Polynomial Relations between Polynomial Roots

Gerd Baron, Michael Drmota, and Mariusz Skałba[1]

August 21, 2000

Abstract

Let $f(x) \in K[x]$ be a polynomial and $x_1, \ldots, x_n$ its roots. By assuming conditions on the Galois group of $f(x)$ we describe which polynomial relations between $x_1, \ldots, x_n$ may exist resp. which relations cannot exist.

1 Introduction

Let K be a field and $f(x) \in K[x]$ a separable polynomial of degree $n > 1$ and denote the roots of $f(x)$ by $x_1, \ldots, x_n$. It is obvious that for any symmetric polynomial $P(X_1, \ldots, X_n)$

$$P(x_1, \ldots, x_n) \in K.$$

However, these are surely not the only polynomial relations between the roots $x_1, \ldots, x_n$, e.g. $f(x_1) = 0$. It is one of the classical results of Galois theory to describe all polynomial relations between $x_1, \ldots, x_n$.

Theorem 1 ([9]) *Let $f(x) \in K[x]$ be separable polynomial of degree $n > 1$. and denote the roots of $f(x)$ by $x_1, \ldots, x_n$. Suppose that $\nu \le n$ and that $P(X_1, \ldots, X_\nu) \in K[X_1, \ldots, X_\nu]$ is a polynomial in ν variables such that*

$$P(x_1, \ldots, x_\nu) = 0.$$

Then $P(X_1, \ldots, X_\nu)$ has a representation of the form

$$\begin{aligned} P(X_1, \ldots, X_\nu) &= f_1(X_1)q_1(X_1, \ldots, X_\nu) + f_2(X_1, X_2)q_2(X_1, \ldots, X_\nu) + \cdots \\ &\quad + f_\nu(X_1, \ldots, X_\nu)q_\nu(X_1, \ldots, X_\nu), \end{aligned}$$

where $q_i(X_1, \ldots, X_\nu) \in K[X_1, \ldots, X_\nu]$, $1 \le i \le \nu$ are arbitrary polynomials and $f_1(X_1)$, $f_2(X_1, X_2)$, ..., $f_\nu(X_1, \ldots, X_\nu)$ are the first ν fundamental modules of $f(x)$.

[1]This work was supported by the Austrian Science Foundation, grants M 0038–PHY and M 00233–MAT.

You can find the definition of "fundamental modules" in [9, pp. 190–196]. There is even a finite algorithm to determine all fundamental modules of $f(x)$, e.g. $f_1(X_1) = f(X_1)$.

It should be remarked, too, that classically the Galois group G of a polynomial $f(x)$ is exactly the subgroup of the permutation group of its roots $x_1, \ldots, x_n$ consisting of those permutations σ which transfer any correct polynomial relation $P(x_1, \ldots, x_n) = 0$ into another correct one $\overline{P}(x_1, \ldots, x_n) = P(\sigma(x_1), \ldots, \sigma(x_n)) = 0$.

Therefore, the general problem concerning polynomial relations between polynomial roots is already solved. The solution depends on the polynomial $f(x)$ and on the structure of the subfields (of the splitting field of $f(x)$) which are generated iteratively by the roots $x_1, \ldots, x_n$. However, there are subproblems which solutions only depend on the Galois group G and not on the special structure of fundamental modules. The following observation is due to Smyth [8].

Theorem 2 ([8]) *Suppose that the Galois group G of a separable polynomial $f(x) \in K[x]$ of degree n is the symmetric group S_n.*

If $\mathrm{char}(K) = 0$ *or if* $\mathrm{char}(K) > n$ *then there are no non-trivial additive relations between the roots $x_1, \ldots, x_n$ of $f(x)$.*

If $f(x)$ does not divide a polynomial of the form $x^N + a$ then there are no non-trivial multiplicative relations between its roots.

An additive relation is a relation of the kind

$$a_1 x_1 + \cdots a_n x_n \in K, \quad a_i \in K,$$

i.e. the polynomial $P(X_1, \ldots, X_n)$ is linear, and a multiplicative relation is of the form

$$x_1^{k_1} \cdots x_n^{k_n} \in K, \quad k_i \in \mathbf{Z},$$

this means that $P(X_1, \ldots, X_n)$ can be rewritten as a binomial. We call them trivial if $a_1 = a_2 = \cdots = a_n$ resp. if $k_1 = k_1 = \cdots = k_n$.

If G is not the symmetric group then the general description of Theorem 1 can be used to get an answer in any given example. But Theorem 1 is surely not the appropriate mean to obtain an answer in general situations.

The aim of this paper is twofold. First we want to find generalizations of Theorem 2 in the sense that not as restrictive conditions on the Galois group of $f(x)$ ensure that there are no polynomial relations $P(x_1, \ldots, x_n) = 0$ between the roots $x_1, \ldots x_n$ for a small class of polynomials $P(X_1, \ldots, X_n)$. On the other hand we want to describe situations where polynomial relations between $x_1, \ldots, x_n$ do exist.

In section 2 we will show that under certain transitivity assumptions on the Galois group of $f(x)$ there are no non-trivial polynomial relations between its roots whereas in section 3 we provide a simple rule how to construct irreducible polynomials $f(x)$ such that its roots satisfy special relations. Finally section 4 gives an algebraic description of multiplicative and additive relations.

It should be noticed that the problem of independence of polynomial roots has been considered several times (e.g. by Mordell [7]) but from a completely different point of view. For example, in [7] the independence of $x_1, \ldots, x_k \in K$ which are roots of polynomials $x^{n_i} - a_i$, $a_i \in K$, $1 \leq i \leq k$ is discussed. But there is almost no literature concerning the subject investigated in this paper. Smyth [8] characterized multiplicative and linear relations between (non necessary different) conjugates of an algebraic number α. Furthermore, the second two authors considered multiplicative and additve relations between (distinct) polynomial roots if n (the degree of $f(x)$) is prime [3] and if the Galois group is abelian [4].

2 Multiple Transitivity of the Galois group

A Galois group G of a polynomial $f(x)$ with roots $x_1, \ldots, x_n$ is k-transitive if for any two ordered subsets $(x_{i_1}, \ldots, x_{i_k})$, $(x_{j_1}, \ldots, x_{j_k})$ of $\{x_1, \ldots, x_n\}$ of size k there exists $\sigma \in G$ with $\sigma(x_{i_1}) = x_{j_1}, \ldots, \sigma(x_{i_k}) = x_{j_k})$. Any Galois group of an irreducible polynomial is transitive (1-transitive). But it need not be k-transitive for $k > 1$. The symmetric group S_n is obviously n-transitive and the alternating group A_n $(n-2)$-transitive.

The characterization of k-transitive permutation groups has a long history and it was an open problem to decide whether there exist non-trivial k-transitive groups for large k or not. In 1969 Wielandt [10] (compare also with [5]) provided a classification of 2-transitive groups. Much less is known for 3-transitive permutations groups. A non-trivial example is the Mathieu group M_{22}. However, if G is 4-transitive then it follows from the classification of finite simple groups that G is either one of the four Mathieu groups M_{11}, M_{12}, M_{23}, M_{24}, or the alternating group A_n, $n \geq 6$, or the symmetric group S_n, $n \geq 4$ (see [2]). Note that M_{11} and M_{23} are 4-transitive and M_{12} and M_{24} are 5-transitive.

Our first observation, which is in fact in the spirit of Theorem 1, should give a hint why the transitivity of the Galois group might play an important rôle in the theory of polynomial relations between polynomial roots. It will also be used in the proofs of Theorems 4 and 5.

Proposition 1 *Suppose that the Galois group G of a separable polynomial $f(x) \in K[x]$ of degree n is k-transitive. Then there are no polynomial relations between k roots $x_{i_1}, \ldots, x_{i_k}$ of degree n_j in x_{i_j} satisfying $n_j \leq n - k$ for some j, $1 \leq j \leq k$.*

PROOF. Without loss of generality we can assume that $n_k \leq n - k$. The Galois group G is k-transitive if and only if the k-th Cauchy module $f_k(x) = f(x)/((x - x_{i_1}) \cdots (x - x_{i_{k-1}}))$ is irreducible in $K[x_{i_1}, \ldots, x_{i_{k-1}}]$. Furthermore

$f_k(x)$ satisfies $f_k(x_{i_k}) = 0$ and it has degree $n-k+1$. Hence there is no polynomial relation of $x_{i_1}, \ldots, x_{i_k}$ of degree $n_k \le n-k$ in x_{i_k}. □.

The next theorem shows that 2-transitivity is also sufficient to guarantee that there are no additive and no multiplicative relations between $x_1, \ldots, x_n$ and therefore generalizes Theorem 2.

Theorem 3 *Suppose that the Galois group G of a separable polynomial $f(x) \in K[x]$ of degree n is 2-transitive.*

If $\mathrm{char}(K) = 0$ *or if* $\mathrm{char}(K)$ *and* $|G|$ *are coprime then there are no non-trivial additive relations between the roots $x_1, \ldots, x_n$ of $f(x)$.*

If $f(x)$ does not divide a polynomial of the form $x^N + a$ then there are no non-trivial multiplicative relations between its roots.

Proof. For $\sigma \in G$ and $P(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ we will use the notation $\sigma P(x_1, \ldots, x_n) = P(\sigma(x_1), \ldots, \sigma(x_n))$. G_i will denote the subgroup of G fixing x_i and G_{ij} the subgroup fixing x_i and x_j. Since G is 2-transitive the number of elements $g = |G_{ij}|$ is independent of i, j. Furthermore, $|G_i| = (n-1)g$ and $|G| = n(n-1)g$.

Suppose that

$$\prod_{i=1}^{n} x_i^{k_i} = a \in K$$

for some integers $k_i \in \mathbf{Z}$ and set $b = \prod_{i=1}^{n} x_i$. By observing that there are exactly g permutations contained in G_1 which map x_i to x_j, $i, j \ne 1$, we obtain

$$\prod_{\sigma \in G_1} \sigma \prod_{i=1}^{n} x_i^{k_i} = x_1^{(n-1)gk_1} \prod_{i=2}^{n} x_i^{g(k-k_1)} = a^{(n-1)g},$$

with $k = \sum_{i=1}^{n} k_i$. Hence

$$x_1^{g(nk_1-k)} b^{g(k-k_1)} = a^{(n-1)g}.$$

If $nk_1 \ne k$ then $f(x)$ would be a divisor of $x^{g(nk_1-k)} - a^{(n-1)g} b^{-g(k-k_1)}$. Hence $k_1 = k/n$. In the same fashion we obtain $k_i = k/n = \text{const.}$, $1 \le i \le n$. Therefore there are no (non-trivial) multiplicative relations.

The additive case can be treated by precisely the same arguments. You only have to take into account that $\sum_{i=1}^{n} x_i \in K$ and that $x_1 \notin K$. □

The above methods can be applied for relations of the kind

$$a_1 x_1^m + \cdots + a_n x_n^m \in K,$$

too. They can be treated as additive relations. Hence, under the above conditions, the only relations of this kind appear if $a_1 = \cdots = a_n$. These are special polynomial relations of degree m. However, the general case of polynomial relations of degree m is not so easy to describe. In the following we will discuss the cases $m = 2$ and $m = 3$ in detail. For this purpose we will write $f(x)$ as

$$f(x) = x^n - p_1 x^{n-1} + p_2 x^{n-2} \mp \cdots + (-1)^n p_n,$$

where p_j, $1 \leq j \leq n$, denote the elementary symmetric functions

$$p_j = \sum_{I \subseteq \{1,2,\ldots,n\}, |I|=j} \prod_{i \in I} x_i$$

of the roots $x_1, \ldots, x_n$.

Theorem 4 *Suppose that the Galois group G of a separable polynomial $f(x) \in K[x]$ of degree n is 4-transitive and that $\mathrm{char}(K) = 0$ or that $\mathrm{char}(K)$ and $|G|$ are coprime. Then the only quadratic polynomials $Q(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ satisfying*

$$Q(x_1, \ldots, x_n) \in K \tag{1}$$

are of the form

$$Q(X_1, \ldots, X_n) = \sum_{i=1}^{n} a_i X_i^2 + \sum_{1 \leq i < j \leq n} (2b + a_i + a_j) X_i X_j + \sum_{i=1}^{n} (c - a_i p_1) X_i + d, \tag{2}$$

where $a_i \in K$, $1 \leq i \leq n$ and $b, c, d \in K$ are $n+3$ arbitrary (free) parameters.

It is interesting to observe that all polynomials of the kind (2) satisfy (1), i.e.

$$Q(x_1, \ldots, x_n) = bp_2 + cp_1 + d \in K,$$

although they are not symmetric in general. However, this cannot happen if $Q(X_1, \ldots, X_n)$ is a quadratic form or if it contains no mixed terms $X_i X_j$, $i \neq j$, as the following Corollary shows.

Corollary 1 *Suppose that $f(x) \in K[x]$ and K satisfy the same assumptions as in Theorem 4.*

If a quadratic form $Q(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ satisfies (1) and if $p_1 \neq 0$ then it is of the form

$$Q(X_1, \ldots, X_n) = a \sum_{i=1}^{n} X_1^2 + 2b \sum_{1 \leq i < j \leq n} X_i X_j,$$

where $a, b \in K$.

If a quadratic polynomial $Q(X_1, \ldots, X_n)$ contains no mixed terms $X_i X_j$, $i \neq j$, and satisfies (1) then it is of the form

$$Q(X_1, \ldots, X_n) = a \sum_{i=1}^{n} X_i^2 + b \sum_{i=1}^{n} X_i + c,$$

where $a, b, c \in K$.

PROOF OF THEOREM 4 It is clear that any quadratic polynomial $Q(X_1, \ldots, X_n)$ can be written in the form

$$Q(X_1, \ldots, X_n) = \sum_{i=1}^{n} a_i X_i^2 + \sum_{1\le i<j\le n} (2b_{ij} + a_i + a_j) X_i X_j + \sum_{i=1}^{n} (c_i - a_i p_1) X_i + d$$

with $a_i, b_{ij}, c_i, d \in K$. Our aim is to show that b_{ij} and c_i are constant. Since

$$\left(\sum_{i=1}^{n} a_i X_i\right)\left(\sum_{i=1}^{n} X_i\right) = \sum_{i=1}^{n} a_i X_i^2 + \sum_{1\le i<j\le n} (a_i + a_j) X_i X_j$$

we can concentrate on the expression

$$\begin{aligned} Q(x_1, \ldots, x_n) &= 2\sum_{1\le i<j\le n} b_{ij} x_i x_j + \sum_{i=1}^{n} c_i x_i + d \\ &= \sum_{i,j=1}^{n} b_{ij} x_i x_j + \sum_{i=1}^{n} c_i x_i + d = q \in K, \end{aligned}$$

where we assume that $b_{ii} = 0$ and $b_{ji} = b_{ij}$ for $j > i$. We will use the abbreviations $B = \sum_{i,j=1}^{n} b_{ij}$, $B_i = \sum_{j=1}^{n} b_{ij}$, $1 \le i \le n$, and $C = \sum_{i=1}^{n} c_i$.

As above let G_i denote the subgroup of permutations of G fixing x_i, $G_{i_1 i_2}$ the subgroup fixing x_{i_1} and x_{i_2}, $G_{i_1 i_2 i_3}$ the subgroup fixing x_{i_1}, x_{i_2}, and x_{i_3}, and $G_{i_1 i_2 i_3 i_4}$ the subgroup fixing x_{i_1}, x_{i_2}, x_{i_3}, and x_{i_4}. Since G is 4-transitive $G_{i_1 i_2 i_3 i_4}$ consists of g_4 elements independent of the choice $\{i_1, i_2, i_3, i_4\}$. Furthermore $|G_{i_1 i_2 i_3}| = g_3 = (n-3)g_4$, $|G_{i_1 i_2}| = g_2 = (n-2)g_3$, and $|G_i| = g_1 = (n-1)g_2$. Hence we get

$$\begin{aligned} &\sum_{\sigma\in G_1} \sigma Q(x_1, \ldots, x_n) \\ &= 2\sum_{j=1}^{n} b_{1j} x_1 \sum_{\sigma\in G_1} \sigma(x_j) + \sum_{i,j=2}^{n} b_{ij} \sum_{\sigma\in G_1} \sigma(x_i)\sigma(x_j) \\ &\quad + c_1 g_1 x_1 + \sum_{i=2}^{n} c_i \sum_{\sigma\in G_1} \sigma(x_i) + g_1 d \\ &= 2\sum_{j=1}^{n} b_{1j} x_1 g_2 (p_1 - x_1) + \sum_{i,j=2}^{n} b_{ij} g_3 2(p_2 - x_1(p_1 - x_1)) \\ &\quad + c_1 g_1 x_1 + \sum_{i=2}^{n} c_i g_2 (p_1 - x_1) + g_1 d \\ &= 2(n-2) g_3 B_1 x_1 (p_1 - x_1) + 2 g_3 (B - 2B_1)(p_2 - x_1(p_1 - x_1)) \\ &\quad + (n-1) g_2 c_1 x_1 + g_2 (C - c_1)(p_1 - x_1) + g_1 d \\ &= 2 g_3 (B - nB_1) x_1^2 + (2 g_3 p_1 (nB_1 - B) + g_2 (nc_1 - C)) x_1 \\ &\quad + (2 g_3 (B - 2B_1) p_2 + g_2 (C - c_1) p_1 + g_1 d = g_1 q. \end{aligned}$$

This means that x_1 satisfies a quadratic polynomial which is impossible by Proposition 1 unless all coefficients vanish. Thus $B_1 = B/n$ and consequently $c_1 = C/n$. In the same fashion we get $B_i = B/n =$ const. and $c_i = C/n =$ const., $1 \le i \le n$.

Since $\sum_{i=1}^n c_i x_i = \frac{C}{n} p_1 \in K$ we now can restrict to the polynomial relation

$$P(x_1, \ldots, x_n) = \sum_{i,j=1}^n b_{ij} x_i x_j = p \in K,$$

in which we know that $B_i = B/n$, $1 \le i \le n$. Similarly as above we calculate

$$\begin{aligned}
\sum_{\sigma \in G_{12}} \sigma P(x_1 \ldots, x_n) &= 2g_2 b_{12} x_1 x_2 + 2g_3 \sum_{j \ne 1,2} b_{1j} \sum_{k \ne 1,2} x_1 x_k \\
&\quad + 2g_3 \sum_{j \ne 1,2} b_{2j} \sum_{k \ne 1,2} x_2 x_k + g_4 \sum_{i,j \ne 1,2} b_{ij} \sum_{k,l \ne 1,2} x_k x_l \\
&= g_2 p \in K
\end{aligned}$$

and by using the relations

$$\begin{aligned}
&\sum_{j \ne 1,2} b_{1j} = B_1 - b_{12}, \quad \sum_{j \ne 1,2} b_{2j} = B_2 - b_{12}, \\
&\sum_{i,j \ne 1,2} b_{ij} = B - 2B_1 - 2B_2 + 2b_{12}, \quad \sum_{k \ne 1,2} x_k = p_1 - x_1 - x_2, \\
&\sum_{k,l \ne 1,2} x_k x_l = 2(p_2 - p_1(x_1 + x_2) + x_1^2 + x_1 x_2 + x_2^2)
\end{aligned}$$

we obtain a quadratic relation of x_1 and x_2. By Proposition 1 the coefficient of x_1^2 which is given by

$$2g_4(B - (n-1)B_1 - 2B_2 + (n-1)b_{12})$$

must vanish. Hence $b_{12} = B_1/(n-1) = B/(n(n-1))$. In the same way we get $b_{ij} = B/(n(n-1)) =$ const., $1 \le i, j \le n$, $i \ne j$. This completes the proof of Theorem 4 $\Box$.

In the case of cubic polynomials $C(X_1, \ldots, X_n)$ we can use similar ideas as above in order to identify those satisfying (1). They are of the form

$$\begin{aligned}
C(X_1, \ldots, X_n) &= \sum_{i=1}^n (\alpha_i + \beta_i) X_i^3 + \sum_{i \ne j} (b_{ij} + \alpha_j + \beta_i) X_i^2 X_j \\
&\quad + \sum_{i<j<k} (6c + b_{ij} + b_{ji} + b_{ik} + b_{ki} + b_{jk} + b_{kj}) X_i X_j X_k \\
&\quad + \sum_{i=1}^n (d_i - \beta_i p_1) X_i^2 \qquad (3)
\end{aligned}$$

$$+\sum_{i<j}(2e+d_i+d_j-b_{ij}-b_{ji})X_iX_j$$
$$+\sum_{i=1}^{n}(f-d_ip_1-\alpha_i(p_1^2-2p_2))X_i+g,$$

where $b_{ij}=b_{ji}\in K$, $1\le i\ne j\le n$, $\alpha_i,\beta_i,d_i\in K$, $1\le i\le n$, $c,e,f,g\in K$ are $(n^2+5n+8)/2$ arbitrary parameters. Conversely it is easy to verify that all polynomials of the form (3) satisfy

$$C(x_1,\ldots,x_n)=6cp_3+2ep_2+fp_1+g\in K.$$

However, in this proof we need the assumption that G is 6-transitive. Thus G is either A_n or S_n. Nevertheless it seems that a proof of (3) is not really easier by assuming that G is A_n or S_n.

A generalization of (3) to polynomials $P(X_1,\ldots,X_n)$ of degree $k>3$ seems to be very difficult. However, if $P(X_1,\ldots,X_n)$ is linear in all variables X_i, $1\le i\le n$, i.e. it has the form

$$P(X_1,\ldots,X_n)=\sum_{j=0}^{k}\sum_{1\le i_1<i_2<\cdots<i_j\le n}c_{i_1i_2\cdots i_j}X_{i_1}X_{i_2}\cdots X_{i_j} \tag{4}$$

then $P(X_1,\ldots,X_n)$ must be symmetric.

Theorem 5 *Suppose that the Galois group G of a separable polynomial $f(x)\in K[x]$ of degree n is $2k$-transitive, $k\ge 1$. (This means that G is A_n, $n\ge 2k+2$, or S_n, $n\ge 2k$, for $k\ge 3$.) Furthermore if $\mathrm{char}(K)>0$ then assume that $\mathrm{char}(K)$ and $|G|$ are coprime and that $\mathrm{char}(K)>k$. Then the only polynomials $P(X_1,\ldots,X_n)\in K[X_1,\ldots,X_n]$ of the form (4) satisfying (1) are given by*

$$P(X_1,\ldots,X_n)=\sum_{j=0}^{k}c_jp_j(X_1,\ldots,X_n),$$

where $p_j(X_1,\ldots,X_n)$, $1\le j\le k$, denote the elementary symmetric functions.

Proof. For any subset $M\subseteq\{1,\ldots,n\}$ of size $m=|M|\le 2k$ let G_M denote the subgroup of G fixing x_i for $i\in M$. If $m\le 2k$ then $|G_M|=g_m$ only depends on m and satisfies $g_m=(n-m)g_{m+1}$. Furthermore, G_M is j-transitive for any $j\le 2k-m$ and for any two ordered subsets $(i_1,\ldots,i_j)$, $(l_1,\ldots,l_j)$ which are disjoint to M there are exactly g_{j+m} permuations $\sigma\in G_M$ satisfying $\sigma(x_{i_1})=x_{l_1}$,…,$\sigma(x_{i_j})=x_{l_j}$.

Let

$$P_j(X_1,\ldots,X_n)=\sum_{1\le i_1<i_2<\cdots<i_j\le n}c_{i_1i_2\cdots i_j}X_{i_1}X_{i_2}\cdots X_{i_j},\quad 0\le j\le k.$$

and consider a subset $M \subseteq \{1, \ldots, n\}$ of size $|M| \le k$. Then

$$R_M(X_1, \ldots, X_n) = \sum_{\sigma \in G_M} \sigma P(X_1, \ldots, X_n)$$

is symmetric in X_i, $i \notin M$. By using the relations

$$p_j(z_1, \ldots, z_l) = p_j(z_1, \ldots, z_l, z_{l+1}) - z_{l+1} p_{j-1}(z_1, \ldots, z_l)$$

we can replace the elementary symmetric functions of X_i, $i \notin M$ by $p_j(X_1, \ldots, X_n)$, $1 \le j \le n$ and by X_i, $i \in M$. Hence $R_M(x_1, \ldots, x_n)$ can be represented by a polynomial of degree k in x_i, $i \in M$. Furthermore the appearing terms of degree k only depend on $P_k(X_1, \ldots, X_n)$ and not on $P_j(X_1, \ldots, X_n)$, $0 \le j < k$. By Proposition 1 all coefficients must vanish. In what follows we will only use the fact that the coefficients of those terms of degree k vanish. Therefore, we will operate with

$$R_{k,M}(X_1, \ldots, X_n) = \sum_{\sigma \in G_M} \sigma P_k(X_1, \ldots, X_n)$$

instead of $R_M(X_1, \ldots, X_n)$ and will show that $c_{i_1 \cdots i_k} = c_k = \text{const}$. In fact this will finish our proof since we can apply an inductive argument for $P(X_1, \ldots, X_n) - P_k(X_1, \ldots, X_n)$.

For any two disjoint subsets $U, V \subseteq \{1, \ldots, n\}$ set

$$D(U, V) = \sum_{I(U,V)} c_{i_1 i_2 \cdots i_k},$$

where $I(U, V)$ denotes the set of k-tuples $i_1 < i_2 < \cdots < i_k$ such that $U \subseteq \{i_1, i_2, \ldots, i_k\}$ and $\{i_1, i_2, \ldots, i_k\} \cap V = \emptyset$. Note that

$$D(U, V) = D(U \cup \{i\}, V) + D(U, V \cup \{i\}) \tag{5}$$

if $i \notin U \cup V$.

In order to finish the proof we will show that $D(U, V) = d_{|U|,|V|}$ only depends on the cardinalities $|U|$ and $|V|$ if $|U| + |V| \le k$. By applying this property to any set $U = \{i_1, \ldots, i_k\}$ of cardinality k and to $V = \emptyset$ we will finally obtain $D(U, V) = c_{i_1 \cdots i_k} = d_{k,0} = \text{const}$.

By (5) it suffices to show $D(U, V) = d_{|U|,|V|}$ for $|U| \le 1$. Consider any set V of cardinality $|V| \le k - 1$ and suppose that $U = \{i\}$ is disjoint to V. Set $M = U \cup V = \{i\} \cup V$ and $m = |V| + 1$. Then

$$\begin{aligned} R_{k,M}(x_1, \ldots, x_n) &= (k-1)! \sum_{I(\{i\},V)} c_{i_1 i_2 \cdots i_k} g_{m+k-1} x_i p_{k-1}\left((x_l)_{l \notin \{i\} \cup V}\right) \\ &\quad + k! \sum_{I(\emptyset, \{i\} \cup V)} c_{i_1 i_2 \cdots i_k} g_{m+k} p_k\left((x_l)_{l \notin \{i\} \cup V}\right) + \cdots \\ &= \Big((-1)^{k-1}(k-1)! g_{m+k-1} D(\{i\}, V) \\ &\qquad + (-1)^k k! g_{m+k} D(\emptyset, \{i\} \cup V)\Big) x_i^k + \cdots \end{aligned}$$

implies that

$$D(\{i\},V) = \frac{k}{n-m-k+1} D(\emptyset,\{i\}\cup V) = \frac{k}{n-|V|-k} D(\emptyset,\{i\}\cup V) \qquad (6)$$

and by (5)

$$D(\emptyset,V) = \frac{n-m+1}{n-m-k-1} D(\emptyset,\{i\}\cup V) = \frac{n-|V|}{n-|V|-k} D(\emptyset,\{i\}\cup V).$$

Starting from $D(\emptyset,\emptyset) = P_k(1,1,\dots,1)$ it follows inductively that $D(\emptyset,V)$ only depends on $|V|$ if $|V| \le k$. Moreover, by (6) the same is true for $D(\{i\},V)$ if $|V| \le k-1$. This completes the proof of Theorem 5. □

3 A Construction Method for Multiplicative Relations

In this section we want to describe a method to construct polyomials which roots satisfy non-trivial multiplicative relations. The first example known to the authors is due to A. Schinzel (Warsaw):

$$f(x) = x^6 - 2x^4 - 6x^3 - 2x^2 + 1 \qquad (7)$$

and has answered a problem by J. Browkin (Warsaw) affirmatively. It has three roots x_1, x_2, x_3 which satisfy

$$x_1 x_2 = x_3.$$

This can be seen by the observation that $f(x)$ factorizes in the following way:

$$f(x) = (x^3 + \sqrt{2}x^2 + \sqrt{2}x - 1)(x^3 - \sqrt{2}x^2 - \sqrt{2}x - 1) = g_1(x)g_2(x).$$

Let x_1, x_2, x_4 denote the roots of the first factor $g_1(x)$. Obviously they satisfy $x_1x_2x_4 = 1$. Since $f(x)$ is reciprocal, the roots of the second factor $g_2(x)$ are $x_5 = 1/x_1, x_6 = 1/x_2, x_3 = 1/x_4$ and hence $x_1x_2 = 1/x_4 = x_3$

The preceding polynomial (7) is an example, where lots of multiplicative relations between its roots exist. A basis of them is given by: $x_1x_2x_4 = 1$, $x_3x_5x_6 = 1$, $x_1x_5 = 1$, $x_2x_6 = 1$, $x_3x_4 = 1$. (There are no non-trivial relations between x_1, x_2, x_4 resp. between x_3, x_5, x_6 by [3, Theorem 1].) The last three relations are more or less trivial since (7) is reciprocal. However, the first two are really non-trivial and are special cases of the following general procedure.

Proposition 2 *Let $K(\alpha)/K$ be an algebraic field extension of degree m and denote $\alpha = \alpha_1, \alpha_2, \dots, \alpha_m$ the conjugates of α. Let $g(x) \in K(\alpha)[x]$ a polynomial of degree k with constant term c satisfying $c^N \in K$ for some $N \in \mathbf{N}$. Set*

$$f(x) = \prod_{j=1}^{m} g_j(x) \in K[x],$$

where $g(x) = g_1(x), g_2(x), \ldots, g_m(x)$, $g_j(x) \in K(\alpha_j)[x]$, $1 \leq j \leq m$, *are the conjugate polynomials of* $g(x)$. *Furthermore, let* $x_{k(j-1)+i}$, $1 \leq i \leq k$ *be the roots of* $g_j(x)$, $1 \leq j \leq m$, *i.e.* $x_1, \ldots, x_n$, $n = mk$, *are the roots of* $f(x)$. *Then these roots of* $f(x)$ *satisfy non-trivial multiplicative relations of the kind*

$$\prod_{j=1}^{m} \prod_{i=1}^{k} x_{k(j-1)+i}^{k_j} \in K,$$

where $k_1 \equiv k_2 \equiv \cdots \equiv k_m \bmod N$.

Finally we want to mention that in principal for any specific polynomial $f(x)$ there is an effective algorithm to determine a basis of all multiplicative relations between its roots $x_1, \ldots, x_n$. Let L denote the splitting field of $f(x)$ and let S be the set of all archimedian valuations of L and of all prime ideals which appear in the prime factorisations of the fractional pricipal ideals (x_i), $1 \leq i \leq n$. Then the roots $x_1, \ldots, x_n$ are S-units. Since a basis of the finitely generated group of S-units can be computed effectively we can represent $x_1, \ldots, x_n$ in this basis. Hence the problem to determine a basis for all multipliciative relations between $x_1, \ldots, x_n$ is translated into an easy problem of linear algebra.

4 Multiplicative and Additive Relations

In this section we will use as little bit different language, namely that of (multiplicative and additive) relations between conjugates of a number α contained in a finite normal extension $F/\mathbf{Q}$ with Galois group G. In [4] it is shown that almost all algebraic integers in F satisfy no (non-trivial) multiplicative relation. In particular we will use the following property.

Lemma 1 ([4]) *Let* $F/\mathbf{Q}$ *be a finite normal extension of* $\mathbf{Q}$ *with Galois group* G. *Then there are infinitely many algebraic integers* $\gamma_j \in F$ *with pairwise relatively prime norms such that*

$$\prod_{\sigma \in G} \sigma(\gamma_j)^{a_\sigma} \in \mathbf{Q}, \qquad a_\sigma \in \mathbf{Z} \tag{8}$$

implies $a_\sigma = \text{const}$. *Furthermore all these* γ_j *can be chosen in a way that there are prime ideals* $\mathbf{p}_j$ *dividing* (γ_j) *with* $e_{\mathbf{p}_j} = f_{\mathbf{p}_j} = 1$.

For any subfield E of F let $\mathcal{R}(E)$ denote the group of $\alpha \in E^*$ satisfying the multiplicative relation

$$\prod_{\sigma \in G} \sigma(\alpha)^{a_\sigma} \in \mathbf{Q}^* \tag{9}$$

where $(a_\sigma)_{\sigma \in G}$ is a fixed sequence of integers.

In the sequel we will also simplify our notation by using the notion of group rings. If

$$R = \sum_{\sigma \in G} a_\sigma \sigma \in \mathbf{Z}[G],$$

then (9) can be rewritten to

$$\alpha^R \in \mathbf{Q}^*.$$

We will further use the set

$$V = \{L \in \mathbf{C}[G] \mid L \cdot R = 0\} \tag{10}$$

and the subgroup

$$H = \{\sigma \in G \mid L \cdot \sigma = L \text{ for all } L \in V\}. \tag{11}$$

Theorem 6 *Let $F/\mathbf{Q}$ be a finite normal extension with Galois group G and let $(a_\sigma)_{\sigma \in G}$ be a fixed sequence of integers. Furthermore, let H be defined by (11) and denote the fixed field of H by F^H.*

Then the factor group $\mathcal{R}(F^H)/\mathcal{R}(E)$ has infinite rank for any proper subfield E of F^H.

If in addition the field extension $(F \cap \mathbf{R})/\mathbf{Q}$ is normal and if H is a normal subgroup of G then $\mathcal{R}(F)/\mathcal{R}(F^H)$ is finite with exponent dividing w, the number of roots of unity in F.

Remark 1. A special (but quite frequently appearing) case of Theorem 6 occurs if $V = \{0\}$. Here $H = G$ and consequently $F^H = \mathbf{Q}$. This means that the "main" part of $\mathcal{R}(F)$ is contained in $\mathbf{Q}$. Note that $V = \{0\}$ is equivalent with the condition that the group determinant $d = \det(a_{\sigma\tau^{-1}})_{\sigma,\tau \in G} \neq 0$. Here the additional assumptions on $F \cap \mathbf{R}$ and on H are not necessary. By direct reasoning (compare with [8, 4]) it follows that there exists $N \in \mathbf{N}$ such that $\alpha \in \mathcal{R}(F)$ satisfies $\alpha^N \in \mathbf{Q}$. Hence $\mathcal{R}(F)/\mathcal{R}(\mathbf{Q})$ is finite. □

Remark 2. Let $\mathcal{R}_0(E)$ denote those $\alpha \in \mathcal{R}(E)$ with $\alpha^R = 1$. Then we get almost the same theorem for $\mathcal{R}_0(E)$. More precisely, if $d \neq 0$ then $\mathcal{R}_0(F)$ contains only roots of unity, whereas if $d = 0$ then we get Theorem 6 with the only difference that $\mathcal{R}(E)$ is replaced by $\mathcal{R}_0(E)$. □

Remark 3. We want to point out that the following proof provides more than the fact that $\mathcal{R}(F^H)/\mathcal{R}(E)$ has infinite rank. Actually $\mathcal{R}(F^H)$ contains a free subgroup $\mathcal{U}$ of infinite rank with $\mathcal{U} \cap \mathcal{R}(E) = \{1\}$ for any proper subfield E of F^H. □

Remark 4. Theorem 6 is a generalization of [4, Theorem 3], where the case of abelian Galois group and only relations of the form $\alpha^R = 1$ are discussed. The following proof is quite similar to that of [4]. However, significant changes had to be made. Therefore we will give a detailed version. □

Proof. For any $\sigma \in G \setminus H$ set

$$V_\sigma = \{L \in V \mid L \cdot (\sigma - 1) = 0\}.$$

Since $\dim_{\mathbf{C}} V_\sigma < \dim_{\mathbf{C}} V$ it follows that

$$(V \cap \mathbf{Z}[G]) \setminus \bigcup_{\sigma \in G \setminus H} (V_\sigma \cap \mathbf{Z}[G])$$

contains non-zero elements. Choose one of them and denote it by L. By Lemma 1 there is an infinite sequence of algebraic integers $\gamma_j \in F$ satisfying (8) such that their norms are pairwise relatively prime. Set

$$\alpha_j = \gamma_j^L.$$

Obviously α_j satisfies (9) by the definition of V and $\alpha_j \in F^H$ by the definition of H (11). Furthermore

$$(1 - \sigma) \cdot L \neq 0 \quad \text{for all } \sigma \in G \setminus H \tag{12}$$

by the choise of L. Since γ is free and

$$L \cdot (1 - \sigma) \neq c \cdot \sum_{\tau \in G} \tau$$

we have

$$\alpha_j^{1-\sigma} = \gamma_j^{L(1-\sigma)} \notin \mathbf{Q}.$$

In particular we have

$$\alpha_j \neq \alpha_j^\sigma$$

for any $\sigma \in G \setminus H$. This proves that

$$\mathbf{Q}(\alpha_j) = F^H.$$

Let E be a proper subfield of F^H and suppose that

$$\prod_j \alpha_j^{k_j} \in E$$

with certain $k_j \in \mathbf{Z}$ not all of them zero. Then there exists $\sigma \in G \setminus H$ such that

$$\prod_j \gamma_j^{Lk_j} = \prod_j \gamma_j^{L\sigma k_j} \in E$$

By Lemma 1 we can write $(\gamma_j) = \mathbf{p}_j I_j$, where $e_{\mathbf{p}_j} = f_{\mathbf{p}_j} = 1$. This means that the prime ideals $\sigma(\mathbf{p}_j)$, $\sigma \in G$, are different. Consequentely, for some j

$$\mathbf{p}_j^{k_j L\sigma} = \mathbf{p}_j^{k_j L}$$

and hence $L(1-\sigma)=0$ in contradiction to (12). This finishes the proof of the first part of Theorem 6.

For the proof of the second part let us consider for any subgroup K of G the right $\mathbf{C}[G]$-module $\mathbf{C}[G/K]$, where G/K is the set of right cosets mod K and the action of G on G/K is defined by

$$(K\tau)\cdot\sigma = K(\tau\sigma).$$

Similarly to (10) we define

$$V(K)=\{L\in\mathbf{C}[G/K]\,|\,L\cdot R=0 \text{ (in } \mathbf{C}[G/K])\}.$$

The basic property we will have to use is that

$$L\cdot\sigma = L \qquad \text{for all } \sigma\in H \text{ and all } L\in V(K) \tag{13}$$

which can be justified as follows. If $L=\sum_{\tau\in G/K} b_\tau\tau \in V(K)$ then consider $L'=\sum_{\sigma\in G} b_{K\sigma}\sigma\in\mathbf{Z}[G]$. Since $L\cdot R=0$ (in $\mathbf{C}[G/K]$) we also have $L'\cdot R=0$ (in $\mathbf{C}[G]$) and hence $L'\cdot\sigma=L'$ for all $\sigma\in H$ which immediately gives (13).

Now let us fix a number $\alpha\in F$ satisfying (9) and consider the fractional ideal (α). We can write

$$(\alpha)=\prod_{\mathbf{p}}\mathbf{p}^{L(\mathbf{p})}$$

where in the above finite product different $\mathbf{p}$ divide different rational primes and $L(\mathbf{p})\in\mathbf{Z}[G/K(\mathbf{p})]$, where $K(\mathbf{p})$ is the decomposition group of $\mathbf{p}$. Since α satisfies (9) it follows from the unique factorization of fractional ideals that for any $\mathbf{p}$ in the above product

$$L(\mathbf{p})\cdot R = a\cdot N_{G/K}$$

for some integer a, where $N_{G/K}=\sum_{\tau\in G/K}\tau$. If $\sum_{\sigma\in G}a_\sigma=0$ then

$$L(\mathbf{p})\in V(K)$$

and if $\sum_{\sigma\in G}a_\sigma=A\neq 0$ then

$$L(\mathbf{p})=\frac{a}{A}N_{G/K}+L'(\mathbf{p}),$$

where

$$L'(\mathbf{p})\in V(K).$$

In both cases we can conclude that

$$L(\mathbf{p})\cdot\sigma = L(\mathbf{p})$$

and hence

$$(\alpha)^\sigma = (\alpha) \quad \text{for all } \sigma \in H, \tag{14}$$

i.e. $\sigma(\alpha) = \varepsilon_\sigma \alpha$ for some $\varepsilon_\sigma \in \mathcal{O}_F^*$. Consequently we obtain

$$\alpha^h = N_{F/F^H}(\alpha) \cdot \varepsilon$$

where h is the order of H and $\varepsilon \in \mathcal{O}_F^*$. Since H is normal the element

$$S = \sum_{\tau \in H} \tau$$

is contained in the centrum of $\mathbf{C}[G]$ and therefore $N_{F/F^H}(\alpha)$ satisfies the relation (9). Moreover, $N_{F/F^H}(\alpha) \in \mathcal{R}(F^H)$ and $\varepsilon^R = 1$. Since the real units multiplied by roots of unity are of index 1 or 2 in the full group of units ([6, Ch.3, Prop.3.6]) there exists a natural number k depending only on F such that

$$\varepsilon^k \in \mathcal{O}_{F \cap \mathbf{R}}^*$$

Now choose a unit $\eta \in \mathcal{O}_{F\cap\mathbf{R}}^*$ such that $N_{(F\cap\mathbf{R})/\mathbf{Q}}(\eta) = 1$ and η generates a $\mathbf{Z}[Gal((F\cap\mathbf{R})/\mathbf{Q})]$-module of finite index m in $\mathcal{O}_{F\cap\mathbf{R}}^*$ ([6, Ch.3, Theorem 3.9]). We identify the group $Gal((F\cap\mathbf{R})/\mathbf{Q})$ with G/K where K corresponds to $F\cap\mathbf{R}$ (actually $|K| \leq 2$). Let us write

$$\varepsilon^{km} = \eta^L$$

with $L \in \mathbf{Z}[G/K]$. Since $\varepsilon^{km} \in \mathcal{R}(F \cap \mathbf{R})$ and

$$\prod_{\tau \in G/K} \tau(\eta)^{b_\tau} = 1 \quad \text{iff } b_\tau = \text{const.}$$

it follows that

$$L \cdot R = a \cdot N_{G/K}$$

for some integer a. As above we obtain $L\sigma = L$ for all $\sigma \in H$. Hence $\varepsilon^{km} \in \mathcal{O}_{F^H}^*$ and denoting $t = hkm$ we obtain

$$\alpha^t \in F^H.$$

$\mathcal{R}(F)/\mathcal{R}(F^H)$ is finite since it can be embedded in the finite factor group (see [4])

$$T = \{\alpha \in F^* \;:\; \text{there exists } t \in \mathbf{N} \text{ such that } \alpha^t \in (F^H)^*\}/(F^H)^*.$$

By (14) we obtain for any $\sigma \in H$

$$\alpha^t = \sigma(\alpha)^t = \varepsilon_\sigma^t \alpha^t$$

and hence ε_σ is a root of unity. Since $\varepsilon_\sigma^w = 1$ we already get

$$\sigma(\alpha^w) = \sigma(\alpha)^w = \alpha^w$$

and therefore $\alpha^w \in F^H$. This means that the exponent of $\mathcal{R}(F)/\mathcal{R}(F^H)$ divides w. $\square$

Theorem 6 has an additive analogon. Let F/K be a finite Galois extension with Galois group G such that $\mathrm{char}(K) = 0$ or that $\mathrm{char}(K)$ does not divide the degree of extension $n = [F : K]$. For any field E lying between K and F let $\mathcal{A}(E)$ denote the K-vector space consisting of $\alpha \in E$ satisfying the additive relation

$$\sum_{\sigma \in G} a_\sigma \sigma(\alpha) = 0, \tag{15}$$

where $(a_\sigma)_{\sigma \in G}$ is a fixed sequence of elements of K. Note that an arbitrary additive relation $\sum_{\sigma \in G} a_\sigma \sigma(\alpha) \in K$ can always be reduced to the case (15). If $\sum_{\sigma \in G} a_\sigma \sigma(\alpha) = a \in K$ then $\alpha' = \alpha - \frac{a}{n}$ satisfies (15). Now, let

$$R = \sum_{\sigma \in G} a_\sigma \sigma$$

be an element of the group ring $K[G]$ and let

$$V = \{L \in K[G] \mid L \cdot R = 0\} \tag{16}$$

and the subgroup

$$H = \{\sigma \in G \mid L \cdot \sigma = L \text{ for all } L \in V\}. \tag{17}$$

defined in the same manner as above. Furthermore we will simply write $\alpha \cdot L$ instead of $\sum_{\sigma \in G} b_\sigma \sigma(\alpha)$, where $L = \sum_{\sigma \in G} b_\sigma \sigma$ is an element of $K[G]$.

Theorem 7 *Let F/K be a finite Galois extension of infinite fields with Galois group G, suppose that $(a_\sigma)_{\sigma \in G}$ is a fixed sequence of elements $a_\sigma \in K$, and let H be defined by (11). Then*

$$\mathcal{A}(F) = \mathcal{A}(F^H) \tag{18}$$

and

$$\dim_K \mathcal{A}(F^H) = \dim_K V.$$

Furthermore there exists a basis of $\mathcal{A}(F^H)$ over K consisting only of elements α satisfying $K(\alpha) = F^H$.

Remark 5. Again the case $d = \det(a_{\sigma\tau^{-1}})_{\sigma,\tau\in G} \neq 0$ is equivalent to $V = \{0\}$ and it is clear that in this case only $\alpha = 0$ satisfies (15). $\Box$

Remark 6. As mentioned above, if $\mathrm{char}(K) = 0$ or if $\mathrm{char}(K)$ does not divide the degree of extension $n = [F : K]$ then Theorem 7 classifies general additive relations of the form $\sum_{\sigma\in G} a_\sigma \sigma(\alpha) \in K$, too. Let $\mathcal{A}'(F)$ denote the K-vector space of all these relations. If $\sum_{\sigma\in G} a_\sigma = 0$ then $\mathcal{A}'(F) = \mathcal{A}(F)$, i.e. $\dim_K \mathcal{A}'(F) = \dim_K \mathcal{A}(F)$, whereas if $\sum_{\sigma\in G} a_\sigma \neq 0$ then $\mathcal{A}'(F) = \mathcal{A}(F) \oplus K$ and hence $\dim_K \mathcal{A}'(F) = \dim_K \mathcal{A}(F) + 1$. (In the first case $K \subseteq \mathcal{A}(F)$ and therfore $\mathcal{A}'(F) = \mathcal{A}(F)$.) $\Box$

Remark 7. If F/K is an extention of finite fields such that $[F : K] < |K|$ then the following proof will show that the first assertion of Theorem 7 ($\mathcal{A}(F) = \mathcal{A}(F^H)$) remains true. (You only have to use the fact that the set (19) is not empty.) $\Box$

Proof. We can proceed similarly to the proof of Theorem 6. Since K contains infinitely many elements the set

$$V \setminus \bigcup_{\sigma\in G\setminus H} V_\sigma \tag{19}$$

contains not only non-zero elements but even a basis of V over K. Now choose a normal basis $\{\gamma\cdot\sigma\}_{\sigma\in G}$ of F/K and observe that $\alpha = \gamma\cdot L$ satisfies (15) if and only if $L \in V$. This proves (18) by the definition of H. Moreover, if $L_1, \ldots, L_k$ is a basis of V then $\alpha_1 = \gamma \cdot L_1, \ldots, \alpha_k = \gamma \cdot L_k$ is a basis of $\mathcal{A}(F)$ over K. In addition, we can assume that L_j, $1 \leq j \leq k$, are contained in the set (19). Hence $K(\alpha_j) = F^H$, $1 \leq j \leq k$. $\Box$

Theorems 6 and 7 are also interesting from the following point of view. In the Introduction it was shown that the description of all polynomial relations between polynomial roots depends more or less on the polynomial $f(x) \in K[x]$ and not only on its Galois group G. However the preceding two theorems only need assumptions on G. In the additive case this is not really surprising since the $K[G]$-structure of the additive group of F is very simple by the existence of a normal basis. However, the $\mathbf{Z}[G]$-structure of the multiplicative group can be very complicated. Therefore the following observation may be of own interest.

Proposition 3 *Let G be a finite Hamiltonian group, i.e. all its subgroups are normal. Furthermore, for a normal extension $F/\mathbf{Q}$ with Galois group G let $B_G(F)$ be the set of $R \in \mathbf{Z}[G]$ such that there exists $\alpha \in F^*$ satisfying $\alpha^R \in \mathbf{Q}$ and $\mathbf{Q}(\alpha^n) = F$ for any $n \in \mathbf{N}$. Then $B_G(F)$ does not depend on F but only on G.*

Proof. Let $R \in B_G(F)$ and let $F'/\mathbf{Q}$ be another normal extension with the same Galois group. By the second part of Theorem 6, H must be trivial. Hence, $R \in B_G(F')$ by the first part of Theorem 6. $\Box$.

Since Hamiltonian groups are almost abelian (i.e. abelian or the direct product of special abelian groups and the group $H = \{\pm 1, \pm i, \pm j, \pm k\}$ of order 8, see [1, p. 114–116]) Proposition 3 is more or less a theorem for abelian groups. However, it is very likely that Proposition 3 is true for any finite group. We would not need the assumption 'Hamiltonian' if it were possible to prove the second part of Theorem 6 without the additional assumptions on $F \cap \mathbf{R}$ and on H.

References

[1] R.D. Carmichael, "Introduction to the Theory of Groups of Finite Order," Dover Publications, 1956.

[2] M. Conder, *Generating the Mathieu groups and associated Steiner systems*, Dicrete Math. **112** (1993), 41-47.

[3] M. Drmota and M. Skałba, *On multiplicative and linear independence of polynomial roots*, in: Contributions to General Algebra 7 (D. Dorninger, G. Eigenthaler, H.K. Kaiser, and W.B. Müller eds.), Hölder-Pichler-Tempsky, Wien; Teubner, Stuttgart, 1991, 127–135.

[4] M. Drmota and M. Skałba, *Relations between polynomial roots*, Acta Arith., to appear.

[5] W. Knapp, *Über Wielandts Kennzeichnung der zweifachen Tansitivität von Permutationsgruppen*, Arch. Math. (Basel) **45** (1985), 385–389.

[6] W. Narkiewicz, "Elementary and Analytic Theory of Algebraic Numbers," Springer, Berlin, 1990.

[7] L.J. Mordell, *On the linear independence of algebraic numbers*, Pacific J. Math. **3** (1953), 625–630.

[8] C.J. Smyth, *Additive and multiplicative relations connecting conjugate algebraic numbers*, J. Number Th. **23** (1986), 243–254.

[9] N. Tschebotaröw - H. Schwerdtfeger, "Grundzüge der Galois'schen Theorie", Noordhoff, Groningen, 1950.

[10] H. Wielandt, *Permutation groups though invariant relations and invariant functions*, Lecture notes, Ohio State University, Columbus, Ohio, 1969.

Gerd Baron, Michael Drmota
Department of Discrete Mathematics
Technical University of Vienna

Wiedner Hauptstrasse 8–10/118
A-1040 Vienna, Austria
E-mail: mdrmota@rsmb.tuwien.ac.at

Mariusz Skałba
Institute of Mathematics
Warsaw University
Banacha 2
02-097 Warsaw, Poland
E-mail: skalba@plearn.bitnet