Relations between Polynomial Roots

Michael Drmota and Mariusz Skałba[1]

August 21, 2000

Abstract

This paper deals with multiplicative relations for roots of rational polynomials. In general it turns out that such relations are rare. In the case of abelian splitting fields a "classification" of those relations which may appear is provided. For example, there only exist irreducible polynomials such that one root is the product of two other roots if the degree is a multiple of 6.

1 Introduction

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

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

A. Schinzel (Warsaw) 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 multipliciative relations between distinct polynomial roots are very rare. In section 3 we restrict to the case of abelian Galois group and give a kind of classification. Especially we can settle Browkin's question completely in the abelian case.

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

- *If $6 \nmid n$ then $x_1 x_2 \neq x_3$ for any three roots x_1, x_2, x_3 of $f(x)$.*

[1]This work was supported by the Austrian Science Foundation, grant Nr. M 0038–PHY.

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

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

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

which have solutions in (non necessary 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 $F/\mathbf{Q}$ be a finite normal extension of $\mathbf{Q}$ with Galois group $G = \{\sigma_1, \ldots, \sigma_n\}$. A number $\gamma \in F^*$ will be called *free* if

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

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

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*

$$p|N_F(\gamma) \quad \textit{and} \quad p \not| \frac{N_F(\gamma)}{p} D, \tag{3}$$

where D *is the discriminant of* F*.Then* γ *is free.*

PROOF. Let

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

such that $\mathrm{N}\mathbf{p} = p$ 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

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

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 $a_1 = a_2 = \cdots a_n = a$ and γ is free. □

Lemma 2 *Set*

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

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. If $\gamma \in A(x) \setminus B(x)$ and $(N_F(\gamma), D) = 1$ then there are positive integers y, z such that

$$|N_F(\gamma)| = y^2 z^3.$$

From this and

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

we obtain the rather rough estimate

$$\#\{(\gamma) \lhd \mathcal{O}_F \,:\, \gamma \in A(x) \setminus B(x), (N_F(\gamma), D) = 1\} = O\left(x^{\frac{11}{12}n}\right).$$

Taking into accout units gives

$$\#\{\gamma \in A(x) \setminus B(x) \,:\, (N_F(\gamma), D) = 1\} = O\left((\log x)^n x^{\frac{11}{12}n}\right)$$

and finally

$$\#\left(A(x) \setminus B(x)\right) = O\left((\log x)^M x^{\frac{11}{12}n}\right) = o(x^n).$$

This proves (4) since

$$\#A(x) \sim cx^n$$

for some constant $c > 0$. $\square$

As an immediate corollary of Lemmata 1 and 2 we obtain

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

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 **??**). The computation of the rank is an analogon of a theorem by A. Schinzel concerning the rank of a cyclic marix ([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*

$$\det(a_{\sigma\tau})_{\sigma,\tau\in G} = \pm \prod_{\chi\in\hat{G}} \left(\sum_{\sigma\in G} \chi(\sigma) a_\sigma \right), \tag{5}$$

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

$$\mathrm{rank}(a_{\sigma\tau})_{\sigma,\tau\in G} = \# \left\{ \chi \in \hat{G} \; : \; \sum_{\sigma\in G} \chi(\sigma) a_\sigma \neq 0 \right\}. \tag{6}$$

PROOF. Let us 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 (5) and (6) follow directly. □.

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

$$T = \{\alpha \in M^* \; : \; \textit{there exists } t \in \mathbf{N} \textit{ such that } \alpha^t \in N^*\}/N^* \tag{7}$$

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 $\sigma \in Gal(M/N)$. 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 fix now representants $I_1, \ldots, I_h$ of all ideal classes in N. With an appropriate choise 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

$$\alpha = \beta \cdot \gamma$$

where $\gamma \in M^*$ is an S-unit for S big enough and chosen independently from α. Therefore the group T is finitely generated and hence finite. □

The main result of this paper is the following theorem.

Theorem 3 *Let $F/\mathbf{Q}$ 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*

$$\prod_{\sigma\in G} \sigma(\alpha)^{a_\sigma} = 1, \tag{8}$$

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*

$$\begin{aligned} \mathcal{H} &= \left\{ \chi \in \hat{G} \,:\, \sum_{\sigma\in G} \chi(\sigma) a_\sigma = 0 \right\} \quad \textit{and} \\ H &= \left\{ \sigma \in G \,:\, \chi(\sigma) = 1 \text{ for all } \chi \in \mathcal{H} \right\}. \end{aligned}$$

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

Proof. The proof of the first part is essentially the same as the end of the proof of Proposition 3 in [3].

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

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

Furthermore, for any subgroup K of G set

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

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

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

then $R \cdot L = 0$ is equivalent with the following linear system:

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

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

$$V(K) = \mathrm{lin}_{\mathbf{C}} \left\{ \sum_{\tau\in G/K} \chi^{(K)}(\tau)\tau \ :\ \chi^{(K)} \in \mathcal{H}^{(K)} \right\}, \tag{9}$$

where

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

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

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

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

$$\sigma\cdot L = L \quad \text{for all } \sigma\in H \text{ and } L\in V(K). \tag{10}$$

By (9) 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 let us fix a number $\alpha\in F$ satisfying (8) 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 (8) it follows from the unique factorization of fractional ideals that for any $\mathbf{p}$ in the above product

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

Therefore $L(\mathbf{p}) \in V(K(\mathbf{p}))$ and by (10)

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

and hence

$$(\alpha)^\sigma = (\alpha) \quad \text{for all } \sigma\in H, \tag{11}$$

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

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

with $L \in \mathbf{Z}[G/K]$. Since $\varepsilon^{km} \in \mathcal{R}(F^+)$ 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 $\sum_{\sigma \in G} a_\sigma = A \neq 0$ then

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

where

$$L' \in V(K).$$

In both cases we can conclude that (10) 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 (7) Lemma 4 implies its finiteness. By (11) 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 miss 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 (9) 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

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

But by a standard linear algebra argument and by Lemma 3

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

and therefore the set

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

contains non-zero elements. Choose one of them and denote it by L. Now take a free algebraic integer γ and define

$$\alpha = \alpha(\gamma) = \gamma^L.$$

Obviously α satisfies (8) by the definition of $V(K)$ and $\alpha \in F^H$ by property (10). 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

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

we have

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

In particular we have

$$\alpha \neq \alpha^\sigma$$

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

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

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 denote $(\gamma_j) = \mathbf{p}_j I_j$. Suppose that

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

with certain $k_j \neq 0$. 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 $(1-\sigma)L = 0$ in contradiction to (12). This finishes the proof of Theorem 3. □

4 Applications

The following theorem provides a complete description of relations of length 3

$$x_1^a x_2^b x_3^c = 1 \qquad (a,b,c \in \mathbf{Z} \setminus \{0\}) \tag{13}$$

for roots of polynomials with abelian splitting field. It contains Theorem 1 as a special case.

Theorem 4 *Let $f(x) \in \mathbf{Q}[x]$ be an irreducible non-cyclotomic polynomial of degree n with abelian Galois group G.*
Case 1: $a \mp b \mp c \neq 0$ for any choise of signs.

- *$a = b = -c$:*
  If $6 \not| n$ then no three distinct roots x_1, x_2, x_3 of $f(x)$ satisfy (13).
  If $6|n$ then using a proper Tschirnhausen transformation one can obtain from $f(x)$ an irrducible polynomial $f^*(x)$ having three distinct roots x_1^*, x_2^*, x_3^* satisfying (13) and moreover

  $$\deg_{\mathbf{Q}} x_1^k = n$$

  for any $k \in \mathrm{N}$.

- *$a = b = c$:*
  The same assertion as in the above case but 6 should be replased by 3. If $3 \not| n$ then no three distinct roots x_1, x_2, x_3 of $f(x)$ satisfy (13).

If $3|n$ then using a proper Tschirnhausen transformation one can obtain from $f(x)$ an irrducible polynomial $f^*(x)$ having three distinct roots x_1^*, x_2^*, x_3^* satisfying (13)and moreover

$$\deg_{\mathbf{Q}} x_1^k = n$$

for any $k \in \mathrm{N}$.

- *In other cases no three distinct roots x_1, x_2, x_3 of $f(x)$ satisfy (13).*

Case 2: $a \mp b \mp c = 0$ for a certain choise of signs.
Then, if three distinct roots x_1, x_2, x_3 of $f(x)$ satisfy (13), then the numbers

$$x_1, x_2^{\mp 1}, x_3^{\mp 1}$$

differ multiplicatively by roots of unity and the signs by the exponents of x_2, x_3 are identical with the signs standing in front of (respectively) b, c in the vanishing sum $a \mp b \mp c = 0$.
In particular

$$\deg_{\mathbf{Q}} x_1^w < n$$

where w is the number of roots of unity contained in the splitting field of $f(x)$.

If additionaly

$$w < h \tag{14}$$

where

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

then no three distinct roots of $f(x)$ satisfy (13).

Remark 2. Note that h defined in (15) is always greater than 2. Hence, if $w = 2$ then (14) is satisfied. For example, if $f(x)$ has a real root then $w = 2$. (But this case can be proved direclty without using Theorem 3)

On the other hand there are many examples of irreducibel non-cyclotomic $f(x) \in \mathbf{Q}[x]$ having (comlex) distinct roots satisfying (13). For example, consider the cyclotomic field $F = \mathbf{Q}(\varepsilon_p)$ with p a prime big enough. Now choose k, l with $p \not| kl(k-l)$ 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

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

and set

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

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

PROOF. Case 1. First we consider the case $a = b = -c$. If (13) holds and if $f(x)$ is non-cyclotomic then by Theorem 3 and Lemma 3 there exist $\chi \in \hat{G}$ and $\sigma_1, \sigma_2, \sigma_3 \in G$ 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 $6|n = |G|$.

Let

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

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

$$\mathrm{ord}\ \tau_j \,|\, \mathrm{ord}\ \tau_{j+1} \quad \text{for } j = 1, \dots, r-1$$

Since $6|\mathrm{ord}\ \tau_r$ we can define

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

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 $\chi \in \hat{G}$ satisfying

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

are contained in $\mathcal{H}$ and therefore $H = \{\mathrm{id}\}$. Hence we can choose $\alpha \in F$ satisfying (16) and

$$\mathbf{Q}(\alpha) = \mathbf{Q}(\alpha^k) = F$$

for any $k \in \mathrm{N}$. Therefore the irreducibel polynomial

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

has three distinct roots x_1^*, x_2^*, x_3^* satisfying (13).

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

In the remaining cases, in which $a + b + c \neq 0$, 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 $F = Q(\alpha)$ and

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

From the assumption it follows that for any $\chi \in \mathcal{H}$

$$\chi(\sigma), \chi(\tau) \in \{-1, 1\}$$

and because only for a unique choise of signs $a \mp b \mp c = 0$ we obtain that both $\chi(\sigma)$ and $\chi(\tau)$ are constants as χ runs through $\mathcal{H}$. It implies that

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

hence $H \neq \{id\}$. From Theorem 3 it follows that

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

but $F^H \neq F$. If all three above numbers are pairwise distinct we can repeat the same reasoning and to obtain

$$\alpha^{ww_1}, \alpha^{\sigma ww_1}, \alpha^{\tau ww_1} \in E$$

with w_1 - the number of roots of unity in an appropriate field E, stricly contained in F^H. It implies that there exists a natural number W such that

$$\alpha^{\rho W} = \alpha^{\nu W} \quad \text{with} \rho, \nu \in \{id, \sigma, \tau\}$$

A posteriori we receive now

$$\alpha^{\rho w} = \alpha^{\nu w}$$

which gives easy the first two parts of the assertion. To prove the last part let us observe that

$$[F : F^H] = \#H \geq h$$

On the other hand

$$\alpha^w \in F^H$$

and therefore

$$[F : F^H] = [F^H(\alpha) : F^H] \leq w$$

which contradicts the assumption $w < h$. This contradiction completes the proof of Theorem 4. □

Remark 3. Basically it is possible to extend the preceding classification to describe all relations up to length 9 using the results of [1].

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*, Acta Arith.**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; Teubner, Stuttgart, 1991, 127–135.

[4] T. Hawkins,*The origins of the theory of group characters*, Archiv. 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*,Journ. of Numb.Th. **23** (1986), 243–254.

Michael Drmota
Department of Algebra and Discrete Mathematics
Technical University of Vienna
Wiedner Hauptstrasse 8-10
A-1040 Vienna
Austria

Mariusz Skałba
Institute of Mathematics
Warsaw University
Banacha 2
02-097 Warsaw
Poland