Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
31 (2015), 207–214
www.emis.de/journals
ISSN 1786-0091

POLYNOMIALS WITH A GIVEN CYCLIC GALOIS GROUP

JIŘÍ CIHLÁŘ, JAROSLAV FUKA, AND MARTIN KUŘIL

ABSTRACT. For every natural number n such that $2n+1$ is a prime, we present an explicit monic irreducible n^{th} degree polynomial with integer coefficients whose Galois group over the field of all rational numbers is isomorphic to the cyclic group $\mathbf{Z}_n$. The discriminant of the splitting field of the presented polynomial is equal to $(2n+1)^{n-1}$.

The topic of our paper is a special case of the Inverse Galois Problem. Recall this problem: Is a finite group G realizable over the field of all rational numbers $\mathbf{Q}$? In other words, is there an extension $\mathbf{Q} \prec F$ such that $\mathrm{Gal}_{\mathbf{Q}} F \simeq G$? Note that this question only asks about the existence of an extension $\mathbf{Q} \prec F$. The second step is to construct a polynomial $f(x) \in \mathbf{Q}[x]$ whose splitting field over $\mathbf{Q}$ is F, and so whose Galois group $\mathrm{Gal}_{\mathbf{Q}} f$ is G.

Note that the Kronecker-Weber Theorem states: Every finite abelian extension of $\mathbf{Q}$ is a subfield of a cyclotomic field. So, if G is a finite abelian group, $f(x) \in \mathbf{Q}[x]$ is an irreducible polynomial whose splitting field over $\mathbf{Q}$ is F and $\mathrm{Gal}_{\mathbf{Q}} F \simeq G$, then there exists a root of unity ξ such that F is a subfield of $\mathbf{Q}(\xi)$.

We are interested in the following task: A natural number n is given. Find a monic irreducible n^{th} degree polynomial f with integer coefficients such that its Galois group over the field of all rational numbers $\mathbf{Q}$ is isomorphic to the cyclic group $\mathbf{Z}_n$, i.e. $\mathrm{Gal}_{\mathbf{Q}} f \simeq \mathbf{Z}_n$.

It is easy to see that there are infinitely many polynomials solving our task. We formulate this in our Proposition 1 below.

More interesting is to present an explicit polynomial solving our task. In our theorem we give such a presentation in the case that $2n+1$ is a prime number. Note that there exist infinitely many natural numbers n with the property $2n+1$ is a prime.

Lemma 1. *If n is a natural number then there is an irreducible polynomial $f \in \mathbf{Q}[x]$ such that f has degree n and the Galois group of f over $\mathbf{Q}$ is isomorphic to $\mathbf{Z}_n$.*

2010 *Mathematics Subject Classification.* 12F12, 11R20.
Key words and phrases. Galois group of a polynomial, discriminant of a number field.

Proof. See [1, page 187, Corollary 4.5]. □

Lemma 2. *Let*

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_2x^2 + a_1x + a_0 \in \mathbf{Q}[x].$$

For any $q \in \mathbf{Q}$, $q \neq 0$, *we put*

$$f_q(x) = x^n + qa_{n-1}x^{n-1} + q^2a_{n-2}x^{n-2} + \ldots + q^{n-1}a_1x + q^na_0.$$

Then the following holds:

(i) $Gal_{\mathbf{Q}}\, f_q = Gal_{\mathbf{Q}}\, f$

(ii) f *is irreducible if and only if* f_q *is irreducible.*

Proof. (i) It is easy to see that $f(\alpha) = 0 \iff f_q(q\alpha) = 0$, which implies that the splitting fields over $\mathbf{Q}$ of the polynomials f and f_q are the same. Consequently, $\mathrm{Gal}_{\mathbf{Q}}\, f_q = \mathrm{Gal}_{\mathbf{Q}}\, f$.

(ii) Let $f(\alpha) = f_q(q\alpha) = 0$. Then f is irreducible $\iff [\mathbf{Q}(\alpha) : \mathbf{Q}] = n$. Similarly, f_q is irreducible $\iff [\mathbf{Q}(q\alpha) : \mathbf{Q}] = n$. Since $\mathbf{Q}(\alpha) = \mathbf{Q}(q\alpha)$, we have f is irreducible if and only if f_q is irreducible.

□

Proposition 1. *Let n be a natural number. There exist infinitely many monic irreducible n^{th} degree polynomials with integer coefficients whose Galois groups over* $\mathbf{Q}$ *are isomorphic to* $\mathbf{Z}_n$.

Proof. By Lemma 1, there is an irreducible polynomial $f \in \mathbf{Q}[x]$ such that f has degree n and $\mathrm{Gal}_{\mathbf{Q}}\, f \simeq \mathbf{Z}_n$. We may assume that f is monic,

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_2x^2 + a_1x + a_0.$$

Clearly, there is a non zero integer l with the property $la_0, la_1, \ldots, la_{n-1} \in \mathbf{Z}$. For any natural number m, the polynomial f_{ml} is a monic irreducible n^{th} degree polynomial with integer coefficients whose Galois group over $\mathbf{Q}$ is isomorphic to $\mathbf{Z}_n$ (see Lemma 2). The polynomials f_{ml} are pairwise distinct because the numbers $m^nl^na_0$ are pairwise distinct (note that $a_0 \neq 0$ since f is irreducible). □

Lemma 3. *Let n, j be integers,* $0 \leq n$, $0 \leq j \leq \frac{n}{2}$. *Then*

$$\sum_{k=0}^{j} (-1)^k \binom{n-k}{k}\binom{n-2k}{j-k} = 1.$$

Proof. At first,

$$\begin{aligned}\binom{n-k}{k}\binom{n-2k}{j-k} &= \frac{(n-k)!}{k!(n-2k)!} \cdot \frac{(n-2k)!}{(j-k)!(n-k-j)!} \\ &= \frac{(n-k)!}{k!(j-k)!(n-k-j)!} \cdot \frac{j!}{j!} \\ &= \binom{j}{k}\binom{n-k}{j}.\end{aligned}$$

So, we have to prove the identity

$$\sum_{k=0}^{j}(-1)^k\binom{j}{k}\binom{n-k}{j}=1.$$

We use generating functions. Put

$$f(x)=\sum_{k=0}^{\infty}(-1)^k\binom{j}{k}x^k,\quad g(x)=\sum_{k=0}^{\infty}\binom{n-j+k}{j}x^k.$$

The jth coefficient of the product $f(x)g(x)$ is equal to $\sum_{k=0}^{j}(-1)^k\binom{j}{k}\binom{n-k}{j}$. Consequently, we would like to show that the jth coefficient of $f(x)g(x)$ is equal to 1. Clearly, $f(x)=(1-x)^j$. Further,

$$\begin{aligned}
g(x)&=\frac{1}{x^{n-2j}}\sum_{k=0}^{\infty}\frac{1}{j!}\left(x^{n-j+k}\right)^{(j)}\\
&=\frac{1}{j!}\cdot\frac{1}{x^{n-2j}}\cdot\left(x^{n-j}\sum_{k=0}^{\infty}x^k\right)^{(j)}\\
&=\frac{1}{j!}\cdot\frac{1}{x^{n-2j}}\cdot\left(x^{n-j}\cdot\frac{1}{1-x}\right)^{(j)}\\
&=\frac{1}{j!}\cdot\frac{1}{x^{n-2j}}\cdot\sum_{i=0}^{j}\binom{j}{i}\left(x^{n-j}\right)^{(i)}\left(\frac{1}{1-x}\right)^{(j-i)}\\
&=\frac{1}{j!}\cdot\frac{1}{x^{n-2j}}\cdot x^{n-j}\cdot j!\cdot\frac{1}{(1-x)^{j+1}}+\\
&\quad\frac{1}{j!}\cdot\frac{1}{x^{n-2j}}\sum_{i=1}^{j}\frac{j!}{i!(j-i)!}(n-j)\dots(n-j-i+1)x^{n-j-i}\frac{(j-i)!}{(1-x)^{j-i+1}}\\
&=\frac{x^j}{(1-x)^{j+1}}+\sum_{i=1}^{j}\binom{n-j}{i}\frac{x^{j-i}}{(1-x)^{j-i+1}}.
\end{aligned}$$

Now,

$$\begin{aligned}
f(x)g(x)&=\frac{x^j}{1-x}+\sum_{i=1}^{j}\binom{n-j}{i}x^{j-i}(1-x)^{i-1}\\
&=(x^j+x^{j+1}+x^{j+2}+\dots)+\sum_{i=1}^{j}\binom{n-j}{i}x^{j-i}(1-x)^{i-1}.
\end{aligned}$$

The polynomial $\binom{n-j}{i}x^{j-i}(1-x)^{i-1}$ has degree $j-1$, for any $i=1,2,\dots,j$. Thus the jth coefficient of the product $f(x)g(x)$ is really equal to 1. $\square$

Theorem 1. *Let n be a natural number such that $2n+1$ is a prime. Let*

$$f(x) = \sum_{0 \le k \le \frac{n}{2}} (-1)^k \binom{n-k}{k} x^{n-2k} + \sum_{0 \le k < \frac{n}{2}} (-1)^k \binom{n-k-1}{k} x^{n-2k-1}.$$

Then f is a monic irreducible nth degree polynomial with integer coefficients such that $Gal_{\mathbf{Q}} f \simeq \mathbf{Z}_n$.

Proof. Put $p = 2n+1$, $\xi = \cos\frac{2\pi}{p} + i \sin\frac{2\pi}{p}$. At first, we prove that $\mathrm{Gal}_{\mathbf{Q}} \mathbf{Q}(\xi + \frac{1}{\xi}) \simeq \mathbf{Z}_n$. The following holds (see [1, page 135, 1.24.4]):

$$\mathrm{Gal}_{\mathbf{Q}} \mathbf{Q}(\xi) \simeq \mathbf{Z}_p^{\times} \simeq \mathbf{Z}_{p-1} = \mathbf{Z}_{2n}.$$

So, $\mathrm{Gal}_{\mathbf{Q}} \mathbf{Q}(\xi)$ contains a (unique) subgroup H of index n. Let $\tau \in \mathrm{Gal}_{\mathbf{Q}} \mathbf{Q}(\xi)$, $\tau(\xi) = \xi^{p-1} = \frac{1}{\xi}$. The automorphism τ has order 2 since $\tau^2(\xi) = \tau(\tau(\xi)) = \tau(\frac{1}{\xi}) = \frac{1}{\tau(\xi)} = \xi$. So, $H = \langle \tau \rangle$. We will show that $H' = \{u \in \mathbf{Q}(\xi) | \ \tau(u) = u\} = \mathbf{Q}(\xi + \frac{1}{\xi})$. Then, by the Fundamental Theorem of Galois Theory ([1, page 129, Theorem 1.22]), $\mathbf{Q}(\xi + \frac{1}{\xi})$ is normal over $\mathbf{Q}$ and

$$\mathrm{Gal}_{\mathbf{Q}} \mathbf{Q}(\xi + \frac{1}{\xi}) \simeq \mathrm{Gal}_{\mathbf{Q}} \mathbf{Q}(\xi)/H \simeq \mathbf{Z}_n.$$

Now, we show that really $H' = \mathbf{Q}(\xi + \frac{1}{\xi})$. Since $\tau(\xi + \frac{1}{\xi}) = \tau(\xi) + \tau(\frac{1}{\xi}) = \frac{1}{\xi} + \xi$, it holds $\xi + \frac{1}{\xi} \in H'$. It gives $\mathbf{Q}(\xi + \frac{1}{\xi}) \prec H'$. Altogether,

$$\mathbf{Q} \prec \mathbf{Q}(\xi + \frac{1}{\xi}) \prec H' \prec \mathbf{Q}(\xi).$$

By the Tower Theorem ([1, page 89, Proposition 2.1]),

$$[\mathbf{Q}(\xi) : \mathbf{Q}] = [\mathbf{Q}(\xi) : H'] \cdot [H' : \mathbf{Q}] = [\mathbf{Q}(\xi) : \mathbf{Q}(\xi + \frac{1}{\xi})] \cdot [\mathbf{Q}(\xi + \frac{1}{\xi}) : \mathbf{Q}].$$

We know that $[\mathbf{Q}(\xi) : \mathbf{Q}] = 2n$. Further, by the Fundamental Theorem of Galois Theory, $[\mathbf{Q}(\xi) : H'] = (H : \langle i_{\mathbf{Q}(\xi)} \rangle) = o(H) = 2$. It remains to show that $[\mathbf{Q}(\xi) : \mathbf{Q}(\xi + \frac{1}{\xi})] = 2$. Put $g(x) = x^2 - (\xi + \frac{1}{\xi})x + 1$. Clearly, $g(x) \in \mathbf{Q}(\xi + \frac{1}{\xi})[x]$ and $g(\xi) = 0$. Suppose that $g(x)$ is reducible over $\mathbf{Q}(\xi + \frac{1}{\xi})$. Then $g(x) = (x - \alpha)(x - \beta)$, $\alpha, \beta \in \mathbf{Q}(\xi + \frac{1}{\xi})$. Thus $0 = g(\xi) = (\xi - \alpha)(\xi - \beta)$, $\xi = \alpha$ or $\xi = \beta$, $\xi \in \mathbf{Q}(\xi + \frac{1}{\xi})$. But then $\xi \in H'$, $\tau(\xi) = \xi$, $\frac{1}{\xi} = \xi$, $1 = \xi^2$. It is a contradiction. Consequently, $g(x)$ is irreducible over $\mathbf{Q}(\xi + \frac{1}{\xi})$. Remember that $g(\xi) = 0$. So, $g(x)$ is the minimal polynomial of ξ over $\mathbf{Q}(\xi + \frac{1}{\xi})$. Then $[\mathbf{Q}(\xi + \frac{1}{\xi})(\xi) : \mathbf{Q}(\xi + \frac{1}{\xi})] = \deg(g) = 2$. But $\mathbf{Q}(\xi + \frac{1}{\xi})(\xi) = \mathbf{Q}(\xi)$ which yields $[\mathbf{Q}(\xi) : \mathbf{Q}(\xi + \frac{1}{\xi})] = 2$.

Let us denote

$$u_i = \xi^i + \xi^{p-i} = \xi^i + \frac{1}{\xi^i}, i \ge 1, u_0 = 1.$$

We have

$$u_0 + u_1 + u_2 + \cdots + u_n = 0.$$

We will also use the next formulas for u_1^k which can be derived from the Binomial Theorem ($k \geq 0$):

$$\begin{aligned}
u_1^k &= \left(\xi + \frac{1}{\xi}\right)^k \\
&= \sum_{i=0}^{k} \binom{k}{i} \xi^i \left(\frac{1}{\xi}\right)^{k-i} \\
&= \sum_{i=0}^{k} \binom{k}{i} \xi^{2i-k} \\
&= \sum_{0 \leq i < \frac{k}{2}} \left(\binom{k}{i} \xi^{2i-k} + \binom{k}{k-i} \xi^{2(k-i)-k}\right) + \underbrace{\binom{k}{\frac{k}{2}} \xi^0}_{\text{for } k \text{ even}} \\
&= \sum_{0 \leq i < \frac{k}{2}} \binom{k}{i} \left(\xi^{k-2i} + \frac{1}{\xi^{k-2i}}\right) + \underbrace{\binom{k}{\frac{k}{2}} u_0}_{\text{for } k \text{ even}} \\
&= \sum_{0 \leq i < \frac{k}{2}} \binom{k}{i} u_{k-2i} + \underbrace{\binom{k}{\frac{k}{2}} u_0}_{\text{for } k \text{ even}} \\
&= \sum_{0 \leq i \leq \frac{k}{2}} \binom{k}{i} u_{k-2i}.
\end{aligned}$$

We have already shown that $[\mathbf{Q}(u_1) : \mathbf{Q}] = n$. Clearly, f is a monic nth degree polynomial with integer coefficients. Suppose that $f(u_1) = 0$. Then, since $[\mathbf{Q}(u_1) : \mathbf{Q}] = n$ and $\deg(f) = n$, f is a minimal polynomial of u_1 over $\mathbf{Q}$. So, f is irreducible. Since $\mathbf{Q}(u_1)$ is normal over $\mathbf{Q}$, $f \in \mathbf{Q}[x]$ is irreducible, $f(u_1) = 0$, it follows that $\mathbf{Q}(u_1)$ is a splitting field of the polynomial f over $\mathbf{Q}$. Thus $\mathrm{Gal}_{\mathbf{Q}} f = \mathrm{Gal}_{\mathbf{Q}} \mathbf{Q}(u_1) \simeq \mathbf{Z}_n$. We have just seen that it remains to prove the equality $f(u_1) = 0$. Let us compute:

$$\begin{aligned}
f(u_1) &= \sum_{0 \leq k \leq \frac{n}{2}} (-1)^k \binom{n-k}{k} u_1^{n-2k} + \sum_{0 \leq k < \frac{n}{2}} (-1)^k \binom{n-k-1}{k} u_1^{n-2k-1} \\
&= \sum_{0 \leq k \leq \frac{n}{2}} (-1)^k \binom{n-k}{k} \cdot \sum_{0 \leq i \leq \frac{n}{2}-k} \binom{n-2k}{i} u_{n-2k-2i} \\
&\quad + \sum_{0 \leq k < \frac{n}{2}} (-1)^k \binom{n-k-1}{k} \cdot \sum_{0 \leq i < \frac{n}{2}-k} \binom{n-2k-1}{i} u_{n-2k-1-2i}
\end{aligned}$$

$$= \sum_{0\le k\le \frac{n}{2}} \sum_{0\le i\le \frac{n}{2}-k} (-1)^k \binom{n-k}{k}\binom{n-2k}{i} u_{n-2(k+i)}$$
$$+ \sum_{0\le k< \frac{n}{2}} \sum_{0\le i< \frac{n}{2}-k} (-1)^k \binom{n-1-k}{k}\binom{n-1-2k}{i} u_{n-1-2(k+i)}.$$

Put $j = k + i$. Then

$$f(u_1) = \sum_{0\le j\le \frac{n}{2}} \sum_{k=0}^{j} (-1)^k \binom{n-k}{k}\binom{n-2k}{j-k} u_{n-2j}$$
$$+ \sum_{0\le j< \frac{n}{2}} \sum_{k=0}^{j} (-1)^k \binom{n-1-k}{k}\binom{n-1-2k}{j-k} u_{n-1-2j}$$
$$= \sum_{0\le j\le \frac{n}{2}} u_{n-2j}\cdot \sum_{k=0}^{j} (-1)^k \binom{n-k}{k}\binom{n-2k}{j-k}$$
$$+ \sum_{0\le j< \frac{n}{2}} u_{n-(2j+1)}\cdot \sum_{k=0}^{j} (-1)^k \binom{n-1-k}{k}\binom{n-1-2k}{j-k}.$$

It follows from Lemma 3 that

$$\begin{aligned} f(u_1) &= \sum_{0\le j\le \frac{n}{2}} u_{n-2j} + \sum_{0\le j< \frac{n}{2}} u_{n-(2j+1)} \\ &= u_0 + u_1 + u_2 + \cdots + u_n \\ &= 0. \end{aligned}$$

The proof of our theorem is complete. □

Problem 1. Formulate and prove analogous theorems for natural numbers n such that $kn + 1$ is a prime ($k = 3, 4, 5, \ldots$).

Remark 1. For some concrete values of n ($n = 5, 8, 9, 11$), the polynomial from the theorem can be found in the Appendix of the book [3].

At the end of our article, we would like to show that the discriminant of the splitting field (over the field of all rational numbers $\mathbf{Q}$) of the polynomial $f(x)$ from our theorem is equal to $(2n+1)^{n-1}$. For the definition of the discriminant of an algebraic number field see [2, page 176].

Recall the notation. Let n be a natural number such that $2n+1$ is a prime. We put $p = 2n + 1, \xi = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}, u_i = \xi^i + \xi^{p-i} = \xi^i + \frac{1}{\xi^i}$ $(i \ge 1)$.

Lemma 4. *Let A be the ring of all algebraic integers in $\mathbf{Q}(\xi)$. Then A is a free abelian group with basis $\{1, \xi, \ldots, \xi^{p-2}\}$.*

Proof. [4, page 82, Statement **U**]. □

Lemma 5. *$u_1, u_2, \dots, u_n$ is an integral basis for the ring D of algebraic integers in $\mathbf{Q}(\xi + \frac{1}{\xi})$.*

Proof. Let $a_1, a_2, \dots, a_n \in \mathbf{Q}, a_1u_1 + a_2u_2 + \cdots + a_nu_n = 0$. Then

$$a_1\xi + a_1\xi^{2n} + a_2\xi^2 + a_2\xi^{2n-1} + \ldots + a_n\xi^n + a_n\xi^{n+1} = 0,$$

$$a_1 + a_1\xi^{2n-1} + a_2\xi + a_2\xi^{2n-2} + \ldots + a_n\xi^{n-1} + a_n\xi^n = 0.$$

Since the minimal polynomial of ξ over $\mathbf{Q}$ is $x^{2n} + x^{2n-1} + \cdots + x + 1$, we have $a_1 = a_2 = \ldots = a_n = 0$ and the elements $u_1, u_2, \dots, u_n$ are linearly independent over $\mathbf{Q}$. As $[\mathbf{Q}(\xi + \frac{1}{\xi}) : \mathbf{Q}] = n$, we have $u_1, u_2, \dots, u_n$ is a basis for $\mathbf{Q}(\xi + \frac{1}{\xi})$ over $\mathbf{Q}$. Now, we want to show that $D = \mathbf{Z}u_1 + \mathbf{Z}u_2 + \cdots + \mathbf{Z}u_n$. Since ξ is an algebraic integer and the set of algebraic integers forms a ring, we have $u_1, u_2, \dots, u_n \in D$. So, it remains to prove the inclusion $D \subseteq \mathbf{Z}u_1 + \mathbf{Z}u_2 + \cdots + \mathbf{Z}u_n$. Let $d \in D$. There exist $b_1, b_2, \dots, b_n \in \mathbf{Q}$ such that $d = b_1u_1 + b_2u_2 + \cdots + b_nu_n$. We are going to prove that $b_1, b_2, \dots, b_n$ are integers. By Lemma 4, since clearly $D \subseteq A$, there exist integers $c_0, c_1, \dots, c_{2n-1}$ such that $d = c_0 + c_1\xi + \cdots + c_{2n-1}\xi^{2n-1}$. Recall that $1 = -\xi - \xi^2 \ldots - \xi^{2n}$. We have obtained the following expressions for d:

$$d = b_1\xi + b_1\xi^{2n} + b_2\xi^2 + b_2\xi^{2n-1} + \cdots + b_n\xi^n + b_n\xi^{n+1},$$

$$d = (c_1 - c_0)\xi + (c_2 - c_0)\xi^2 + \cdots + (c_{2n-1} - c_0)\xi^{2n-1} - c_0\xi^{2n}.$$

The elements $1, \xi, \dots, \xi^{2n-1}$ are linearly independent over $\mathbf{Q}$. Consequently, the elements $\xi, \xi^2, \dots, \xi^{2n}$ are also linearly independent over $\mathbf{Q}$. Now, we compare our two expressions for d and get the equalities

$$b_i = c_i - c_0$$

for $i = 1, 2, \dots, n$. We see that $b_1, b_2, \dots, b_n$ are integers. □

Proposition 2. *The discriminant of the splitting field of the polynomial $f(x)$ from the theorem is equal to $(2n+1)^{n-1}$.*

Proof. We have shown in the proof of the theorem that $\mathbf{Q}(\xi + \frac{1}{\xi})$ is a splitting field of the polynomial $f(x)$ over $\mathbf{Q}$. Let us denote the discriminant of $\mathbf{Q}(\xi + \frac{1}{\xi})/\mathbf{Q}$ by δ. According to the definition, in view of Lemma 5,

$$\delta = \operatorname{discr}(u_1, u_2, \dots, u_n).$$

Let $1 \le i \le 2n, \tau_i \in \operatorname{Gal}_{\mathbf{Q}} \mathbf{Q}(\xi), \tau_i(\xi) = \xi^i$. Then

$$\tau_i(u_1) = \tau_i\left(\xi + \frac{1}{\xi}\right) = \tau_i(\xi) + \frac{1}{\tau_i(\xi)} = \xi^i + \frac{1}{\xi^i} = u_i.$$

Since $f(u_1) = 0$ (see the proof of our theorem), $f(u_i) = 0$ and f is the minimal polynomial of u_i over $\mathbf{Q}$. Note that the coefficient of the polynomial f at x^{n-1} is $(-1)^0\binom{n-0-1}{0} = 1$. Thus $\operatorname{Tr}(u_i) = -1$. Let $1 \le j < i \le n$. We can compute

$$u_iu_j = \left(\xi^i + \frac{1}{\xi^i}\right)\left(\xi^j + \frac{1}{\xi^j}\right) = \xi^{i+j} + \xi^{i-j} + \frac{1}{\xi^{i-j}} + \frac{1}{\xi^{i+j}} = u_{i+j} + u_{i-j},$$

$$\mathrm{Tr}(u_i u_j) = \mathrm{Tr}(u_{i+j} + u_{i-j}) = \mathrm{Tr}(u_{i+j}) + \mathrm{Tr}(u_{i-j}) = (-1) + (-1) = -2.$$

Similarly, for $1 \leq i \leq n$,

$$u_i u_i = \left(\xi^i + \frac{1}{\xi^i}\right)\left(\xi^i + \frac{1}{\xi^i}\right) = \xi^{2i} + 1 + 1 + \frac{1}{\xi^{2i}} = u_{2i} + 2,$$

$$\mathrm{Tr}(u_i u_i) = \mathrm{Tr}(u_{2i} + 2) = \mathrm{Tr}(u_{2i}) + \mathrm{Tr}(2) = -1 + 2n.$$

The traces of elements were computed using the elementary facts mentioned in [4, pages 16-17, Paragraph 10]. Finally,

$$\delta = \det \begin{pmatrix} 2n-1 & -2 & \dots & -2 \\ -2 & 2n-1 & \dots & -2 \\ \vdots & \vdots & \ddots & \vdots \\ -2 & -2 & \dots & 2n-1 \end{pmatrix} = (2n+1)^{n-1}. \qquad \square$$

Acknowledgement

The authors thank the referee for his suggestions about the paper.

References

[1] M. H. Fenrick. *Introduction to the Galois correspondence.* Birkhäuser Boston, Inc., Boston, MA, second edition, 1998.

[2] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1990.

[3] G. Malle and B. H. Matzat. *Inverse Galois theory.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.

[4] P. Ribenboim. *Algebraic numbers.* Wiley-Interscience [A Division of John Wiley & Sons, Inc.], New York-London-Sydney, 1972. Pure and Applied Mathematics, Vol. 27.

Received November 6, 2013.

Jiří Cihlář,
Department of Mathematics,
Faculty of Science,
J. E. Purkyne University
Ceske mladeze 8
400 96 Usti nad Labem
Czech Republic
E-mail address: `jiri.cihlar@ujep.cz`

Martin Kuřil (corresponding author),
Department of Mathematics,
Faculty of Science,
J. E. Purkyne University
Ceske mladeze 8
400 96 Usti nad Labem
Czech Republic
E-mail address: `martin.kuril@ujep.cz`