ACTA ARITHMETICA
LXXXII.3 (1997)

Polynomials with nontrivial relations between their roots

by

John D. Dixon (Ottawa, Ont.)

1. Introduction. Consider an irreducible polynomial $f(X)$ over a field K. We are interested in situations where some distinct roots $\alpha_1, \ldots, \alpha_k$ of $f(X)$ satisfy a multiplicative relation of the form $\alpha_1^{m_1} \ldots \alpha_k^{m_k} = c$ where $m_1, \ldots, m_k$ are nonzero integers and $c \in K$. In Section 4 we also look at additive relations. As we might expect, such relations imply special conditions on the Galois group of the polynomial and sometimes on the form of $f(X)$ itself.

The problem of when relations like these hold arises naturally in the study of polynomials; see, for example, the papers [5]–[6] of Smyth, [4] of Ferguson and [3] of Drmota and Ska/lba. The object of the present paper is to show how representation theory of finite groups can be used to solve some of these questions.

Throughout this paper K will denote a subfield of $\mathbb{C}$ (although some of the results can be extended to other fields). If Ω is the set of roots in $\mathbb{C}$ of a polynomial $f(X) \in K[X]$, then $G := \mathrm{Gal}(K(\Omega)/K)$ denotes the Galois group of the splitting field of $f(X)$ over K. The group G acts on the set Ω and is transitive on Ω if and only if $f(X)$ is irreducible. Moreover, G acts primitively on Ω if and only if the stabilizer G_α of a root $\alpha \in \Omega$ is a maximal subgroup; by elementary Galois theory the latter is equivalent to the condition that there is no field lying properly between K and $K(\alpha)$.

We shall be studying connections between the Galois group G and its action on Ω and the existence of relations between the roots of $f(X)$. Lemma 1 of [6] shows that the existence of a nontrivial relation between the roots implies that G does not act as the symmetric group on Ω (see Theorem 1 below for a significant generalization). Since "almost all" polynomials over $\mathbb{Q}$ have the full symmetric group as their Galois group, this proves the unsurprising fact that polynomials with nontrivial relations between their roots are quite special and are restricted in their possible Galois groups. On the other hand,

1991 *Mathematics Subject Classification*: 12E10, 12F12.

simple examples show that knowledge of the Galois group by itself does not permit us to deduce the existence of a nontrivial relation.

In Section 2 we introduce the relation modules corresponding to multiplicative relations between roots of $f(X)$ and derive some of the consequences of the existence of nontrivial relations in terms of the permutation action of G on Ω. Such relation modules have been studied in rather different forms by other authors in the papers [3]–[6]. In Section 3 we show how the linear action of G can also be used, and use it to generalize the main theorem of [3]. Finally, in Section 4 we discuss some of the analogous results for additive relations.

2. Module of relations. Let $f(X) \in K[X]$ be an irreducible polynomial of degree $n > 1$ where K is a subfield of $\mathbb{C}$, let $\Omega \subseteq \mathbb{C}$ be the set of roots of $f(X)$ and put $G := \mathrm{Gal}(K(\Omega)/K)$. For any commutative ring L with unity, L^Ω will denote the L-module consisting of all n-tuples of elements of L indexed by the elements of Ω. For each $\alpha \in \Omega$, $e_\alpha \in L^\Omega$ denotes the αth standard basis element, namely, an n-tuple with 1 in the αth position and 0's elsewhere. Then G has a natural L-linear action on L^Ω defined by $e_\alpha x := e_\beta$ when $x \in G$ maps α onto β. This defines L^Ω as an LG-module. We put $e := \sum e_\alpha$, and note that eLG is an LG-submodule of L^Ω.

First consider the special case where $L = \mathbb{Z}$ and put $M := \mathbb{Z}^\Omega$. Then we can define two submodules modules R and R_1 as follows. An element $\sum m_\alpha e_\alpha$ from M (with the $m_\alpha \in \mathbb{Z}$) lies in R if and only if $\prod \alpha^{m_\alpha} \in K$; and it lies in R_1 if and only if $\prod \alpha^{m_\alpha} = 1$. Note that $e \in R$; the relations $(\prod \alpha)^m \in K$ corresponding to me will be called *trivial relations*.

Next consider the case where L is a subfield of $\mathbb{R}$. We use the standard notation $S^\perp$ to denote the orthogonal complement in L^Ω of a subset $S \subseteq L^\Omega$ with respect to the usual dot product $u \cdot v$. Recall that $S^\perp$ is always an L-subspace of L^Ω, and that $L^\Omega = S \oplus S^\perp$ whenever S is an L-subspace. Furthermore, if S is mapped into itself by all elements of G, then $S^\perp$ is clearly an LG-submodule. In particular, $L^\Omega = eLG \oplus (L^\Omega)_0$ as a direct sum of LG-submodules where $(L^\Omega)_0 := (eLG)^\perp$ consists of the elements in L^Ω whose components sum to 0. A simple calculation shows that $(L^\Omega)_0$ is spanned by the vectors $e_\alpha - e_\beta$ $(\alpha, \beta \in \Omega)$.

In the special case where $L = \mathbb{Q}$ we have $V := \mathbb{Q}^\Omega = \mathbb{Q} \otimes_\mathbb{Z} M$ with $W := \mathbb{Q} \otimes R$ and $W_1 := \mathbb{Q} \otimes R_1$ as $\mathbb{Q}G$-submodules of V. Note that, if $v := \sum m_\alpha e_\alpha \in M$, then $v \in W$ (respectively, $v \in W_1$) if and only if, for some integer $d \geq 1$, the dth power of $\prod \alpha^{m_\alpha}$ lies in K (resp. equals 1). Using the notation above, the subspace V_0 is equal to $(e\mathbb{Q}G)^\perp$.

Lemma 1. *With the notation above*:

(i) $W \cap V_0 = W_1 \cap V_0$;

(ii) $W = e\mathbb{Q}G + W_1$ *and so* $W = W_1$ *if and only if* $\prod \alpha$ *is a root of unity*;

(iii) $W = V$ *if and only if*, *for some integer* m *and some* $c \in K$, $f(X)$ *divides* $X^m - c$.

Proof. (i) Suppose that $v := \sum m_\alpha e_\alpha \in W \cap V_0 \cap M$. Then $\sum m_\alpha = 0$ and the dth power of $c := \prod \alpha^{m_\alpha}$ lies in K for some $d \geq 1$. Now take the dth power of both sides of this last equation. Then applying $x \in G$ to both sides of the new equation and forming the product over G we get $c^{d|G|} = 1$ (using transitivity of G and the condition $\sum m_\alpha = 0$). Hence $v \in W_1$. Since $W \cap V_0 = \mathbb{Q} \otimes (W \cap V_0 \cap M)$, this shows that $W \cap V_0 \subseteq W_1 \cap V_0$. The reverse inequality is trivial so (i) is proved.

(ii) Since $e \in W$ and $V = e\mathbb{Q}G \oplus V_0$, therefore $W = e\mathbb{Q}G + W_1$ by (i). Hence $W = W_1$ if and only if $e \in W_1$. As we saw above this is equivalent to the condition that $\prod \alpha$ is a root of unity.

(iii) Suppose that $f(X)$ divides $X^m - c$. Then $\alpha^m = c$ for all $\alpha \in \Omega$, and so $\alpha^m \beta^{-m} = 1$ for all $\alpha, \beta \in \Omega$. Hence all the vectors of the form $e_\alpha - e_\beta$ lie in W_1. As noted above, these vectors span V_0, and so $W \supseteq e\mathbb{Q}G + V_0 = V$ by (ii). Conversely, if $W = V$ and $\alpha \in \Omega$, then $e_\alpha \in W$ and so there exists an integer m and $c \in K$ such that $\alpha^m - c = 0$. Since $f(X)$ is irreducible, this implies that $f(X)$ divides $X^m - c$. ∎

The following result is a classical (and easily proved) result from Galois theory (see, for example, [8], Sect. 55).

Lemma 2. *Consider a* (*not necessarily irreducible*) *polynomial of the form* $h(X) := X^m - c \in K[X]$. *Let* α *be a root of* $h(X)$ *and* ω *be a primitive* m*th root of* 1. *Then the splitting field for* $h(X)$ *over* K *is* $E := K(\alpha, \omega)$, *and the Galois group* $H := \mathrm{Gal}(E/K)$ *has a cyclic normal subgroup* $N := \mathrm{Gal}(E/K(\omega))$ *of order dividing* m *with a factor group* $H/N \cong \mathrm{Gal}(K(\omega)/K)$ *which is abelian. In particular*, *the derived subgroup* $H' \leq N$, *and so* H' *is also cyclic.* ∎

Lemma 3. *Consider* $\alpha, \beta \in \Omega$ *with* $\alpha \neq \beta$. *Then the following are equivalent*:

(i) $e_\alpha - e_\beta \in W$;

(ii) $e_\alpha - e_\beta \in W_1$;

(iii) α/β *is an* m*th root of* 1 *for some integer* $m \geq 1$.

Moreover, *condition* (iii) *holds for some pair of roots* $\alpha \neq \beta$ *if and only if* $f(X) \mid g(X^m)$ *for some monic irreducible* $g(X) \in K[X]$ *of degree smaller than* n. *In the latter case*, $g(X)$ *is unique and its degree divides* n.

Proof. (ii) and (iii) are equivalent by the observations made when we defined W_1, and (ii) is equivalent to (i) because $W_1 \cap V_0 = W \cap V_0$ by

Lemma 1. It remains to prove the assertions in the final paragraph. Fix some root α of $f(X)$, and let $g(X)$ be the minimal polynomial for α^m over K. Since $f(X)$ is irreducible, and α is a root of $g(X^m)$, therefore $f(X) \mid g(X^m)$. There is only one monic irreducible polynomial $g(X)$ satisfying the condition $f(X) \mid g(X^m)$ since the latter implies that $g(X)$ has α^m as a root. Now consider the equivalence relation $\sim$ on Ω defined by: $\gamma \sim \delta$ if and only if $\gamma^m = \delta^m$. The $\sim$-equivalence classes clearly form a set of blocks of imprimitivity for G, and so the degree d of $g(X)$ (which equals the number of classes) must divide $|\Omega| = n$. Moreover, $d < n$ if and only if each class has size at least 2, and the latter is equivalent to (iii) for some α, β. ∎

R e m a r k. A classical theorem of Capelli (see, for example, [7], p. 288) states that a composite $g(h(X))$ of polynomials $g(X), h(X) \in K[X]$ is irreducible over K if and only if: (a) $g(X)$ is irreducible over K; and (b) $h(X)-\gamma$ is irreducible over $K(\gamma)$ for each root γ of $g(X)$. Hence in Lemma 3 we have: $f(X) = g(X^m) \Rightarrow g(X^m)$ is irreducible over $K \Rightarrow X^m - \gamma$ is irreducible over $K(\gamma)$ for each root γ of $g(X)$. Thus the cases where $f(X) \neq g(X^m)$ occur precisely when there exists $\theta \in \mathbb{C}$ such that $g(X)$ is the minimal polynomial for θ^m over K but the degree of θ over $K(\theta^m)$ is not m. For example, take $K = \mathbb{Q}$ and $\theta = 1+\sqrt{2}$, so $\theta^3 = 7+5\sqrt{2}$. The minimal polynomials for θ and θ^3 over $\mathbb{Q}$ are $h(X) = X^2 - 2X - 1$ and $g(X) = X^2 - 14X - 1$, respectively, and $g(X^3) = h(X)f(X)$ where $f(X) = X^4 + 2X^3 + 5X^2 - 2X + 1$. The polynomial $f(X)$ is irreducible and has two pairs of complex conjugate roots whose ratios are cube roots of 1. Its Galois group is the Klein 4-group. Incidentally the ratio of the two roots of $h(X)$ is not a root of 1 (and of course $\deg g(X)$ is not less than $\deg h(X)$).

Theorem 1. *Suppose that $f(X) \in K[X]$ is monic irreducible and that the Galois group G of $f(X)$ acts primitively on the set Ω of roots of $f(X)$.*

(i) *Suppose that some pair of distinct roots of $f(X)$ has a ratio which is an mth root of unity. Then the ratio of every pair of roots is an mth root of unity, $f(X) \mid X^m - c$ for some $c \in K$, the degree of $f(X)$ is a prime, and G is solvable.*

(ii) *If G acts 2-transitively on Ω and there is any nontrivial multiplicative relation between the roots of $f(X)$ then, for some prime p, $f(X)$ has degree p and G is isomorphic to the affine group of order $p(p-1)$. Moreover, if $K \subseteq \mathbb{R}$ and $\deg f(X) > 2$, then $f(X)$ has the form $X^p - b$ for some $b \in K$.*

P r o o f. (i) Since G acts primitively on Ω, it follows from the last paragraph of the proof of Lemma 3 that all the mth powers γ^m ($\gamma \in \Omega$) are equal and so the polynomial $g(X)$ defined there has degree 1. Hence the lemma shows that $f(X) \mid X^m - c$ for some $c \in K$. Since the Galois group G of $f(X)$ is a factor group of the Galois group of the splitting field of $X^m - c$ over K,

Lemma 2 now shows that G is solvable and its derived group G' is cyclic. On the other hand, a solvable primitive permutation group always has prime power degree, say p^k for some prime p, and has a unique minimal normal subgroup which is elementary abelian of order p^k (see [2], Theorem 4.3B). Since G acts primitively (and faithfully) as a permutation group of degree $|\Omega|$ and G' is cyclic, this shows that $|\Omega| = p^k$ with either $k = 1$ or $G' = 1$. In the latter case G is a primitive abelian group, which again only occurs when its degree is prime. Thus in either case we conclude that G is solvable and that $\deg f(X) = |\Omega|$ is equal to a prime p.

(ii) Because G is 2-transitive, the $\mathbb{Q}G$-module V_0 defined above is irreducible; indeed, it is absolutely irreducible (see [1], Sect. 32B). Since there is a nontrivial relation between the roots of $f(X)$, W properly contains $e\mathbb{Q}G$, and so $W = V$ by irreducibility. Thus $e_\alpha - e_\beta \in W$ for all $\alpha, \beta \in \Omega$. Since any 2-transitive group is primitive, (i) and Lemma 3 now show that $|\Omega| = p$ for some prime p and G acts faithfully as a solvable 2-transitive group on Ω. Hence G is isomorphic to the affine group of order $p(p-1)$ (see [2], Sect. 3.5).

Finally, if $K \subseteq \mathbb{R}$ and $\deg f(x) > 2$, then p is odd and $f(X)$ has a real root α. The other roots of $f(X)$ differ from α by a factor which is a root of unity, so all roots of $f(X)$ have the same absolute value. There are p roots, $f(X)$ is monic and K is real; therefore $b := \alpha^p = \pm f(0) \in K$. Thus $f(X) \mid X^p - b$ by the irreducibility of $f(X)$. Since $f(X)$ is monic of degree p we conclude $f(X) = X^p - b$ as claimed. ∎

Remark. The condition that $\deg f(X) > 2$ in the last assertion of Theorem 1 cannot be dropped. There are polynomials of degree 2 not of the form $X^2 - c$ whose roots have a ratio which is a root of unity. Indeed, suppose that $f(X)$ has degree 2 and has roots α and $\alpha\omega$ where ω is a primitive mth root of 1 for some $m \geq 2$. When $m = 2$, $f(X)$ has the form $X^2 - c$, but suppose that $m > 2$. Then $f(X) = X^2 + aX + b$ for some $a, b \in K$ with $a \neq 0$ such that $a^2/b = \omega^{-1} + 2 + \omega$ is an algebraic integer lying in K. In the special case where $K = \mathbb{Q}$, this shows that $k := a^2/b$ must be one of the integers 1, 2 or 3, corresponding respectively to the cases where ω is a primitive mth root of unity for $m = 3$, 4 or 6. Conversely, for these values of k, the ratio of the two roots of $f(X) = X^2 + aX + a^2/k$ is an mth root of 1. In general, when K is an arbitrary field, the quadratics which can arise depend on which roots of unity have degree at most 2 over K.

Theorem 2. *Suppose that an irreducible polynomial $f(X) \in \mathbb{Z}[X]$ has degree n which is not prime and that the Galois group G of $f(X)$ acts primitively on the set Ω of roots of $f(X)$. If the roots of $f(X)$ satisfy a nontrivial relation, then $f(X)$ is reducible modulo p for each prime p not dividing the leading coefficient of $f(X)$.*

P r o o f. Since n is not prime, Theorem 1 shows that the Galois group G of $f(X)$ over $\mathbb{Q}$ is not 2-transitive on Ω. On the other hand, G is primitive on Ω by hypothesis. Now a classical theorem of Schur (see [9], Theorem 25.4, or [2], Sect. 3.5) shows that a permutation group of degree n which contains an n-cycle is either 2-transitive or imprimitive. Hence G cannot contain an n-cycle in its action on Ω, and so by a theorem of Frobenius (see [8], Sect. 61), $f(X)$ is reducible modulo p for all primes p not dividing the leading coefficient of $f(X)$. ∎

LEMMA 4. *Suppose that L is a subfield of $\mathbb{R}$ and that U is an LG-submodule of L^Ω. If none of the vectors $e_{\alpha\beta} := e_\alpha - e_\beta$ ($\alpha, \beta \in \Omega$ with $\alpha \neq \beta$) lies in U, then $U^\perp$ contains a vector whose entries are all distinct.*

P r o o f. For all $\alpha, \beta \in \Omega$ with $\alpha \neq \beta$ we define $U_{\alpha\beta} := (e_{\alpha\beta}LG + U)^\perp = e_{\alpha\beta}^\perp \cap U^\perp$. Then $U_{\alpha\beta}$ is the set of all vectors in $U^\perp$ whose αth and βth components are equal, and $U_{\alpha\beta}$ is a proper L-subspace of $U^\perp$ because $e_{\alpha\beta} \notin U$. Since a vector space over an infinite field cannot be written as a union of a finite number of proper subspaces, there exists $w \in U^\perp$ such that w is not contained in any $U_{\alpha\beta}$ and such a vector has distinct components. ∎

This gives a short alternative proof of a theorem given in [4] and [6].

THEOREM 3. *Let $f(X) \in K[X]$ be irreducible, and let $\alpha_1, \ldots, \alpha_r$ be distinct roots of $f(X)$ with $r \geq 3$. If there is a nontrivial relation $\prod_{i=1}^r \alpha_i^{m_i} \in K$ for some nonzero integers m_i with $m_j \geq \sum_{i \neq j} |m_i|$ for some j, then the ratio of some pair of distinct roots of $f(X)$ is a root of unity.*

P r o o f. Suppose that no pair of distinct roots has a ratio which is a root of unity. Then Lemma 3 shows that none of the vectors $e_\alpha - e_\beta$ ($\alpha, \beta \in \Omega$ with $\alpha \neq \beta$) lies in W, and so Lemma 4 shows that $W^\perp$ contains a vector v all of whose components are distinct. Since $W^\perp$ is G-invariant, and G acts transitively on Ω, we may choose $x \in G$ so that the component of vx with largest absolute value is the (α_j)th component (there may be two such components, in which case choose one). On the other hand, the hypothesis shows that $u := \sum_{i=1}^r m_i e_{\alpha_i} \in W$ so $u \cdot (vx) = 0$. Since $r \geq 3$, the inequality on the m_i now gives an immediate contradiction. ∎

R e m a r k. A similar proof goes through when $r = 2$ except when $m_1 = m_2$. In the latter case there are genuine exceptions to the theorem; for example, the two roots of the polynomial $X^2 - 3X + 1$ have product 1 but their ratio is not a root of 1.

3. Linear representations of the Galois group. We continue the notation of the previous section, but now we consider in more detail the linear representation of G on the vector space L^Ω where L is a subfield of $\mathbb{C}$.

Fix $\delta \in \Omega$ and note that $\mathrm{Gal}(K(\Omega)/K(\delta))$ is equal to the point stabilizer G_δ of δ in the action of G on Ω.

LEMMA 5 ($L = \mathbb{Q}$). *Suppose that the roots of $f(X)$ are not roots of unity. Consider the action of an element c in the group ring $\mathbb{Q}G$ on $V := \mathbb{Q}^\Omega$. If $(e_\delta)c \in W$ (as defined in Section 2), then c is not invertible as a $\mathbb{Q}$-linear transformation on V/W. Consequently, $\varrho(c)$ is singular for some irreducible matrix representation ϱ of G over $\mathbb{C}$. Moreover, ϱ may be chosen as an irreducible constituent of the representation of G obtained by inducing from the trivial representation of G_δ.*

P r o o f. Since δ is not a root of unity, $e_\delta \notin W$. Thus $W + e_\delta$ is a nonzero vector in V/W and the hypothesis shows that it lies in the null space of c. Hence $\varrho(c)$ must be singular for one of the irreducible constituents of a matrix representation of G afforded by V/W. The final assertion of the lemma follows from the fact that the permutation module V can be obtained by induction from the trivial representation of the point stabilizer G_δ. ∎

As a simple application of Lemma 5 we have the following result.

THEOREM 4. *Let $f(X) \in K[X]$ be an irreducible polynomial whose set Ω of roots does not consist of roots of unity. Suppose that the Galois group G can be written $G = G_\delta C$ for some $\delta \in \Omega$ where $C := \langle x \rangle$ is a cyclic subgroup of order $n := |\Omega|$. Then we can enumerate the elements of Ω so that δ_i is the image of δ under x^i $(i = 0, 1, \ldots, n-1)$. If $\prod_{i=0}^{n-1} \delta_i^{m_i} \in K$ is a relation on Ω, then the polynomial $\sum_{i=0}^{n-1} m_i X^i$ must vanish at some nth root of 1.*

P r o o f. The hypothesis shows that $e_\delta(\sum m_i x^i) = \sum m_i e_{\delta_i} \in W$. Then Lemma 5 shows that $\varrho(\sum m_i x^i) = \sum m_i \varrho(x)^i$ is singular for some irreducible matrix representation ϱ of G. Since x has order n, $\varrho(x)$ is similar to a diagonal matrix whose nonzero entries are nth roots of 1. Thus the singularity condition shows that $\sum m_i \zeta^i = 0$ for some ζ where ζ is an nth root of 1. ∎

A similar but more complicated argument enables us to prove a generalization of the main theorem of Drmota and Ska/lba in [3]. (The methods in [3] do not seem to generalize easily from the case where the Galois group G is an abelian group and $K = \mathbb{Q}$.)

THEOREM 5. *Let $f(X) \in K[X]$ be an irreducible polynomial whose set Ω of roots does not consist of roots of unity. Suppose that the Galois group G of $f(X)$ can be written in the form $G = G_\delta M$ for some $\delta \in \Omega$ where M is either abelian or contains a normal abelian subgroup of index 2. If there are distinct $\alpha, \beta, \gamma \in \Omega$ such that $\alpha\beta\gamma^{-1} \in K$, then $|M|$ is divisible by either 6 or 10; moreover, when M is abelian, $|M|$ is divisible by 6.*

P r o o f. Since G is transitive on Ω and $G = G_\delta M$, therefore M is also transitive. Define F to be the subfield of $K(\Omega)$ which is fixed by M. Then $f(X)$ is still irreducible over F by the transitivity of $M = \mathrm{Gal}(K(\Omega)/F)$. Thus without loss in generality we can replace K by F and G by M, and so (by a change in notation) assume that G itself is abelian or has an abelian normal subgroup of index 2. Put $g := |G|$. We have to show that either 6 or 10 divides g, and that 6 divides g when G is abelian.

Because G acts transitively on Ω there is no loss in generality in assuming that $\gamma = \delta$. Then $\alpha\beta\delta^{-1} \in K$ implies that for some $x, y \in G$ we have $e_\delta(1 - x - y) \in W$. Lemma 5 now shows that for some irreducible representation ϱ of G, $\varrho(1-x-y)$ is singular. If G is abelian, then every irreducible representation has degree 1. On the other hand, if G has a normal abelian subgroup A of index 2, then a simple application of the Frobenius reciprocity theorem shows that each representation of G of degree > 1 can be induced from an irreducible representation (of degree 1) of A and so is a monomial representation of degree 2 (see [1], Sect. 38, Ex. 8). We consider the two cases for ϱ.

If ϱ has degree 1, then the condition that $\varrho(1 - x - y)$ is singular implies that $1 - \xi - \eta = 0$ where ξ and η are gth roots of 1. This in turn implies that 0, 1 and ξ are vertices of an equilateral triangle in the complex plane and so $\xi = \pm\exp(2\pi i/6)$. Hence $6 \,|\, g$. In particular, 6 always divides g in the abelian case.

If ϱ is monomial of degree 2 then $\varrho(x)$ and $\varrho(y)$ can each be written in one of the forms $\left[\begin{smallmatrix} \mu & 0 \\ 0 & \nu \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} 0 & \mu \\ \nu & 0 \end{smallmatrix}\right]$ where μ and ν are $(g/2)$th roots of 1 since $g/2 = |A|$. If both $\varrho(x)$ and $\varrho(y)$ are diagonal then the result follows at once from the case of degree 1 proved above, so suppose that at least one is not diagonal. In the latter case the condition $\det \varrho(1 - x - y) = 0$ reduces either to a condition of the form $(1 - \xi_1)(1 - \xi_2) = \eta_1\eta_2$ or to one of the form $1 = (\xi_1 + \eta_1)(\xi_2 + \eta_2)$ where $\xi_1, \xi_2, \eta_1, \eta_2$ are $(g/2)$th roots of 1. In the first of these cases we replace ξ_i by ζ_i $(i = 1, 2)$ and $\eta_1\eta_2$ by θ; and in the second case we replace $-\xi_i\eta_i^{-1}$ by ζ_i $(i = 1, 2)$ and $(\eta_1\eta_2)^{-1}$ by θ. Then in either case we obtain a relation $(1 - \zeta_1)(1 - \zeta_2) = \theta$ where ζ_1, ζ_2 and θ are all gth roots of 1. If ζ_1 is a primitive dth root of 1 (where $d \,|\, g$), then a suitable field automorphism applied to the last relation gives a relation of the form $(1 - \zeta_1')(1 - \zeta_2') = \theta'$ where $\zeta_1' = \exp(2\pi i/d)$, $\zeta_2' = \exp(2\pi ri/s)$ for some integers r and s, and d and s divide g. This implies that $4\sin(\pi/d)\sin(\pi r/s) = |(1-\zeta_1')(1-\zeta_2')| = 1$; in particular, $4\sin(\pi/d) \geq 1$ and so $d \leq 12$. A similar argument (with a different field automorphism) shows that $s \leq 12$. Finally, examination of the 12 possible cases for d shows that only the following cases can actually arise: $(1/d, r/s) = (1/12, 5/12)$, $(1/10, 3/10)$ and $(1/6, 1/6)$. Thus in all cases g is divisible by either 6 or 10 and the proof of the theorem is complete. ∎

4. Additive relations. Many of the results obtained in Sections 2 and 3 for multiplicative relations can be proved also for additive relations. As before, let K be an arbitrary subfield of $\mathbb{C}$, Ω be the set of roots of an irreducible polynomial $f(X) \in K[X]$ and G be the Galois group of $f(X)$ over K. We define U and U_1 to be the KG-submodules of K^Ω consisting of all $\sum c_\alpha e_\alpha$ in K^Ω such that $\sum c_\alpha \alpha \in K$ (or $\sum c_\alpha \alpha = 0$, respectively). Clearly U and U_1 cannot contain any e_γ when $\deg f(X) \geq 2$. Nor can they contain $e_\gamma - e_\delta$ for any $\gamma \neq \delta$. Indeed, otherwise $c := \gamma - \delta$ is a nonzero element of K; this implies that $f(X+c) = f(X)$ and then $f(0) = f(c) = f(2c) = \dots$ leads to a contradiction. On the other hand, we always have $e \in U$ corresponding to the trivial relation $\sum \alpha \in K$; we say that the roots of $f(X)$ satisfy *nontrivial K-linear relations* if $U \neq eKG$.

We have the following additive analogues of our theorems for multiplicative relations. The proofs are very similar and are omitted.

THEOREM 1′. *Suppose that $f(X) \in K[X]$ is irreducible and its Galois group acts 2-transitively on the set of roots. Then the roots of $f(X)$ cannot satisfy a nontrivial K-linear relation.* ∎

The exact analogue of Theorem 2 holds for $\mathbb{Q}$-linear relations. In the analogue of Theorem 3 we must restrict K to being real in order to apply Lemma 4 (see [5] and [6] for similar results).

THEOREM 3′. *Suppose that $K \subseteq \mathbb{R}$. Let $f(X) \in K[X]$ be irreducible, and let $\alpha_1, \dots, \alpha_r$ be distinct roots of $f(X)$ with $r \geq 3$. Then there is no nontrivial K-linear relation $\sum_{i=1}^r c_i \alpha_i \in K$ with all c_i nonzero in which $c_j \geq \sum_{i \neq j} |c_i|$ for some j.* ∎

COROLLARY. *Suppose that $f(X) \in K[X]$ is irreducible and $K \subseteq \mathbb{R}$. Then*:

(i) *no root α of $f(X)$ lies in the K-convex hull of the remaining roots*;

(ii) *if α, β and γ are distinct roots of $f(X)$ and $\theta := (\alpha-\beta)/(\beta-\gamma) \in \mathbb{R}$, then $f(X)$ is reducible over $K(\theta)$.*

Proof. (i) This follows immediately from the theorem taking $\sum_{i \neq j} c_i = 1 = -c_j$ with $c_i > 0$ for all $i \neq j$.

(ii) Since $\alpha - (1+\theta)\beta + \theta\gamma = 0$, therefore α, β and γ are collinear in the complex plane, and the root which lies between the other two is in the $K(\theta)$-convex hull of those two. Thus (i) shows that $f(X)$ is not irreducible over $K(\theta)$. ∎

Remark. The condition that K (respectively, $K(\theta)$) is a real field cannot be dropped in the preceding theorem and its corollary. For example, let $f(X) = X^p - 2$ where p is an odd prime. The roots of $f(X)$ are $\gamma\omega^i$ $(i = 0, 1, \dots, p-1)$ where $\gamma := \sqrt[p]{2}$ and ω is a primitive pth root of 1. Put

$K := \mathbb{Q}(\omega)$. We claim $f(X)$ is not reducible over $\mathbb{Q}(\omega)$. Indeed, $f(X)$ is irreducible over $\mathbb{Q}$ by the Eisenstein criterion, so $[\mathbb{Q}(\gamma) : \mathbb{Q}] = p$. Thus $p \,|\, [K(\gamma) : \mathbb{Q}]$ by the tower theorem and $[K(\gamma) : K] \le p$. Since $p \nmid [K : \mathbb{Q}]$, we conclude that $[K(\gamma) : K] = p$ and so $f(X)$ is irreducible over K. Since $(\gamma\omega^2 - \gamma\omega)/(\gamma\omega - \gamma) = \omega \in K$, this yields a counterexample to both parts of the corollary when the condition of reality is dropped.

Lemma 5 has the following analogue.

LEMMA 5′. *Suppose that $(e_\delta)c \in U$ for some $c \in KG$. Then there is an irreducible matrix representation ϱ of G over $\mathbb{C}$ such that $\varrho(c)$ is singular; ϱ may be chosen as an irreducible constituent of the representation of G induced from the trivial representation of G_δ.* ∎

This leads to straightforward analogues of Theorems 4 and 5 for additive relations.

Acknowledgements. This research was supported in part by grant NSERC A7171. The author wishes to acknowledge the hospitality of the Department of Mathematics of the University of British Columbia during 1995–96 when much of this work was done.

References

[1] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley, New York, 1962.
[2] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer, New York, 1996.
[3] M. Drmota and M. Ska/lba, *Relations between polynomial roots*, Acta Arith. 71 (1995), 65–77.
[4] R. Ferguson, *Irreducible polynomials with many roots of equal modulus*, ibid. 78 (1997), 221–225.
[5] C. J. Smyth, *Conjugate algebraic numbers on conics*, ibid. 40 (1982), 333–346.
[6] —, *Additive and multiplicative relations connecting conjugate algebraic numbers*, J. Number Theory 23 (1986), 243–254.
[7] N. Tschebotaröw, *Grundzüge der Galoisschen Theorie* (transl. and revised by H. Schwerdtfeger), Noordhoff, Groningen, 1950.
[8] B. L. van der Waerden, *Modern Algebra*, Vol. I, Ungar, New York, 1948.
[9] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario K1S 5B6
Canada
E-mail: jdixon@math.carleton.ca

Received on 23.12.1996
and in revised form on 13.6.1997 (3100)