T$ from which (2.19) follows.

As an illustration of the above theory, let $K = \mathrm{GF}(5)$ and suppose that in cyclic notation $\varphi_2 = (01)(23)$ so that $s = 3$. The lengths of the cycles of φ_2 are $k_1 = k_2 = 2$ and $k_3 = 1$ so that $\tau(k_1)\tau(k_2)\tau(k_3) = 4$. For simplicity of notation let N be the value of (2.12). We list in (2.20) all partitions π with the property that $\pi\varphi_2 = \pi$.

Consider the partition $s = 3$:

$\beta_1(k_1, k_2, k_3) = 5$, $a = 1$, and $N = 0$.

Consider the partition $s = 2+1$:

$\beta_1(k_1, k_2)\beta_2(k_3) = 3$, $a = 0$, $N = 2$ and the corresponding partitions are π_1 and π_2.

$\beta_1(k_1, k_3)\beta_2(k_2) = 6$, $a = 1$, $N = 1$ and the corresponding partition is π_3.

$\beta_1(k_2, k_3)\beta_2(k_1) = 6$, $a = 1$, $N = 1$ and the corresponding partition is π_4.

Consider the partition $s = 1+1+1$:

$\beta_1(k_1)\beta_2(k_2)\beta_3(k_3) = 4$, $a = 0$, $N = 3$ and the corresponding partitions are π_5, π_6, and π_7.

Each of the partitions π_i $(i = 1, \dots, 7)$ has the property that φ_2 moves at least one subset of the partition and thus $N(\varphi_2) = 7$. There are five partitions π_i $(i = 8, \dots, 12)$ listed in (2.20) with the property that φ_2 leaves each subset fixed so that by (2.19) there are a total of 12 partitions π such that $\pi\varphi_2 = \pi$.

$$\begin{aligned}
\pi_1 &= \{\{0, 2\}, \{1, 3\}, \{4\}\}, & \pi_7 &= \{\{0\}, \{1\}, \{2\}, \{3\}, \{4\}\},\\
\pi_2 &= \{\{0, 3\}, \{1, 2\}, \{4\}\}, & \pi_8 &= \{\{0, 1, 2, 3, 4\}\},\\
\pi_3 &= \{\{2\}, \{3\}, \{0, 1, 4\}\}, & \pi_9 &= \{\{0, 1, 2, 3\}, \{4\}\},\\
\pi_4 &= \{\{0\}, \{1\}, \{2, 3, 4\}\}, & \pi_{10} &= \{\{0, 1\}, \{2, 3, 4\}\},\\
\pi_5 &= \{\{0, 1\}, \{2\}, \{3\}, \{4\}\}, & \pi_{11} &= \{\{2, 3\}, \{0, 1, 4\}\},\\
\pi_6 &= \{\{2, 3\}, \{0\}, \{1\}, \{4\}\}, & \pi_{12} &= \{\{0, 1\}, \{2, 3\}, \{4\}\}.
\end{aligned} \tag{2.20}$$

We now consider a partition π with the property $\pi\varphi_2 = \pi$ and for some $T_i \in \pi$, $T_i\varphi_2 = T_j$ where $j \neq i$. We will then determine the number of functions f such that $\pi_f = \pi$ and $\varphi_1 f \varphi_2 = f$ where φ_1 is a fixed permutation. The number of such f will only depend upon the number of cycles of φ_1 of a given length.

DEFINITION 2.3. We say that a partition π has a *cyclic part of length* j relative to φ_2 if there are sets $T_1, \dots, T_j \in \pi$ such that $T_i\varphi_2 = T_{i+1}$ for $i = 1, \dots, j-1$ and $T_j\varphi_2 = T_1$.

We denote by $c(j)$ the number of cyclic parts of length j even though this number depends upon the permutation φ_2. We now prove

THEOREM 2.14. *Suppose* φ_1 *has* $m(j)$ *cycles of length* j. *Let* π *be a partition such that* $\pi\varphi_2 = \pi$, *for some* $T_i \in \pi$, $T_i\varphi_2 = T_j$ $(j \neq i)$, *and suppose* π *has* $c(j)$ *cyclic parts of length* j. *Then the number of functions* f *such that* $\varphi_1 f \varphi_2 = f$ *where* $\pi_f = \pi$ *is given by*

$$\prod_j j^{c(j)} \left[m(j)\left(m(j)-1\right) \dots \left(m(j)-\left(c(j)-1\right)\right)\right] \tag{2.21}$$

where the product is over all distinct lengths j *of cycles of* φ_1.

Proof. Suppose $T_1, \dots, T_j$ are sets in a partition π_f where $\varphi_1 f \varphi_2 = f$. If $f(T_1) = a_i$ where $a_i \in \sigma$ a cycle of φ_1 and $f(T_2) = \gamma$, then $\varphi_1(\gamma) = a_i$ so that $\gamma = a_{i-1}$. Similarly $f(T_3) = a_{i-2}, \dots, f(T_j) = a_1$. Hence we must define f so that the sets $T_1, \dots, T_j$ get mapped by f to a cycle of φ_1 of length j. For each of the $m(j)$ cycles of φ_1 of length j there are j choices

for $f(T_1)$. For each distinct j there are

$$j^{c(j)}\big[m(j)\big(m(j)-1\big)\dots\big(m(j)-\big(c(j)-1\big)\big)\big]$$

ways to define f on the $c(j)$ cyclic parts of length j from which (2.21) follows.

We note that if π is a partition arising from Theorem 2.12 then the cyclic parts of π are each of length $j=(k_{i1}+\dots+k_{ih})/(l_{i1}+\dots+l_{ih})$ for some h. Theorems 2.6, 2.12 and 2.14 can then be applied to determine the total number of functions f with the property that $\varphi_1 f\varphi_2 = f$.

3. Cyclic groups. In this section we apply the results of Section 2 in the case where Ω_1 and Ω_2 are cyclic groups whose orders are relatively prime. We determine the number of equivalence classes of a given order and in particular the total number of classes.

Let Ω_1 and Ω_2 be cyclic groups of orders m_1 and m_2 where $(m_1, m_2) = 1$ so that $\Omega_1\times\Omega_2$ is a cyclic group of order m_1m_2. For each $t_i|m_i$ $(i=1,2)$ let $H_i(t_i)$ denote the subgroup of Ω_i of order t_i so that $H_1(t_1)\times H_2(t_2)$ is a subgroup of $\Omega_1\times\Omega_2$ of order t_1t_2. Let $W(t_1,t_2)$ denote the number of functions f such that $A(f,\Omega_1,\Omega_2) = H_1(t_1)\times H_2(t_2)$.

If $\Omega_i = \langle\psi_i\rangle$ for $i=1,2$ then $H_i(t_i) = \langle\psi_i^{m_i/t_i}\rangle$. If $\varphi_i\in\Omega_i$ define $M(\varphi_1,\varphi_2)$ to be the number of f such that $\varphi_1 f\varphi_2 = f$. For any pair (φ_1,φ_2), $M(\varphi_1,\varphi_2)$ depends only upon the cycle structure of φ_1,φ_2 and can be determined from Theorems 2.6, 2.12 and 2.14.

THEOREM 3.1. *For each* $t_1t_2|m_1m_2$

$$W(t_1,t_2) = M(\psi_1^{m_1/t_1},\psi_2^{m_2/t_2}) - \sum' W(u_1,u_2) \tag{3.1}$$

where the sum is over all u_1, u_2 *such that* $u_1u_2|m_1m_2$, $t_1t_2|u_1u_2$, *and* $t_1t_2 \neq u_1u_2$.

Proof. $M(\psi_1^{m_1/t_1},\psi_2^{m_2/t_2})$ counts the number of functions f such that $H_1(t_1)\times H_2(t_2) < A(f,\Omega_1,\Omega_2)$. There are $W(u_1,u_2)$ such f for which the containment is proper for each $u_1u_2|m_1m_2$, $t_1t_2|u_1u_2$ and $t_1t_2\neq u_1u_2$.

COROLLARY 3.2. *For each* $t_1t_2|m_1m_2$ *there are* $t_1t_2W(t_1,t_2)/m_1m_2$ *classes of order* m_1m_2/t_1t_2 *and*

$$\lambda(\Omega_1,\Omega_2) = \frac{1}{m_1m_2}\sum_{t_1t_2|m_1m_2} t_1t_2W(t_1,t_2). \tag{3.2}$$

COROLLARY 3.3. *Suppose* $f\in K[x]$, $\pi_f = \{S_i \mid i=1,\dots,t\}$, *and* $f(S_i) = \delta_i$. *Then* $\nu(f,\Omega_1,\Omega_2) = t_1t_2$, *or equivalently* $\mu(f,\Omega_1,\Omega_2) = m_1m_2/t_1t_2$ *if and only if* $H_1(t_1)\times H_2(t_2)$ *is the largest subgroup of* $\Omega_1\times\Omega_2$ *such that if* $(\varphi_1,\varphi_2)\in H_1(t_1)\times H_2(t_2)$, *then* $\pi_f\varphi_2 = \pi_f$ *and* $\varphi_1(\gamma_i) = \delta_i$ $(i=1,\dots,t)$ *where* $f\varphi_2(S_i) = \gamma_i$.

We now extend Definition 3.1 of [7] and [8] to

DEFINITION 3.1. Let $\Omega = \Omega_1\times\Omega_2$ and $\Omega' = \Omega_1'\times\Omega_2'$ where Ω_1, Ω_2, Ω_1' and $\Omega_2' < \Phi$. Suppose that Ω and Ω' decompose $K[x]$ into the weak equivalence classes $A_1,\dots,A_{r_1}$ and $B_1,\dots,B_{r_2}$. Then Ω and Ω' induce *equivalent* weak decompositions of $K[x]$ if $\{|A_i|\}$ is a permutation of $\{|B_i|\}$ where $|A|$ denotes the order of the set A. Otherwise, the decompositions are *inequivalent*.

By Lemma 4.1 of [8] we may define the cycles of a cyclic group to be the cycles of any generator of that group. Hence we may state

THEOREM 3.4. *Suppose* Ω_1, Ω_1' *are cyclic groups of order* m_1 *and* Ω_2, Ω_2' *are cyclic groups of order* m_2 *where* $(m_1,m_2)=1$. *Let* $H_i(t_i)$ *and* $H_i'(t_i)$ *denote the subgroups of* Ω_i *and* Ω_i' *of order* t_i *for* $i=1,2$. *If for each* $t_1t_2|m_1m_2$, $H_1(t_1)$ *and* $H_1'(t_1)$ *have the same number of cycles of the same length and* $H_2(t_2)$ *and* $H_2'(t_2)$ *have the same number of cycles of the same length then* $\Omega_1\times\Omega_2$ *and* $\Omega_1'\times\Omega_2'$ *induce equivalent weak decompositions of* $K[x]$.

We illustrate the above theory in the case $K = \mathrm{GF}(5)$. Suppose that in cyclic notation $\psi_1 = (012)$, $\psi_2 = (01)(23)$, and $\Omega_i = \langle\psi_i\rangle$ for $i=1,2$ so that $|\Omega_1\times\Omega_2| = 6$. For $i=1,2,3$ and 6 let $c(i)$ denote the number of equivalence classes of order i induced by $\Omega_1\times\Omega_2$. If $M(\varphi_1,\varphi_2)$ represents the number of f such that $\varphi_1 f\varphi_2 = f$, then by Theorems 2.6, 2.12, and 2.14 we see that

$$M(\psi_1,\psi_2) = 8, \qquad M(\mathrm{id.},\psi_2) = 125,$$
$$M(\psi_1,\mathrm{id.}) = 32, \qquad M(\mathrm{id.},\mathrm{id.}) = 3125$$

so that by Theorem 3.1

$$W(3,2) = 8, \qquad W(1,2) = 117,$$
$$W(3,1) = 24, \qquad W(1,1) = 2976.$$

Hence by Corollary 3.2

$$c(1) = 8, \qquad c(3) = 39,$$
$$c(2) = 12, \qquad c(6) = 496$$

and thus by (3.2) $\lambda(\Omega_1,\Omega_2) = 555$.

4. Application to similarity. In [3] S. Cavior studied similarity of functions over a finite field. We extend his definition in

DEFINITION 4.1. Let $\Omega < \Phi$ and $f, g\in K[x]$. Then f is *similar* to g relative to Ω if there exists $\varphi\in\Omega$ such that $\varphi^{-1}f\varphi = g$.

Let $\Omega^{-1}f\Omega$ and $\mu'(f,\Omega)$ denote the class of f and the number of elements in the class of f relative to Ω. Let $\lambda'(\Omega)$ denote the number of classes induced by Ω.

DEFINITION 4.2. Let $\Omega < \Phi$ and $f\in K[x]$. If $\varphi\in\Omega$ then φ is a *similar automorphism* of f relative to Ω if $\varphi^{-1}f\varphi = f$.

The set of similar automorphisms of a function f relative to Ω forms a group $S(f, \Omega)$ of order $\nu'(f, \Omega)$. One may easily prove that if $\Omega < \Phi$ and $f \in K[x]$ then

$$\mu'(f, \Omega)\nu'(f, \Omega) = |\Omega|. \tag{4.1}$$

Suppose now Ω is cyclic of order m. For each $t|m$ let $H(t)$ denote the unique subgroup of Ω of order t so that if $\Omega = \langle\psi\rangle$ then $H(t) = \langle\psi^{m/t}\rangle$. Let $S(t)$ denote the number of functions f such that $S(f, \Omega) = H(t)$. If $\varphi \in \Omega$ define $M(\varphi)$ to be the number of f such that $\varphi^{-1}f\varphi = f$. For any permutation φ, $M(\varphi)$ can be determined from Theorems 2.6, 2.12 and 2.14.

Proceeding as in Section 3 we may prove

THEOREM 4.1. *For each $t|m$*

$$S(t) = M(\psi^{m/t}) - \sum S(u) \tag{4.2}$$

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

COROLLARY 4.2. *For each $t|m$ there are $tS(t)/m$ classes of order m/t and*

$$\lambda'(\Omega) = \frac{1}{m}\sum_{t|m} tS(t). \tag{4.3}$$

COROLLARY 4.3. *Suppose Ω_1 and Ω_2 are cyclic groups of order m. Let $H_i(t)$ $(i = 1, 2)$ denote the subgroups of Ω_1 and Ω_2 of order t where $t|m$. If for each $t|m$, $H_1(t)$ and $H_2(t)$ have the same number of cycles of the same length then Ω_1 and Ω_2 induce equivalent similar decompositions of $K[x]$.*

We illustrate the theory of similarity with the following example where $K = \mathrm{GF}(5)$. Suppose that in cyclic notation $\psi = (0123)$ and $\Omega = \langle\psi\rangle$. For $i = 1, 2$ and 4 let $c'(i)$ denote the number of equivalence classes of order i induced by Ω. If $M(\varphi)$ represents the number of f such that $\varphi^{-1}f\varphi = f$ then by Theorems 2.6, 2.12 and 2.14 we see that $M(\psi) = 5$, $M(\psi^2) = 25$ and $M(\mathrm{id.}) = 3125$ so that by Theorem 4.1 $S(4) = 5$, $S(2) = 20$ and $S(1) = 3100$. Hence by Corollary 4.2, $c'(1) = 5$, $c'(2) = 10$ and $c'(4) = 775$ so that by (4.3) $\lambda'(\Omega) = 790$.

5. Permutation polynomials. In this section we present several applications of weak equivalence to permutation polynomials over a finite field. A general theory of permutation polynomials has already been discussed in the literature, see for example [5], [9], [10], [11], [12] and their references. If $f \in K[x]$ is a permutation polynomial and g is weakly equivalent to f then g is also a permutation polynomial so that the class $\Omega_1 f \Omega_2$ consists entirely of permutation polynomials.

THEOREM 5.1. *If $f \in K[x]$ then f is a permutation polynomial if and only if f is weakly equivalent to x relative to the groups Φ and Φ.*

Proof. The sufficiency is clear. For necessity suppose f is a permutation polynomial and $f(a_i) = a_{j_i}$ where $K = \{a_1, \ldots, a_q\}$. Define φ_2 by $\varphi_2(a_{j_i}) = a_i$ and $\varphi_1(a_i) = a_i$ for $i = 1, \ldots, q$. Then $\varphi_1 f \varphi_2(a_{j_i}) = a_{j_i}$ so that $\varphi_1 f \varphi_2 = x$.

Thus the group of permutation polynomials comprises exactly one class relative to the groups Φ and Φ.

THEOREM 5.2. *Let $f \in K[x]$ be a permutation polynomial. Suppose $\Omega_1, \Omega_2 < \Phi$ where $(|\Omega_1|, |\Omega_2|) = 1$. Then $\mu(f, \Omega_1, \Omega_2) = |\Omega_1||\Omega_2|$.*

Proof. Using (2.1) we have

$$\Omega_1 f \Omega_2 = \Omega_1 f_1 \cup \ldots \cup \Omega_1 f_n \tag{5.1}$$

where $f\Omega_2 = \{f = f_1, f_2, \ldots, f_n\}$ is the right equivalence class of f relative to Ω_2 and $\Omega_1 f_i$ is the left equivalence class of f_i relative to Ω_1. Since f is a permutation polynomial, by Corollary 9 of [9] the number of elements in $\Omega_1 f_i$ is $|\Omega_1|$ for $i = 1, \ldots, n$. Thus $|\Omega_1|k = \mu(f, \Omega_1, \Omega_2)$ where k denotes the number of distinct left equivalence classes in the decomposition of $\Omega_1 f \Omega_2$ from (5.1). Hence $|\Omega_1| | \mu(f, \Omega_1, \Omega_2)$. Similarly $|\Omega_2| | \mu(f, \Omega_1, \Omega_2)$ from which the theorem follows.

COROLLARY 5.3. *Let $\Omega_1, \Omega_2 < \Phi$ where $(|\Omega_1|, |\Omega_2|) = 1$. Then the group of permutation polynomials on K is weakly decomposed by $\Omega_1 \times \Omega_2$ into $[\Phi \times \Phi\colon \Omega_1 \times \Omega_2]$ weak equivalence classes each containing $|\Omega_1||\Omega_2|$ elements.*

COROLLARY 5.4. *Let $\Omega_1, \Omega_2, \Omega_1', \Omega_2' < \Phi$ where $(|\Omega_1|, |\Omega_2|) = (|\Omega_1'|, |\Omega_2'|) = 1$. If $|\Omega_1 \times \Omega_2| = |\Omega_1' \times \Omega_2'|$ then $\Omega_1 \times \Omega_2$ and $\Omega_1' \times \Omega_2'$ decompose the group of permutation polynomials on K into the same number of weak equivalence classes of the same size.*

We note that the results of this section correspond to the results of Sections 3 and 4 of [9].

References

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

[2] — *Invariant theory of systems of equations in a finite field*, J. Analyse Math. 3(1953/54), pp. 382–413.

[3] S. R. Cavior, *Equivalence classes of functions over a finite field*, Acta Arith. 10 (1964), pp. 119–136.

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

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

[6] M. Eisen, *Elementary combinatorial analysis*, Gordon and Breach, New York 1969.

[7] G. L. Mullen, *Equivalence classes of functions over a finite field*, Acta Arith. 29 (1976), pp. 353–358.
[8] — *Equivalence classes of polynomials over finite fields*, ibid. 31 (1976), pp. 113–123.
[9] — *Permutation polynomials in several variables over finite fields*, ibid. 31 (1976), pp. 107–111.
[10] H. Niederreiter, *Permutation polynomials in several variables over finite fields*, Proc. Japan Acad. 46 (1970), pp. 1001–1005.
[11] — *Permutation polynomials in several variables*, Acta Sci. Math. (Szeged), 33 (1972), pp. 53–58.
[12] W. Nöbauer, *Zur theorie der polynomtransformationen und permutationspolynome*, Math. Ann. 157 (1964), pp. 332–342.

Received on 24. 8. 1976 (871)

ACTA ARITHMETICA
XXXV (1979)

On normal radical extensions of real fields

by

DAVID GAY* (Geneva)

In 1926 Darbi [1] and Bessel-Hagen (see [8], p. 302) found all normal binomials $x^m - a$ over the rationals Q. Here is their list:

L_1: $x^2 - c$ $(c \neq c_1^2)$; $x^4 + c^2$ $(c \neq 2c_1^2)$; $x^{2^k} + c^{2^{k-1}}$ $(k \geqslant 3)$; $x^{2^k} + 2^{2^{k-2}} c^{2^{k-1}}$ $(k \geqslant 4)$; $x^6 + 3c^2$ $(c \neq 3c_1^3)$; $x^{12} + 36c^4$ $(c \neq 6c_1^3)$

(In all cases above, it is understood that $c, c_1 \in Q$.) In 1975 Mann and Vélez [5] considered the problem of determining all binomials $x^m - a$ over Q with the property that $Q(\alpha)$ is the splitting field for all roots α of $x^m - a$. We call such binomials *weakly normal*. They obtained a complete list of weakly normal binomials over Q which, of course, includes the irreducible binomials above as well as the following reducible ones:

L_2: $x^2 - c^2$; $x^4 + 4c^4$; $x^6 + 27c^6$; $x^{12} + (36c^4)^3$.

More recently, Norris and Vélez [6] have shown that the normal binomials over a field K play a central rôle in the general structure theory of all radical extensions of K.

The purpose of this paper is to determine all weakly normal (including normal) binomials over an arbitrary real field. Our main results are contained in Section 4 (in particular, Theorems 4.1 and 4.4) where we obtain binomials as explicit as those on the lists above. In Section 1 we present some general results about weakly normal binomials forming a point of departure for our study. Section 2 is devoted to finding explicit (and convenient for our purposes) generators for, and Galois groups of, certain cyclotomic fields. In Section 3, we use these technical results to obtain a precise framework for weakly normal binomials enabling us to complete

* The author was jointly supported by Fonds National Suisse de la Recherche Scientifique and Battelle Institute Grant No. 333-205.