ACTA ARITHMETICA
LXXI.1 (1995)

Relations between polynomial roots

by

Michael Drmota (Wien) and Mariusz Skałba (Warszawa)

1. Introduction. As in [3] the main inspiration of this paper is again the following question by J. Browkin:

Does there exist an irreducible non-cyclotomic polynomial such that one root is the product of two other roots?

A. Schinzel found the following polynomial of degree 6:

$$f(x) = x^6 - 2x^4 - 6x^3 - 2x^2 + 1 \tag{1}$$

and therefore answered the preceding question affirmatively (see [3]). On the other hand, there is no such polynomial of prime degree ([3, Theorem 1]).

The aim of this paper is to provide general results for relations between distinct roots of polynomials with rational coefficients. In Section 2 we will prove that multiplicative relations between distinct polynomial roots are very rare. In Section 3 we restrict ourselves to the case of abelian Galois group and give a kind of classification. In particular, we can settle an analogue of Browkin's question in the abelian case.

Theorem 1. *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree n with abelian Galois group.*

- *If $6 \nmid n$ and if $f(x)$ is non-cyclotomic then $x_1 x_2 \ne x_3$ for any three roots x_1, x_2, x_3 of $f(x)$.*
- *If $6 \mid n$ then using a proper Tschirnhausen transformation one can obtain from $f(x)$ an irreducible non-cyclotomic polynomial $f^*(x)$ having three roots x_1^*, x_2^*, x_3^* satisfying $x_1^* x_2^* = x_3^*$.*

A *Tschirnhausen transformation* $f^*(x)$ of a polynomial $f(x) = \prod_{i=1}^n (x - x_i)$ is of the form

$$f^*(x) = \prod_{i=1}^{n} (x - \varphi(x_i)),$$

This work was supported by the Austrian Science Foundation, grant Nr. M 0038-PHY.

where $\varphi(x) \in \mathbb{Q}[x]$ is a polynomial of degree $< n$. In the case of Theorem 1 this is equivalent to the property that $f(x)$ and $f^*(x)$ have the same splitting field.

In order to give a flavour of our method to be developed below, let

$$f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

whose splitting field is the cyclotomic field $F = \mathbb{Q}(\varepsilon_7)$, $\varepsilon_7 = \exp(2\pi i/7)$. We will show how to construct explicitly a (non-cyclotomic) polynomial $f^*(x)$ of degree 6 having three roots x_1^*, x_2^*, x_3^* satisfying $x_1^* x_2^* = x_3^*$.

Let σ denote the generator of the Galois group of $f(x)$ which is defined by $\sigma(\varepsilon_7) = \varepsilon_7^3$. The starting point of our construction is a free number $\gamma \in F^*$ (see (2)). By Lemma 1, $\gamma = 2 + \varepsilon_7$ is a proper choice since $N_F(2 + \varepsilon_7) = 43$. Then

$$\begin{aligned}\alpha = \gamma^{\mathrm{id} + \sigma - \sigma^3 - \sigma^4} &= \frac{\gamma\sigma(\gamma)}{\sigma^3(\gamma)\sigma^4(\gamma)} = \frac{(2+\varepsilon_7)(2+\varepsilon_7^3)}{(2+\varepsilon_7^6)(2+\varepsilon_7^4)} \\ &= \frac{6}{43}\varepsilon_7^5 + \frac{10}{43}\varepsilon_7^4 + \frac{36}{43}\varepsilon_7^3 + \frac{6}{43}\varepsilon_7^2 + \frac{39}{43}\varepsilon_7 + \frac{30}{43}\end{aligned}$$

satisfies

$$\alpha\sigma^2(\alpha) = \sigma(\alpha).$$

We only have to check that (in the proper group ring $\mathbb{Z}[G]$)

$$(\mathrm{id} + \sigma - \sigma^3 - \sigma^4)(\mathrm{id} - \sigma + \sigma^2) = 0.$$

Hence the characteristic polynomial of α,

$$f^*(x) = x^6 - \frac{83}{43}x^5 + \frac{5587}{1849}x^4 - \frac{6551}{1849}x^3 + \frac{5587}{1849}x^2 - \frac{83}{43}x + 1,$$

has the desired property.

In the case $n = 6$ our method provides only reciprocal polynomials such that all roots x_i have modulus $|x_i| = 1$, $1 \le i \le 6$. However, it is an easy exercise to show that the sequence $(\alpha^n, (\sigma^2(\alpha))^n)$, $n \ge 1$, is uniformly distributed on the torus $T = \{(z_1, z_2) \in \mathbb{C}^2 : |z_1| = |z_2| = 1\}$. Furthermore, $\deg_{\mathbb{Q}} \alpha^n = 6$ for all $n \ge 1$ (see Remark 3). Therefore, the set of pairs $(x_1, x_2) \in T$ such that x_1, x_2, x_1x_2 are roots of an irreducible polynomial of degree $n = 6$ with splitting field $F = \mathbb{Q}(\varepsilon_7)$ is dense in T. These remarks should indicate that our method provides lots of examples but it seems that there are others.

It should be further mentioned that there is almost no literature concerning this subject. Smyth [8] considered a little bit different problem. He characterized those relations

$$\alpha_1^{a_1}\alpha_2^{a_2}\ldots\alpha_k^{a_k} = 1$$

which have solutions in (not necessarily different) conjugates $\alpha_1, \ldots, \alpha_k$ of an algebraic number α. Relations of length 2 are also discussed in [2].

2. General case. Let $F/\mathbb{Q}$ be a finite normal extension of $\mathbb{Q}$ with Galois group $G = \{\sigma_1, \ldots, \sigma_n\}$. A number $\gamma \in F^*$ will be called *free* if

$$\prod_{i=1}^{n} \sigma_i(\gamma)^{a_i} \in \mathbb{Q} \qquad (a_i \in \mathbb{Z}) \tag{2}$$

implies $a_1 = a_2 = \ldots = a_n$.

LEMMA 1. *Let $\gamma \in \mathcal{O}_F$ (i.e. it is an algebraic integer) and suppose that there exists a rational prime p satisfying*

$$p \mid N_F(\gamma) \quad \text{and} \quad p \nmid \frac{N_F(\gamma)}{p} D, \tag{3}$$

where D is the discriminant of F and N_F denotes the norm. Then γ is free.

Proof. The principal ideal (γ) generated by γ can be represented by

$$(\gamma) = \mathbf{p}I,$$

such that the absolute norms $\mathrm{N}\mathbf{p}$, $\mathrm{N}I$ of the ideals $\mathbf{p}$, I satisfy $\mathrm{N}\mathbf{p} = p$ and $(\mathrm{N}I, p) = 1$. Hence (3) implies $e_p = f_p = 1$ and consequently

$$(p) = \prod_{i=1}^{n} \sigma_i(\mathbf{p}),$$

where all factors on the right-hand side are distinct. Now, if

$$\prod_{i=1}^{n} \sigma_i(\gamma)^{a_i} \in \mathbb{Q}$$

then we (locally) get

$$\prod_{i=1}^{n} \sigma_i(\mathbf{p})^{a_i} = \prod_{i=1}^{n} \sigma_i(\mathbf{p})^{a}$$

for some integer a. Thus $a_1 = a_2 = \ldots = a_n = a$ and γ is free. ∎

LEMMA 2. *Set*

$$A(x) = \{\gamma \in \mathcal{O}_F : \overline{|\gamma|} \le x\},$$

where $\overline{|\gamma|} = \max_{1 \le i \le n} |\sigma_i(\gamma)|$, *and*

$$B(x) = \{\gamma \in A(x) : \gamma \text{ satisfies } (3)\}.$$

Then

$$\lim_{x \to \infty} \frac{\#B(x)}{\#A(x)} = 1. \tag{4}$$

Proof. Let $D = p_1^{k_1} \ldots p_d^{k_d}$ be the prime factorization of the discriminant D. For any $\gamma \in A(x) \setminus B(x)$ we have a representation of the form

$$|N_F(\gamma)| = p_1^{l_1} \ldots p_d^{l_d} t,$$

where $(t,D)=1$ and all exponents in the prime factorization of t are greater than 1. Therefore there exist natural numbers y,z such that $t=y^2z^3$. Since $|N_F(\gamma)|\le x^n$ we surely have $y\le x^{n/2}$ and $y\le x^{n/3}$. Furthermore, for any $j=1,\ldots,d$,

$$l_j\le \frac{n}{\log p_j}\log x.$$

Thus

$$\#\{|N_F(\gamma)|\,:\,\gamma\in A(x)\setminus B(x)\}=O((\log x)^d x^{5n/6}).$$

Using a rather rough estimate

$$\#\{J\lhd \mathcal{O}_F\,:\,\mathrm{N}J=m\}=O(m^{\varepsilon})\qquad(\varepsilon>0)$$

for $\varepsilon=1/12$ we obtain

$$\#\{(\gamma)\lhd \mathcal{O}_F:\gamma\in A(x)\setminus B(x)\}=O((\log x)^d x^{11n/12}).$$

Since $\gamma\in\mathcal{O}_F$ we have

$$\sum_{i=1}^{n}\log|\sigma_i(\gamma)|=\log|N_F(\gamma)|\ge 0$$

and consequently for any $\gamma\in A(x)$,

$$-(n-1)\log x\le\log|\sigma_i(\gamma)|\le\log x. \tag{5}$$

If $\gamma_1,\gamma_2\in A(x)\setminus B(x)$ generate the same ideal then there exists a unit $\varepsilon\in\mathcal{O}_F^*$ with $\gamma_2=\gamma_1\varepsilon$. By (5) this unit surely satisfies $|\log|\sigma_i(\varepsilon)||\le n\log x$. Hence by considering the representation of the group of units as a lattice in the logarithmic space we have

$$\#\{\varepsilon\in\mathcal{O}_F^*:|\log|\sigma_i(\varepsilon)||\le n\log x,\ 1\le i\le n\}=O((\log x)^{r_1+r_2-1}),$$

where r_1 is the number of real embeddings and r_2 the number of pairs of conjugate complex embeddings of F. This finally gives

$$\#(A(x)\setminus B(x))=O((\log x)^{d+r_1+r_2-1}x^{11n/12})=o(x^n).$$

This proves (4) since $\#A(x)\sim cx^n$ for some constant $c>0$. ∎

As an immediate corollary of Lemmata 1 and 2 we obtain

Theorem 2. *In any finite normal extension $F/\mathbb{Q}$ almost all algebraic integers are free.*

3. Abelian case.

3. Abelian case. The following lemma provides a natural generalization of the well-known computation of the cyclic determinant and was originally due to Dedekind (see [4]). The computation of the rank is an analogue of a theorem by A. Schinzel concerning the rank of a cyclic matrix ([3]).

LEMMA 3. *Let G be a finite abelian group and K a field satisfying* $(|G|, \mathrm{char}(K)) = 1$. *For any sequence $(a_\sigma)_{\sigma\in G}$ of elements of K we have*

$$\det(a_{\sigma\tau})_{\sigma,\tau\in G} = \pm \prod_{\chi\in\hat{G}} \Big(\sum_{\sigma\in G} \chi(\sigma)a_\sigma\Big), \tag{6}$$

where $\widehat{G}$ denotes the dual group of G. Moreover,

$$\mathrm{rank}(a_{\sigma\tau})_{\sigma,\tau\in G} = \#\Big\{\chi \in \widehat{G} : \sum_{\sigma\in G} \chi(\sigma)a_\sigma \neq 0\Big\}. \tag{7}$$

Proof. Consider the matrix

$$(b_{\chi,\tau})_{\chi\in\hat{G},\tau\in G} = (\chi(\sigma))_{\chi\in\hat{G},\sigma\in G} \cdot (a_{\sigma\tau})_{\sigma,\tau\in G}.$$

Since

$$b_{\chi,\tau} = \sum_{\sigma\in G} \chi(\sigma)a_{\sigma\tau} = \chi(\tau^{-1}) \sum_{\sigma\in G} \chi(\sigma)a_\sigma$$

and the matrix $(\chi(\sigma))_{\chi\in\hat{G},\sigma\in G}$ is non-singular, (6) and (7) follow directly. ∎

LEMMA 4. *For any extension M/N of algebraic number fields the group*

$$T = \{\alpha \in M^* : \text{there exists } t \in \mathbb{N} \text{ such that } \alpha^t \in N^*\}/N^* \tag{8}$$

is finite.

Proof. We can assume that M/N is normal. If $\alpha^t \in N^*$ then denoting $(\alpha) = \prod_{\mathbf{p}} \mathbf{p}^{a(\mathbf{p})}$ we have $a(\sigma\mathbf{p}) = a(\mathbf{p})$ for any $\sigma \in \mathrm{Gal}(M/N)$. Hence we can write

$$(\alpha) = I\mathcal{O}_M \cdot \prod_{e(\mathbf{p})>1} \mathbf{p}^{a(\mathbf{p})}$$

with a fractional ideal I in N. Let us now fix representatives $I_1, \ldots, I_h$ of all ideal classes in N. With an appropriate choice of j we obtain

$$(\alpha) = (\beta)\mathcal{O}_M \cdot I_j\mathcal{O}_M \cdot \prod_{e(\mathbf{p})>1} \mathbf{p}^{a(\mathbf{p})}$$

with $\beta \in N^*$ and hence $\alpha = \beta\gamma$, where $\gamma \in M^*$ is an S-unit for S large enough and chosen independently of α. Therefore the group T is finitely generated and hence finite. ∎

The main result of this paper is the following theorem.

THEOREM 3. *Let $F/\mathbb{Q}$ be a finite abelian extension with Galois group G and for any subfield E of F let $\mathcal{R}(E)$ denote the group of $\alpha \in E^*$ satisfying the multiplicative relation*

$$\prod_{\sigma\in G} \sigma(\alpha)^{a_\sigma} = 1, \tag{9}$$

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

• *If* $\det(a_{\sigma\tau})_{\sigma,\tau\in G} \neq 0$ *then* $\mathcal{R}(F)$ *is a finite group* (*containing only roots of unity*).

• *If* $\det(a_{\sigma\tau})_{\sigma,\tau\in G} = 0$ *then* $\mathcal{R}(F)$ *is infinitely generated. More precisely*, *set*

$$\mathcal{H} = \Big\{\chi \in \widehat{G} : \sum_{\sigma\in G} \chi(\sigma)a_\sigma = 0\Big\},$$

$$H = \{\sigma \in G : \chi(\sigma) = 1 \text{ for all } \chi \in \mathcal{H}\}.$$

Then the factor group $\mathcal{R}(F^H)/\mathcal{R}(E)$ *has infinite rank for any proper subfield* E *of* F^H (*the fixed field of* H) *whereas* $\mathcal{R}(F)/\mathcal{R}(F^H)$ *is finite with exponent dividing* w, *the number of roots of unity in* F.

Remark 1. The link between multiplicative relations connecting conjugate algebraic numbers and group determinants was earlier pointed out in [8] but, as mentioned above, a little bit different problem was tackled there.

Remark 2. 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 3. Theorem 3 suggests introducing the following distinction. If $\alpha \in \mathcal{R}(F)$ and if $\deg_{\mathbb{Q}} \alpha^k = \deg_{\mathbb{Q}} \alpha$ for all $k \in \mathbb{N}$ then α is called a *strong solution*, otherwise a *weak solution*. Using this terminology the main assertion of Theorem 3 (combined with Remark 2) is that all strong solutions are contained in F^H and that the free subgroup $\mathcal{U}$ of $\mathcal{R}(F^H)$ mentioned in Remark 2 contains only strong solutions α with $\deg_{\mathbb{Q}} \alpha = [F^H : \mathbb{Q}]$ with the only exception $\alpha = 1$.

Proof of Theorem 3. The proof of the first part is essentially contained in [8]; cf. also the end of the proof of Proposition 3 in [3].

In order to prove the second part consider the group ring $\mathbb{Z}[G]$ and set

$$R = \sum_{\sigma\in G} a_\sigma \sigma \in \mathbb{Z}[G].$$

Furthermore, for any subgroup K of G set

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

where the group ring $\mathbb{C}[G/K]$ is considered as a $\mathbb{Z}[G]$-module via $\sigma \cdot \tau K = (\sigma\tau)K$. If

$$L = \sum_{\tau\in G/K} x_\tau \tau \qquad (x_\tau \in \mathbb{C})$$

then $R \cdot L = 0$ is equivalent to the linear system

$$(x_{\tau^{-1}})_{\tau\in G/K} \cdot (a^{(K)}_{\tau\varrho})_{\tau,\varrho\in G/K} = (0),$$

in which $a^{(K)}_{\tau\varrho} = \sum_{\sigma\in\tau\varrho} a_\sigma$. By Lemma 3 we obtain

$$V(K) = \operatorname{lin}_{\mathbb{C}}\Big\{\sum_{\tau\in G/K}\chi^{(K)}(\tau)\tau : \chi^{(K)}\in\mathcal{H}^{(K)}\Big\}, \tag{10}$$

where

$$\mathcal{H}^{(K)} = \Big\{\chi^{(K)}\in\widehat{G/K} : \sum_{\tau\in G/K}\chi^{(K)}(\tau)a^{(K)}_\tau = 0\Big\}.$$

Every character $\chi^{(K)}$ of G/K can be uniquely lifted to a character χ of G that is trivial on K. It is easy to verify that

$$\sum_{\tau\in G/K}\chi^{(K)}(\tau)a^{(K)}_\tau = \sum_{\sigma\in G}\chi(\sigma)a_\sigma$$

and therefore the lifted character χ is in H if $\chi^{(K)}\in\mathcal{H}^{(K)}$. Next we will prove that

$$\sigma\cdot L = L \quad \text{for all } \sigma\in H \text{ and } L\in V(K). \tag{11}$$

By (10) this follows from

$$\sigma\cdot\sum_{\tau\in G/K}\chi^{(K)}(\tau)\tau = \chi(\sigma^{-1})\sum_{\tau\in G/K}\chi^{(K)}(\sigma\tau)\sigma\tau = \chi(\sigma^{-1})\,L$$

and from the definition of H.

Now fix $\alpha\in F$ 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 $L(\mathbf{p})\in\mathbb{Z}[G/K(\mathbf{p})]$, 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,

$$R\cdot L(\mathbf{p}) = 0 \quad (\text{in } \mathbb{Z}[G/K(\mathbf{p})]).$$

Therefore $L(\mathbf{p})\in V(K(\mathbf{p}))$ and by (11),

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

and hence

$$(\alpha)^\sigma = (\alpha) \quad \text{for all } \sigma\in H, \tag{12}$$

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 $\varepsilon\in\mathcal{O}_F^*$. All three numbers in the above equation are elements of $\mathcal{R}(F)$ and $N_{F/F^H}(\alpha)$ belongs even to $\mathcal{R}(F^H)$. 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 $\varepsilon^k \in \mathcal{O}_{F^+}^*$.

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

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

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

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

it follows that $R \cdot L = a \cdot N_{G/K}$ for some integer a, where $N_{G/K} = \sum_{\tau \in G/K} \tau$. If $\sum_{\sigma \in G} a_\sigma = 0$ then $L \in V(K)$, and if $\sum_{\sigma \in G} a_\sigma = A \ne 0$ then

$$L = \frac{a}{A} N_{G/K} + L', \quad \text{where } L' \in V(K).$$

In both cases we can conclude that (11) is still satisfied. Hence $\varepsilon^{km} \in \mathcal{O}_{F^H}^*$ and denoting $t = hkm$ we obtain $\alpha^t \in F^H$. Since $\mathcal{R}(F)/\mathcal{R}(F^H)$ can be embedded in (8) Lemma 4 implies its finiteness. By (12) 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.

For the rest of the proof we preserve our earlier notation, but specify it for $K = \{\mathrm{id}\}$ and therefore suppress any indices connected with K. For any $\sigma \in G \setminus H$ define

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

Assume for a moment that there exists $\sigma \in G \setminus H$ satisfying $V_\sigma = V$. By (10) we would have in particular

$$\sum_{\tau \in G} \chi(\tau)\tau = \sum_{\tau \in G} \chi(\tau)\sigma\tau$$

and hence $\chi(\sigma) = 1$ for any $\chi \in \mathcal{H}$, which contradicts the choice of σ. So we have proved

$$\dim_{\mathbb{C}} V_\sigma < \dim_{\mathbb{C}} V = \#\mathcal{H} \quad \text{for all } \sigma \in G \setminus H.$$

But by a standard linear algebra argument and by Lemma 3,

$$\dim_{\mathbb{Z}}(V \cap \mathbb{Z}[G]) = \#\mathcal{H},$$

and therefore the set

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

contains non-zero elements. Choose one of them and denote it by L. Now take a free algebraic integer γ and define $\alpha = \alpha(\gamma) = \gamma^L$. Obviously α satisfies (9) by the definition of $V(K)$ and $\alpha \in F^H$ by property (11). Furthermore,

$$(13) \qquad (1-\sigma) \cdot L \neq 0 \quad \text{for all } \sigma \in G \setminus H$$

by the choice of L. Since γ is free and

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

we have $\alpha^{1-\sigma} = \gamma^{(1-\sigma)\cdot L} \notin \mathbb{Q}$. In particular, $\alpha \neq \alpha^\sigma$ for any $\sigma \in G \setminus H$. This proves that $\mathbb{Q}(\alpha) = F^H$.

In a standard way we construct an infinite sequence $\gamma_j \in \mathcal{O}_F$ satisfying (3) such that their norms are pairwise relatively prime and set $\alpha_j = \gamma_j^L$. Let E be a proper subfield of F^H. As in Lemma 1 define $(\gamma_j) = \mathbf{p}_j I_j$. Suppose that $\prod_j \alpha_j^{k_j} \in E$ with some $k_j \neq 0$. Then there exists $\sigma \in G \setminus H$ such that $\mathbf{p}_j^{k_j \sigma L} = \mathbf{p}_j^{k_j L}$ and hence $(1-\sigma) \cdot L = 0$, contrary to (13). This finishes the proof of Theorem 3. ∎

4. Applications. The aim of this section is to provide a complete description of relations of length 3,

$$(14) \qquad x_1^a x_2^b x_3^c = 1 \quad (a, b, c \in \mathbb{Z} \setminus \{0\}),$$

between distinct roots of irreducible polynomials with abelian splitting field. Essentially we prove that (under the assumption $|a| \leq |b| \leq |c|$) (14) has a solution if and only if

$$|a| = |b| = |c| \quad \text{or} \quad |a| + |b| = |c|.$$

The statement of Theorem 4, which contains Theorem 1 as a special case, is much more precise and takes into account the degree of the solutions. Case 2 of Theorem 4 seems not to be as satisfactory as Case 1. But the example given in Remark 4 indicates that we cannot expect much more in general. Furthermore, this example provides solutions in the case $|a| + |b| = |c|$.

THEOREM 4. *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree n with abelian Galois group G.*

Case 1: $a \pm b \pm c \neq 0$ *for any choice of signs.*

- $a = b = -c$: *If $6 \nmid n$ and if $f(x)$ is non-cyclotomic then no three distinct roots x_1, x_2, x_3 of $f(x)$ satisfy* (14).

If $6\,|\,n$ then using a proper Tschirnhausen transformation one can obtain from $f(x)$ an irreducible non-cyclotomic polynomial $f^*(x)$ having three distinct roots x_1^*, x_2^*, x_3^* satisfying (14). *Moreover*,

$$\deg_{\mathbb{Q}}\,(x_1^*)^k = n \quad \textit{for any } k \in \mathbb{N}.$$

- *$a = b = c$: The same assertion as in the case $a = b = -c$ holds but* 6 *must be replaced by* 3.
- *$|a| \neq |b|$ or $|a| \neq |c|$ or $|b| \neq |c|$: If $f(x)$ is non-cyclotomic then no three distinct roots x_1, x_2, x_3 of $f(x)$ satisfy* (14).

Case 2: *$a \pm b \pm c = 0$ for a certain choice of signs.*

- *$a + b + c \neq 0$ and $2 \nmid n$: If $f(x)$ is non-cyclotomic then no three distinct roots x_1, x_2, x_3 of $f(x)$ satisfy* (14).
- *$a + b + c = 0$ and $w < h$, where*

$$h = \min_{\sigma \neq \tau \in G \setminus \{\mathrm{id}\}} \#\langle \sigma, \tau \rangle \tag{15}$$

and w is the number of roots of unity contained in the splitting field of $f(x)$. Then no three distinct roots of $f(x)$ satisfy (14).

- *Remaining cases*: *If three distinct roots x_1, x_2, x_3 of $f(x)$ satisfy* (14), *then the numbers $x_1, x_2^{\pm 1}, x_3^{\pm 1}$ differ multiplicatively by roots of unity and the signs at the exponents of x_2, x_3 are identical with the signs in front of b, c in the vanishing sum $a \pm b \pm c = 0$. In particular*,

$$\deg_{\mathbb{Q}} x_1^w < n.$$

Remark 4. It should be mentioned that our approach is solely based on algebraic considerations. However, the last assertion of Theorem 4 does not hold only in the case of abelian splitting fields. It can be generally proved by a slight modification of the geometric argument of [9, Lemma 1]. The following example will show that it cannot be improved, even in the abelian case. (We will consider the case $a+b+c = 0$. The other cases can be treated similarly.)

Let $F = \mathbb{Q}(\varepsilon_p)$, where ε_p is primitive pth root of unity and p a prime sufficiently large. Now choose k, l with $p \nmid kl(k - l)$ and

$$p \,|\, a + kb + lc.$$

Then ε_p satisfies (17) where σ, τ are defined by $\sigma(\varepsilon_p) = \varepsilon_p^k$ and $\tau(\varepsilon_p) = \varepsilon_p^l$. Now take any $\beta \in \mathcal{R}(F^H)$ (where $H = \langle \sigma, \tau \rangle$) satisfying

$$F^H = \mathbb{Q}(\beta^k) \quad \text{for any } k \in \mathbb{N}$$

and set

$$f(x) = \prod_{\varrho \in G} (x - \varrho(\beta\varepsilon_p)).$$

From $\beta^w \in \mathbb{Q}(\beta\varepsilon_p)$ and $\mathbb{Q}(\beta^w) = \mathbb{Q}(\beta)$ it follows that $\beta \in \mathbb{Q}(\beta\varepsilon_p)$ and finally $\varepsilon_p \in \mathbb{Q}(\beta\varepsilon_p)$. Hence $f(x)$ is irreducible and obviously $\beta\varepsilon_p \in \mathcal{R}(F)$. ■

Proof of Theorem 4. Case 1. First we consider the case $a = b = -c$. If (14) holds and if $f(x)$ is non-cyclotomic then by Theorem 3 and Lemma 3 there exist $\chi \in \widehat{G}$ and σ_1, σ_2, $\sigma_3 \in G$ such that

$$\chi(\sigma_1) + \chi(\sigma_2) = \chi(\sigma_3).$$

One of the numbers $\chi(\sigma_2\sigma_1^{-1})$, $\chi(\sigma_3\sigma_1^{-1})$ must be a 6-th primitive root of unity, whence $6 \mid n = |G|$.

Let

$$G = \prod_{j=1}^{r} \langle \tau_j \rangle$$

be the second decomposition of G, i.e. the above product is direct and

$$\operatorname{ord} \tau_j \mid \operatorname{ord} \tau_{j+1} \quad \text{for } j = 1, \ldots, r-1.$$

Since $6 \mid \operatorname{ord} \tau_r$ we can define

$$\sigma_1 = \mathrm{id}, \qquad \sigma_2 = \tau_r^{\frac{1}{3}\operatorname{ord}\tau_r}, \qquad \sigma_3 = \tau_r^{\frac{1}{6}\operatorname{ord}\tau_r}$$

and the remaining elements of G can be ordered arbitrarily.

We apply Theorem 3 to the relation

$$\sigma_1(\alpha)^a \cdot \sigma_2(\alpha)^a \cdot \sigma_3(\alpha)^{-a} = 1. \tag{16}$$

All characters $\chi \in \widehat{G}$ satisfying

$$\chi(\tau_r) = \exp\left(\frac{2\pi i}{\operatorname{ord}\tau_r}\right)$$

are contained in $\mathcal{H}$ and therefore $H = \{\mathrm{id}\}$. Hence we can choose $\alpha \in F$ satisfying (16) and $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^k) = F$ for any $k \in \mathbb{N}$. Therefore the irreducible polynomial

$$f^*(x) = \prod_{i=1}^{n} (x - \sigma_i(\alpha))$$

has three distinct roots x_1^*, x_2^*, x_3^* satisfying (14).

The proof in the case $a = b = c$ is essentially the same.

In the remaining cases it follows from [5] (see also [7, Theorem 4]) that

$$a\chi(\sigma_1) + b\chi(\sigma_2) + c\chi(\sigma_3) \neq 0.$$

Hence the first part of Theorem 3 applies.

Case 2. Assume that there exist non-trivial distinct $\sigma, \tau \in G$ and $\alpha \in F$ such that $F = \mathbb{Q}(\alpha)$ and

$$\alpha^{a\cdot\mathrm{id} + b\sigma + c\tau} = 1. \tag{17}$$

If $\chi \in \mathcal{H}$ then $\chi(\sigma), \chi(\tau) \in \{-1, 1\}$. Furthermore, since $a \pm b \pm c = 0$ holds for a unique choice of signs we see that both $\chi(\sigma)$ and $\chi(\tau)$ are independent of $\chi \in \mathcal{H}$.

If $a + b + c \neq 0$ then $\chi(\sigma) = -1$ or $\chi(\tau) = -1$ and hence $2 \mid n$. Therefore there are no relations for odd n.

Next observe that in the case $a + b + c = 0$ we have $\sigma, \tau \in H$ and therefore $[F : F^H] = \# H \geq h$. If $\alpha \in \mathcal{R}(F)$ then $\alpha^w \in F^H$ and hence $[F : F^H] = [F^H(\alpha) : F^H] \leq w$, which contradicts the assumption $w < h$.

In order to prove the last part note that always

$$\{\mathrm{id}, \sigma, \tau, \sigma\tau, \sigma\tau^3\} \cap H \neq \{\mathrm{id}\}.$$

Thus $H \neq \{\mathrm{id}\}$ and it follows from Theorem 3 that

$$\alpha^w, \alpha^{\sigma w}, \alpha^{\tau w} \in F^H \subset F$$

and $F^H \neq F$. If $\alpha^w, \alpha^{\sigma w}, \alpha^{\tau w}$ are pairwise distinct we can repeat the same reasoning and obtain

$$\alpha^{w w_1}, \alpha^{\sigma w w_1}, \alpha^{\tau w w_1} \in E,$$

where w_1 is the number of roots of unity in an appropriate field E which is strictly contained in F^H. Consequently, there exists a natural number W such that $\alpha^{\varrho W} = \alpha^{\nu W}$ with $\varrho, \nu \in \{\mathrm{id}, \sigma, \tau\}$. Since the ratio $\alpha^{\varrho}/\alpha^{\nu}$ is a root of unity we already get $\alpha^{\varrho w} = \alpha^{\nu w}$.

Now suppose that $a + b + c = 0$. Then it follows from (17) that the third conjugate differs from the first two by a root of unity. Next, consider the case $a + b - c = 0$. Then $\{\varrho, \nu\} = \{\mathrm{id}, \sigma\}$. Otherwise $f(x)$ would be a cyclotomic polynomial since there are no non-trivial relations of length 2 (see [2]). Hence $\alpha^{-\tau}$ differs from α by a root of unity. The other cases can be treated similarly. This proves the last assertion of Theorem 4. ∎

Remark 5. Basically it is possible to extend the preceding classification to describe all relations up to length 9 using the results of [1]. ∎

Acknowledgements. The authors want to thank an anonymous referee for pointing out reference [8] and for some useful remarks improving our presentation.

References

[1] J. H. Conway and A. J. Jones, *Trigonometric diophantine equations* (*On vanishing sums of roots of unity*), Acta Arith. 30 (1976), 229–240.

[2] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, ibid. 34 (1979), 391–401.

[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, and Teubner, Stuttgart, 1991, 127–135.

[4] T. Hawkins, *The origins of the theory of group characters*, Arch. Hist. Exact Sci. 7 (1971), 142–170.

[5] H. B. Mann, *On linear relations between roots of unity*, Mathematika 12 (1965), 107–117.

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

[7] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. 11 (1965), 1–34.

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

[9] —, *Conjugate algebraic numbers on conics*, Acta Arith. 40 (1982), 333–346.

DEPARTMENT OF ALGEBRA
AND DISCRETE MATHEMATICS
TECHNICAL UNIVERSITY OF VIENNA
WIEDNER HAUPTSTRASSE 8-10
A-1040 VIENNA, AUSTRIA
E-mail:MDRMOTA@ECX.TUWIEN.AC.AT

INSTITUTE OF MATHEMATICS
WARSAW UNIVERSITY
BANACHA 2
02-097 WARSZAWA, POLAND

Received on 28.3.1994
and in revised form on 14.9.1994 (2588)