DE GRUYTER
OPEN

uniform distribution theory

DOI: 10.1515/udt-2017–0017
Unif. Distrib. Theory **12** (2017), no.2, 91–117

NOTES ON THE DISTRIBUTION OF ROOTS MODULO A PRIME OF A POLYNOMIAL

Yoshiyuki Kitaoka

ABSTRACT. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ with roots $\alpha_1, \dots, \alpha_n$. We point out the importance of linear relations among $1, \alpha_1, \dots, \alpha_n$ over rationals with respect to the distribution of local roots of f modulo a prime. We formulate it as a conjectural uniform distribution in some sense, which elucidates data in previous papers.

Communicated by Shigeki Akiyama

In this note, a polynomial means always a monic one over the ring $\mathbb{Z}$ of integers and the letter p denotes a prime number, unless specified. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \tag{0}$$

be a polynomial of degree n. As in the previous papers, we put

$$\mathrm{Spl}_X(f) := \{p \le X \mid f(x) \text{ is fully splitting modulo } p\}$$

for a positive number X and $\mathrm{Spl}\,(f) := \mathrm{Spl}_\infty(f)$. In this note, we require the following conditions on the local roots $r_1, \dots, r_n\ (\in \mathbb{Z})$ of $f(x) \equiv 0 \bmod p$ for a prime $p \in \mathrm{Spl}\,(f)$:

$$f(x) \equiv \prod_{i=1}^{n}(x - r_i) \bmod p, \tag{1}$$

$$0 \le r_1 \le r_2 \le \cdots \le r_n < p. \tag{2}$$

We can determine local roots r_i uniquely with this global ordering. If f is irreducible and of $\deg(f) > 1$, and p is sufficiently large, then (2) is equivalent to $0 < r_1 < \cdots < r_n < p$. Here, we consider two types of distribution of local roots r_i of f.

2010 Mathematics Subject Classification: 11K.
Keywords: distribution, polynomial, roots modulo a prime,

Before stating them, let $\alpha_1, \ldots, \alpha_n$ be roots of a polynomial f in (0) and suppose a linear relation

$$\sum_{i=1}^{n} m_i\alpha_i = m \quad (m_i, m \in \mathbb{Q}). \tag{3}$$

Let us give three typical examples of a linear relation (3) among roots:
The first example is

$$\sum_{i=1}^{n} \alpha_i = \mathrm{tr}\,(f) \quad (:= -a_{n-1}).$$

We call a linear relation (3) trivial if $m_1 = \cdots = m_n$, otherwise non-trivial. A trivial relation is reduced to the above. We know that for an irreducible polynomial f, there is only a trivial relation if the degree n is prime or the Galois group $\mathrm{Gal}\,(\mathbb{Q}(\alpha_1, \ldots, \alpha_n)/\mathbb{Q})$ is S_n or A_n $(n \geq 6)$ as a permutation group of $\{\alpha_1, \ldots, \alpha_n\}$ (Proposition 2).
The second is a reducible polynomial

$$f(x) = g(x)h(x) \quad \text{with} \quad 1 < \deg g < \deg f.$$

There is a non-trivial relation $\sum \beta_i = \mathrm{tr}\,(g)$ for roots β_i of g, since a set of roots of g is a proper subset of roots of f.
The third is a decomposable polynomial, that is

$$f(x) = g\big(h(x)\big) \quad \text{with} \quad 1 < \deg h < \deg f.$$

For a root β of $g(x) = 0$, a set of solutions γ_i of $h(x) = \beta$ is a proper subset of roots of $f(x)$, and we have a non-trivial relation $\sum \gamma_i = \mathrm{tr}\,(h - \beta) = \mathrm{tr}(h) \in \mathbb{Z}$. Some other examples are given in [3] and in the text.

If the degree of f is less than 6, there is no non-trivial linear relation except the above two types, as shown below. In case of degree 6, other non-trivial linear relations appear.

The first subject is a kind of uniformity: Let f be a polynomial in (0) of degree n and put

$$\hat{\mathfrak{D}}_n := \{(x_1 \ldots, x_n) \in [0,1)^n \mid 0 \leq x_1 \leq \cdots \leq x_n < 1, \sum_{i=1}^{n} x_i \in \mathbb{Z}\} \tag{4}$$

and for a set $D \subset [0,1)^n$ with $D = \overline{D^\circ}$

$$\mathrm{Pr}_D(f, X) := \frac{\#\{p \in \mathrm{Spl}_X(f) \mid (r_1/p, \ldots, r_n/p) \in D\}}{\#\mathrm{Spl}_X(f)},$$

where local roots r_i satisfy properties (1), (2).
We expect, under an assumption that a polynomial f has only a trivial linear relation (3) among roots.

Expectation 1.
$$\mathrm{Pr}_D(f) := \lim_{X\to\infty} \mathrm{Pr}_D(f, X) = \frac{\mathrm{vol}\,(D \cap \hat{\mathfrak{D}}_n)}{\mathrm{vol}\,(\hat{\mathfrak{D}}_n)}. \tag{5}$$

The set $\hat{\mathfrak{D}}_n$ is parametrized by $x_1, \ldots, x_{n-1}$, since x_n equals $\lceil \sum_{i<n} x_i \rceil - \sum_{i<n} x_i$, and the volume of the projection $\mathfrak{D}_n$ of $\hat{\mathfrak{D}}_n$ to a hyperplane $\mathbb{R}^{n-1}$ defined by $x_n = 0$ is $1/n!$. Here, $\lceil x \rceil$ denotes an integer satisfying $x \le \lceil x \rceil < x + 1$ for a real number x.

In case of $\mathrm{tr}\,(f) = 0$, we may suppose that D is limited to a domain on $\hat{\mathfrak{D}}_n$ by virtue of $(r_1/p, \ldots, r_n/p) \in \hat{\mathfrak{D}}_n$, and it is easy to see that the right--hand side of (5) is $\mathrm{vol}\big(\mathrm{pr(D)}\big)/(1/\mathrm{n}!)$, where pr is a projection $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{n-1})$.

In general, a polynomial has non-trivial linear relations among roots, and suppose that a system of linear equations
$$\sum_{i=1}^{n} m_{j,i}\,\alpha_i = m_j \quad (j = 1, \ldots, t) \tag{6}$$
is a basis of all linear relations (3) restricted to $m_{j,i}, m_j \in \mathbb{Z}$. If f is irreducible, then we see $(\sum_i m_{j,i})\mathrm{tr}\,(f) = nm_j$. We fix a numbering of roots α_i of f. For a prime $p \in \mathrm{Spl}\,(f)$, there is a permutation $\sigma \in S_n$ (dependent on p) such that local roots r_i satisfy induced relations (cf. Proposition 1)
$$\sum_i m_{j,i}\, r_{\sigma(i)} \equiv m_j \bmod p \quad (1 \le {}^\forall j \le t) \tag{7}$$
which implies $\sum_i m_{j,i} \cdot r_{\sigma(i)}/p - m_j/p \in \mathbb{Z}$. Let $\boldsymbol{x} = (x_1, \ldots, x_n) \in [0,1]^n$ be an accumulation point of $(r_1/p, \ldots, r_n/p)$ with the same permutation σ above; then we see that $\boldsymbol{x}$ is in the closure of
$$\mathfrak{D}(f,\sigma) := \left\{ (x_1 \ldots, x_n) \in [0,1)^n \;\middle|\; \begin{array}{l} 0 \le x_1 \le \cdots \le x_n < 1, \\ \sum_i m_{j,i}\, x_{\sigma(i)} \in \mathbb{Z} \text{ for } 1 \le {}^\forall j \le t \end{array} \right\}.$$
If $\boldsymbol{x}$ is not in $\mathfrak{D}(f,\sigma)$, then x_n is equal to 1 and we neglect the case since we are concerned with the volume. We note that the set $\mathfrak{D}(f,\sigma)$ depends on a numbering of roots α_i and may be the same for distinct permutations.
If f has only a trivial linear relation, then $\mathfrak{D}(f,\sigma)$ is nothing but $\hat{\mathfrak{D}}_n$.

Put
$$\mathrm{Spl}_X(f,\sigma) := \{p \in \mathrm{Spl}_X(f) \mid \sum_i m_{j,i}\, r_{\sigma(i)} \equiv m_j \bmod p\,(1 \le {}^\forall j \le t)\}.$$
If $\mathrm{Spl}_\infty(f,\sigma_1) \cap \mathrm{Spl}_\infty(f,\sigma_2)$ is an infinite set, then $\mathrm{Spl}_\infty(f,\sigma_1)$ and $\mathrm{Spl}_\infty(f,\sigma_2)$ are equal except a finite set. The following is a generalization of Expectation 1.

Expectation 1′.

$$
\begin{aligned}
\mathrm{Pr}_D(f,\sigma) :&= \lim_{X\to\infty} \frac{\#\{p \in \mathrm{Spl}_X(f,\sigma) \mid (r_1/p,\ldots,r_n/p) \in D\}}{\#\mathrm{Spl}_X(f,\sigma)} \\
&= \frac{\mathrm{vol}\big(D \cap \mathfrak{D}(f,\sigma)\big)}{\mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big)}
\end{aligned} \tag{8}
$$

for a permutation σ with $\dim \mathfrak{D}(f,\sigma) = n-t$, and vol is the volume as a set of dim being $n-t$. With respect to the density of a set $\mathrm{Spl}\,(f,\sigma)$ of primes, our observation is

Expectation 1″.

$$
\lim_{X\to\infty} \frac{\#\mathrm{Spl}_X(f,\sigma)}{\#\mathrm{Spl}_X(f)} = c^{-1}\cdot \mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big),
$$

where the constant c is independent of σ.

We give a remark on the numbering of roots : Since (6) and (7) are equivalent to $\sum_{i=1}^n m_{j,\sigma^{-1}(i)}\alpha_{\sigma^{-1}(i)} = m_j$ and $\sum_{i=1}^n m_{j,\sigma^{-1}(i)} r_i \equiv m_j \bmod p$, we may assume that σ in Expectation $1', 1''$ is the identity for any numbering of roots with replacing "c is independent of σ" by "c is independent of the numbering of roots of f" in Expectation $1''$.

We note that for a sufficiently large prime p, we see that $0 < r_1 + a_{n-1}/n,\ r_n + a_{n-1}/n < p$, and then $\big((r_1 + a_{n-1}/n)/p, \ldots, (r_n + a_{n-1}/n)/p\big) \in \mathfrak{D}(f,\sigma)$ if f is irreducible and that a point $(r_1/p,\ldots,r_n/p)$ is on $\mathfrak{D}(f,\sigma)$ if and only if $a_{n-1} = 0$. Is it possible to reduce the problem to the case of trace being 0, using $g(x) := n^n f\big((x - a_{n-1})/n\big) = x^n + 0\cdot x^{n-1} + \cdots$? The relation between local roots R_i of $g(x)$ and r_i of $f(x)$ is $R_i \equiv n r_{\sigma(i)} + a_{n-1} \bmod p$ for a permutation σ dependent on p.

The second subject is as follows.
For given integers $L\,(>1), R_i$ with $0 \le R_i < L$ and a prime $p \in \mathrm{Spl}\,(f)$, we require a following congruence condition besides (1), (2) on the local roots $r_1,\ldots,r_n$ of $f(x) \equiv 0 \bmod p$:

$$
r_i \equiv R_i \bmod L \quad (1 \le {}^\forall i \le n). \tag{9}
$$

We put

$$
\mathrm{Pr}_X(f, L, \{R_i\}) := \frac{\#\{p \in \mathrm{Spl}_X(f) \mid (1),(2),(9)\}}{\#\mathrm{Spl}_X(f)} \tag{10}
$$

and

$$
\mathrm{Pr}\,(f, L, \{R_i\}) := \lim_{X\to\infty} \mathrm{Pr}_X(f, L, \{R_i\}). \tag{11}
$$

Although the existence of the limit is not proved in this case either, there is no data to deny it. By putting

$$
R_f := a_{n-1} + \sum_{i=1}^n R_i \quad \text{and} \quad d := (R_f, L),
$$

our second expectation is as follows:
For a polynomial f of degree ≥ 2 with only a trivial relation (3)

Expectation 2.

$$\Pr(f, L, \{R_i\}) := \frac{1}{L^{n-1}} \sum_{K,\, q} \frac{E_n(K)}{[\mathbb{Q}(\zeta_L) : \mathbb{Q}(f) \cap \mathbb{Q}(\zeta_{L/d})]}, \tag{12}$$

where K runs over a set of integers satisfying

$$1 \leq K \leq n-1, \ (K, L) = d,$$

and $q \in (\mathbb{Z}/L\mathbb{Z})^{\times}$ satisfy the conditions

$$\begin{cases} R_f \equiv Kq \bmod L \quad (\Leftrightarrow R_f/d \equiv K/d \cdot q \bmod L/d), \\ [[q]] = [[1]] \text{ on } \mathbb{Q}(f) \cap \mathbb{Q}(\zeta_{L/d}). \end{cases}$$

Let us explain notations: $E_n(k)$ is the volume of the set $\{x \in [0,1)^{n-1} \mid \lceil x_1 + \cdots + x_{n-1} \rceil = k\}$. $E_n(k)$ is also defined as $E_n(k) := A(n-1, k)/(n-1)!$, using Eulerian numbers $A(n, k)$ $(1 \leq k \leq n)$ defined recursively by

$$A(1,1) = 1, A(n,k) = (n-k+1)A(n-1,k-1) + kA(n-1,k).$$

ζ_L is a primitive Lth root of unity, and $\mathbb{Q}(f)$ is a Galois extension of the rational number field $\mathbb{Q}$ generated by all roots of f. For an abelian field F in $\mathbb{Q}(\zeta_c)$ and an integer a relatively prime to c, $[[a]]$ denotes an automorphism of F induced by $\zeta_c \to \zeta_c^a$.

Expectations 1, 2 are supported by numerical data by computer for irreducible and indecomposable polynomials of degree < 6 ([6],[7]), which are polynomials with only a trivial linear relation among roots. Expectation 2 fails for some polynomials of $\deg f = 6$ with non-trivial linear relations.

Let us refer to a relation with a one-dimensional distribution of r_i/p $(i = 1, \ldots, n)$: Let f be a polynomial of degree n with only a trivial linear relation among roots. Given number $a \in [0,1]$, put $D_{i,a} := \{(x_1, \ldots, x_n) \in [0,1)^n \mid x_i \leq a\}$. Then we see

$$\begin{aligned}
&\lim_{X \to \infty} \frac{\sum_{p \in \mathrm{Spl}_X(f)} \#\{i \mid r_i/p \leq a, 1 \leq i \leq n\}}{n \cdot \#\mathrm{Spl}_X(f)} \\
&= \lim_{X \to \infty} \frac{\sum_{p \in \mathrm{Spl}_X(f)} \#\{i \mid (r_1/p, \ldots, r_n/p) \in D_{i,a}\}}{n \cdot \#\mathrm{Spl}_X(f)} \\
&= \sum_{i=1}^{n} \Pr_{D_{i,a}}(f)/n \\
&= \sum_{i=1}^{n} \frac{\mathrm{vol}\,(D_{i,a} \cap \hat{\mathfrak{D}}_n)}{n \cdot \mathrm{vol}\,(\hat{\mathfrak{D}}_n)} \qquad \text{(by Expectation 1)}
\end{aligned}$$

which is equal to a, as far as we check approximately by the Monte Carlo method (definitely for $n = 2, 3$), that is we have the equi-distribution of r_i/p.

Lastly, let us give a relation between Expectation 1 and a series of observations in the references. Let a polynomial f of degree n have only a trivial linear relation among roots, and put, for an integer k

$$D_k := \{(x_1, \ldots, x_n) \in [0, 1)^n \mid \lceil x_1 + \cdots + x_{n-1} \rceil = k\}.$$

Then, under Expectation 1, we have

$$\begin{aligned}
&\lim_{X\to\infty} \frac{\#\{p \in \mathrm{Spl}_X(f) \mid \big(r_1 + \cdots + r_n - \mathrm{tr}\,(f)\big)/p = k\}}{\#\mathrm{Spl}_X(f)} \\
&= \lim_{X\to\infty} \frac{\#\{p \in \mathrm{Spl}_X(f) \mid \lceil r_1/p + \cdots + r_{n-1}/p \rceil = k\}}{\#\mathrm{Spl}_X(f)} \\
&= \lim_{X\to\infty} \frac{\#\{p \in \mathrm{Spl}_X(f) \mid (r_1/p, \ldots, r_n/p) \in D_k\}}{\#\mathrm{Spl}_X(f)} && (= \mathrm{Pr}_{D_k}(f)) \\
&= \frac{\mathrm{vol}\,(\{(x_1, \ldots, x_n) \in \hat{\mathfrak{D}}_n \mid \lceil \sum_{i=1}^{n-1} x_i \rceil = k\})}{\mathrm{vol}\,(\hat{\mathfrak{D}}_n)} && (\text{by Expectation 1}) \\
&= \frac{\mathrm{vol}\,(\{(x_1, \ldots, x_n) \in [0, 1)^n \mid x_1 \le \cdots \le x_n, \sum_{i=1}^{n} x_i = k\})}{\mathrm{vol}\,(\hat{\mathfrak{D}}_n)} \\
&= \frac{\mathrm{vol}\,(\{(x_1, \ldots, x_n) \in [0, 1)^n \mid \sum_{i=1}^{n} x_i = k\})}{n! \cdot \mathrm{vol}\,(\{(x_1, \ldots, x_n) \in [0, 1)^n \mid x_1 \le \cdots \le x_n, \sum_{i=1}^{n} x_i \in \mathbb{Z}\})} \\
&= \mathrm{vol}\left(\left\{(x_1, \ldots, x_{n-1}) \in [0, 1)^{n-1} \mid \left\lceil \sum_{i=1}^{n-1} x_i \right\rceil = k\right\}\right) && (\text{projected to } \mathbb{R}^{n-1}) \\
&= E_n(k),
\end{aligned}$$

which elucidates most of numerical observations in previous papers. We note that the last vol is the usual volume on $\mathbb{R}^{n-1}$, but others are the one on hyperplanes defined by

$$\sum_{i=1}^{n} x_i \in \mathbb{Z} \quad \text{in} \quad \mathbb{R}^n.$$

We discuss a linear relation among roots in the first section, and in the second section, we correct insufficient data given in [6] with respect to (12) and add new ones.

When we refer to an explicit value of a density, it is an approximation by computer, unless specified.

1. Linear relation among roots

Let $f(x)$ be a polynomial f in (0) of degree n with roots α_i $(i = 1, \ldots, n)$ and suppose a linear relation (3). We may suppose that $m = 0$ in (3) to discuss the non-triviality of a linear relation, if necessary. Because, if $\mathrm{tr}\,(f) = -a_{n-1} = 0$ holds, then taking traces, we have $nm = (\sum_i m_i)\mathrm{tr}\,(f) = 0$, hence $m = 0$. Otherwise, we have $\sum M_i\alpha_i = 0$ for $M_i := m_i + m/a_{n-1}$. The non-triviality of (3) is unchanging by this operation.

Just to make sure, let us see a relation between global relations of roots α_i and local relations of roots r'_i of $f(x) \equiv 0 \bmod p$.

Proposition 1. *Let $f(x)$ be a polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n$ and suppose that it has no multiple roots, and let $g_j(x_1, \ldots, x_n)$ $(j = 1, \ldots, t)$ be polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$.*

If there are global relations $g_j(\alpha_1, \ldots, \alpha_n) = 0$ $(j = 1, \ldots, t)$, then there are roots r'_i of $f(x) \equiv 0 \bmod p$ satisfy $g_j(r'_1, \ldots, r'_n) \equiv 0 \bmod p$ $(j = 1, \ldots, t)$ for $p \in \mathrm{Spl}\,(f)$.

Conversely, if roots r'_i of $f(x) \equiv 0 \bmod p$ satisfy $g_j(r'_1, \ldots, r'_n) \equiv 0 \bmod p$ $(j = 1, \ldots, t)$ for infinitely many primes $p \in \mathrm{Spl}\,(f)$, then there is a permutation σ such that $g_j(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0$ $(j = 1, \ldots, t)$.

Proof. Put $K = \mathbb{Q}(f)$ and take a prime $p \in \mathrm{Spl}\,(f)$. K is a Galois extension and a prime p is fully splitting in K.

First, assume $g_j(\alpha_1, \ldots, \alpha_n) = 0$ $(j = 1, \ldots, t)$: For a prime ideal $\mathfrak{p}$ of K over p, take a rational integer r'_i satisfying $\alpha_i \equiv r'_i \bmod \mathfrak{p}$, which implies $g_j(r'_1, \ldots, r'_n) \equiv 0 \bmod \mathfrak{p}$, hence $g_j(r'_1, \ldots, r'_n) \equiv 0 \bmod p$. Let us see that $r'_1, \ldots, r'_n$ are roots of $f(x) \equiv 0 \bmod p$. We see $0 = f(\alpha_i) \equiv f(r'_i) \bmod \mathfrak{p}$, hence $f(r'_i) \equiv 0 \bmod p$. If p is sufficiently large, then we see that $\alpha_i \not\equiv \alpha_j \bmod \mathfrak{p}$ for $i \neq j$, hence $r'_i \not\equiv r'_j \bmod p$, that is, $r'_1, \ldots, r'_n$ are all distinct roots of $f(x) \equiv 0 \bmod p$.

Conversely, suppose that there are infinitely many primes $p \in \mathrm{Spl}\,(f)$ such that $g_j(r'_1, \ldots, r'_n) \equiv 0 \bmod p$ $(j = 1, \ldots, t)$ for roots r'_i of $f(x) \equiv 0 \bmod p$. For such a prime, we fix any prime ideal $\mathfrak{p}$ over p; then there is a permutation σ_p of $\{1, \ldots, n\}$ such that $\alpha_{\sigma_p(i)} \equiv r'_i \bmod \mathfrak{p}$ as above. We take a permutation σ satisfying $\sigma = \sigma_p$ for infinitely many primes $p \in \mathrm{Spl}\,(f)$. For such infinitely many primes p, we see $g_j(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \equiv g_j(r'_1, \ldots, r'_n) \equiv 0 \bmod \mathfrak{p}$, hence a global relation $g_j(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0$ $(j = 1, \ldots, t)$. □

We apply this to linear equations $g_j := \sum_{i=1}^{n} m_{j,i}x_i - m_j$ $(j = 1, \dots, t)$ (cf. (6), (7)). The following is a sufficient condition to a polynomial being without non-trivial linear relation.

Proposition 2. *Let $f(x)$ be an irreducible polynomial of degree n. If n is a prime number p, or the Galois group* $\mathrm{Gal}\,(\mathbb{Q}(f)/\mathbb{Q})$ *is S_n or A_n $(n \geq 6)$ as a permutation group of roots of f, then f has only a trivial linear relation among roots.*

Proof. First, suppose that the degree of a polynomial f is a prime p, and let $\alpha_1, \dots, \alpha_p$ be roots of f, and suppose a linear relation (3). Adding a trivial relation $\sum \alpha_i = \mathrm{tr}\,(f)$ to (3) if necessary, we may assume that $\sum m_i \neq 0$. The Galois group $\mathrm{Gal}\,(\mathbb{Q}(f)/\mathbb{Q})$ acts faithfully on the set of all roots and contains an element σ of order p, hence we may assume that $\big(\sigma(\alpha_1), \dots, \sigma(\alpha_p)\big) = (\alpha_2, \dots, \alpha_p, \alpha_1)$. Then from the assumption (3) follows

$$\begin{pmatrix} m_1 & m_2 & \dots & m_p \\ m_p & m_1 & \dots & m_{p-1} \\ \vdots & & & \\ m_2 & m_3 & \dots & m_1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_p \end{pmatrix} = \begin{pmatrix} m \\ m \\ \vdots \\ m \end{pmatrix}.$$

Since α_i's are not rational, the determinant of the coefficient matrix of entries m_i vanishes, hence we have

$$\prod_{i=0}^{p-1} \big(m_1 + \zeta^i m_2 + \zeta^{2i} m_3 + \dots + \zeta^{(p-1)i} m_p\big) = 0$$

for a primitive pth root $\zeta := \zeta_p$ of unity, using a formula for cyclic determinant. By the assumption $\sum m_i \neq 0$, we have

$$m_1 + \zeta^i m_2 + \zeta^{2i} m_3 + \dots + \zeta^{(p-1)i} m_p = 0 \quad \text{for some} \quad i \ \ (0 < i < p),$$

which implies $m_1 = \dots = m_p$, that is, (3) is trivial, since ζ^i is still a primitive pth root of unity.

Next, suppose that the Galois group $\mathrm{Gal}\,(\mathbb{Q}(f)/\mathbb{Q})$ is the symmetric group S_n. For any $1 \leq i < j \leq n$, there is an automorphism σ which induces a transposition of α_i and α_j. Hence we have

$$m = \left(\sum_{k \neq i,j} m_k \alpha_k \right) + m_i \alpha_i + m_j \alpha_j = \left(\sum_{k \neq i,j} m_k \alpha_k \right) + m_i \alpha_j + m_j \alpha_i,$$

which implies

$$m_i(\alpha_i - \alpha_j) = m_j(\alpha_i - \alpha_j).$$

By $\alpha_i \neq \alpha_j$, we have $m_i = m_j$, thus (3) is trivial.

Finally, suppose that $\mathrm{Gal}\bigl(\mathbb{Q}(f)/\mathbb{Q}\bigr)$ is the alternative group A_n and that (3) is non-trivial. Let us show that coefficients $m_1, \dots, m_n$ are mutually distinct, first. Suppose that $m_1 = m_2$; acting an even permutation $\alpha_1 \to \alpha_2 \to \alpha_3 \to \alpha_1$ on (3), we have

$$m_1\alpha_1 + m_2\alpha_2 + m_3\alpha_3 = m - \sum_{i>3} m_i\alpha_i,$$
$$m_3\alpha_1 + m_1\alpha_2 + m_2\alpha_3 = m - \sum_{i>3} m_i\alpha_i,$$

which imply $(m_1 - m_3)(\alpha_1 - \alpha_3) = 0$, hence $m_2 = m_1 = m_3$. Considering other α_i $(i > 3)$ instead of α_3, we get $m_1 = m_2 = \cdots = m_n$, which contradicts the non-triviality of (3). Thus coefficients m_i are mutually distinct.

Next, considering even permutations:

$$\{\alpha_1 \leftrightarrow \alpha_2,\ \alpha_3 \leftrightarrow \alpha_4\}, \quad \{\alpha_1 \leftrightarrow \alpha_3,\ \alpha_2 \leftrightarrow \alpha_4\}, \quad \{\alpha_1 \leftrightarrow \alpha_4,\ \alpha_2 \leftrightarrow \alpha_3\},$$

we get

$$\begin{cases} m_1\alpha_1 + m_2\alpha_2 + m_3\alpha_3 + m_4\alpha_4 = m - \sum_{i>4} m_i\alpha_i, \\ m_2\alpha_1 + m_1\alpha_2 + m_4\alpha_3 + m_3\alpha_4 = m - \sum_{i>4} m_i\alpha_i, \end{cases}$$

$$\begin{cases} m_3\alpha_1 + m_4\alpha_2 + m_1\alpha_3 + m_2\alpha_4 = m - \sum_{i>4} m_i\alpha_i, \\ m_4\alpha_1 + m_3\alpha_2 + m_2\alpha_3 + m_1\alpha_4 = m - \sum_{i>4} m_i\alpha_i, \end{cases}$$

which imply

$$(m_1 - m_2)(\alpha_1 - \alpha_2) + (m_3 - m_4)(\alpha_3 - \alpha_4) = 0,$$
$$(m_3 - m_4)(\alpha_1 - \alpha_2) + (m_1 - m_2)(\alpha_3 - \alpha_4) = 0,$$

hence $(\alpha_1 - \alpha_2)^2 = (\alpha_3 - \alpha_4)^2$. Similarly, we have $(\alpha_1 - \alpha_2)^2 = (\alpha_3 - \alpha_5)^2$. Therefore we get

$$\begin{aligned} 0 &= (\alpha_3 - \alpha_4)^2 - (\alpha_3 - \alpha_5)^2 \\ &= (\alpha_3 - \alpha_4 + \alpha_3 - \alpha_5)(\alpha_3 - \alpha_4 - \alpha_3 + \alpha_5) \\ &= (2\alpha_3 - \alpha_4 - \alpha_5)(-\alpha_4 + \alpha_5), \end{aligned}$$

i.e., $2\alpha_3 = \alpha_4 + \alpha_5$, similarly, $2\alpha_3 = \alpha_4 + \alpha_6$. Thus we have a contradiction

$$\alpha_5 = \alpha_6. \qquad \square$$

Proposition 3. *Let $f = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ be an irreducible polynomial. If there is a non-trivial linear relation among roots of f, then f is decomposable, that is $f(x) = g\bigl(h(x)\bigr)$ for quadratic polynomials $g(x), h(x)$.*

P r o o f. Let $\alpha_1, \dots, \alpha_4$ be the roots of f. Let $G := \mathrm{Gal}\,(\mathbb{Q}(f)/\mathbb{Q})$ be the Galois group; then it operates faithfully on a set $\{\alpha_1, \dots, \alpha_4\}$ and there is a subgroup of order 4 in G. Noting that for permutations:

$$\begin{aligned}
&\sigma = (1,2), && \mu = (1,3) && \Rightarrow \quad \sigma\mu \neq \mu\sigma,\\
&\sigma = (1,2)(3,4), && \mu = (2,3) && \Rightarrow \quad \sigma\mu \neq \mu\sigma,\\
&\sigma = (1,2)(3,4), && \mu = (1,3)(2,4) && \Rightarrow \quad \sigma\mu = \mu\sigma,
\end{aligned}$$

we see that:

(i) there is a cyclic permutation σ in G so that

$$\sigma : (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \to (\alpha_2, \alpha_3, \alpha_4, \alpha_1),$$

(ii) there are permutations σ_1, σ_2 in G so that

$$\begin{aligned}
&\sigma_1 : (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \to (\alpha_2, \alpha_1, \alpha_4, \alpha_3),\\
&\sigma_2 : (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \to (\alpha_3, \alpha_4, \alpha_1, \alpha_2) \quad \text{or}
\end{aligned}$$

(iii) there are permutations σ_1, σ_2 such that σ_1 (resp. σ_2) is a transposition of α_1 and α_2 (α_3 and α_4), respectively.

Suppose that (3) is non-trivial, that is ${}^\exists m_i \neq {}^\exists m_j$, and if $a_3 = 0$ happens, then considering $f(x-1)$ instead of $f(x)$, we may assume that $a_3 \neq 0$ and furthermore $\sum m_i \neq 0$, adding a trivial relation.

First, let us consider

Case (i). By linear equations $\sum m_i \sigma^j(\alpha_i) = m$ $(j = 0, 1, 2, 3)$, we have

$$\begin{pmatrix} m_1 & m_2 & m_3 & m_4 \\ m_4 & m_1 & m_2 & m_3 \\ m_3 & m_4 & m_1 & m_2 \\ m_2 & m_3 & m_4 & m_1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 \\ \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 \\ \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \end{pmatrix} = \begin{pmatrix} m \\ m \\ m \\ m \end{pmatrix}.$$

Since α_i's are irrational, the determinant of coefficient matrix on m_i vanishes, i.e., $\prod_{i=0}^{3}(m_1 + \zeta^i m_2 + \zeta^{2i} m_3 + \zeta^{3i} m_4) = 0$ for a primitive fourth root $\zeta := \zeta_4$ of unity. By the assumption $\sum m_i \neq 0$, we have

$$m_1 + \zeta^i m_2 + \zeta^{2i} m_3 + \zeta^{3i} m_4 = 0 \quad \text{for some} \quad i = 1,\ 2,\ 3,$$

hence

(i.1) $m_1 - m_3 = m_2 - m_4 = 0$ in the case of $i = 1, 3$ or

(i.2) $m_1 - m_2 + m_3 - m_4 = 0$ in the case of $i = 2$.

Case of (i.1), i.e., $m_1 = m_3$, $m_2 = m_4$:
The difference of the first row and the second row gives

$$(m_1 - m_2)(\alpha_1 - \alpha_2 + \alpha_3 - \alpha_4) = 0.$$

If $m_1 = m_2$ holds, we have a contradiction $m_1 = \cdots = m_4$. It implies $\alpha_1 + \alpha_3 = \alpha_2 + \alpha_4 = -a_3/2$, hence $f(x) = (x^2 + a_3 x/2 + \alpha_1\alpha_3)(x^2 + a_3 x/2 + \alpha_2\alpha_4)$ is a polynomial in $x^2 + a_3 x/2$, that is f is decomposable.

Case of (i.2), hence $m_1 + m_3 = m_2 + m_4$:
It is easy to see that

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 \\ \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 \\ \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} \begin{pmatrix} m_1 - m_2 \\ m_2 - m_3 \\ m_3 - m_4 \\ m_4 - m_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

By non-triviality $(m_1 - m_2, \ldots, m_4 - m_1) \neq (0, \ldots, 0)$, the cyclic determinant of coefficients matrix vanishes, i.e.,

$$a_3(\alpha_1 + \zeta\alpha_2 - \alpha_3 - \zeta\alpha_4)(\alpha_1 - \alpha_2 + \alpha_3 - \alpha_4)(\alpha_1 - \zeta\alpha_2 - \alpha_3 + \zeta\alpha_4) = 0.$$

(i.2.1) Suppose $\alpha_1 + \zeta\alpha_2 - \alpha_3 - \zeta\alpha_4 = 0$, i.e., $\alpha_1 - \alpha_3 = -\zeta(\alpha_2 - \alpha_4)$. By equations $\sum m_i\alpha_i = m$ and (by acting σ^2 on it) $m_1\alpha_3 + m_2\alpha_4 + m_3\alpha_1 + m_4\alpha_2 = m$, we have

$$(m_1 - m_3)(\alpha_1 - \alpha_3) + (m_2 - m_4)(\alpha_2 - \alpha_4) = 0,$$

hence $\big((m_1 - m_3)(-\zeta) + m_2 - m_4\big)(\alpha_2 - \alpha_4) = 0$. Therefore we get $m_1 = m_3$, $m_2 = m_4$ and so a contradiction $m_1 = m_2 = m_3 = m_4$ by the assumption $m_1 + m_3 = m_2 + m_4$.
(i.2.2) Suppose that $\alpha_1 - \alpha_2 + \alpha_3 - \alpha_4 = 0$; it implies $\alpha_1 + \alpha_3 = \alpha_2 + \alpha_4$, which implies that f is decomposable as above.
(i.2.3) The case of $\alpha_1 - \zeta\alpha_2 - \alpha_3 + \zeta\alpha_4 = 0$ is similar to (i.2.1).

Thus we have shown that in the case of (i), f is decomposable.

Case (ii). The second case gives the following equations:

$$m_1\alpha_1 + m_2\alpha_2 + m_3\alpha_3 + m_4\alpha_4 = m, \tag{13}$$

$$m_2\alpha_1 + m_1\alpha_2 + m_4\alpha_3 + m_3\alpha_4 = m, \tag{14}$$

$$m_3\alpha_1 + m_4\alpha_2 + m_1\alpha_3 + m_2\alpha_4 = m, \tag{15}$$

$$m_4\alpha_1 + m_3\alpha_2 + m_2\alpha_3 + m_1\alpha_4 = m. \tag{16}$$

(13), (14) (resp. (15), (16)) give

$$(m_1 + m_2)(\alpha_1 + \alpha_2) + (m_3 + m_4)(\alpha_3 + \alpha_4) = 2m,$$
$$(m_3 + m_4)(\alpha_1 + \alpha_2) + (m_1 + m_2)(\alpha_3 + \alpha_4) = 2m,$$

hence if $m_1 + m_2 \neq m_3 + m_4$ holds, then $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4$ follows, i.e., f is decomposable. Hence we may suppose that $m_1 + m_2 = m_3 + m_4$.

Similarly, using (13), (16) (resp. (14), (15)) , we may suppose $m_1 + m_4 = m_2 + m_3$, and $m_1 + m_3 = m_2 + m_4$, using (13), (15) (resp. (14), (16)). These give a contradiction $m_1 = m_2 = m_3 = m_4$.

Finally, let us consider:

Case (iii). Acting σ_1, σ_2 on $\sum m_i\alpha_i = m$, we have

$$\begin{aligned} m_1\alpha_1 + m_2\alpha_2 + m_3\alpha_3 + m_4\alpha_4 &= m, \\ m_1\alpha_2 + m_2\alpha_1 + m_3\alpha_3 + m_4\alpha_4 &= m, \\ m_1\alpha_1 + m_2\alpha_2 + m_3\alpha_4 + m_4\alpha_3 &= m, \end{aligned}$$

which implies

$$(m_1 - m_2)(\alpha_1 - \alpha_2) = (m_3 - m_4)(\alpha_3 - \alpha_4) = 0.$$

Since α_i's are distinct, we have

$$m_1 = m_2, \quad m_3 = m_4.$$

By $m_1 \neq m_3$, the equations

$$(\alpha_1 + \alpha_2) + (\alpha_3 + \alpha_4) = -a_3, \quad m_1(\alpha_1 + \alpha_2) + m_3(\alpha_3 + \alpha_4) = m$$

imply

$$b_1 := \alpha_1 + \alpha_2 \in \mathbb{Q}, \quad b_2 := \alpha_3 + \alpha_4 \in \mathbb{Q}.$$

Therefore

$$f(x) = \big(x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2\big)\big(x^2 - (\alpha_3 + \alpha_4)x + \alpha_3\alpha_4\big)$$

is equal to

$$x^4 + a_3x^3 + (\alpha_3\alpha_4 + b_1b_2 + \alpha_1\alpha_2)x^2 - (b_1\alpha_3\alpha_4 + b_2\alpha_1\alpha_2)x + f(0),$$

hence we have

$$\alpha_1\alpha_2 + \alpha_3\alpha_4 = a_2 - b_1b_2, \quad b_2\alpha_1\alpha_2 + b_1\alpha_3\alpha_4 = -a_1.$$

If $b_1 \neq b_2$ holds, then solving them, we have $\alpha_1\alpha_2,\ \alpha_3\alpha_4 \in \mathbb{Q}$, which implies that f is reducible. Thus we have $b_1 = b_2$ and then f is a polynomial in $x^2 - b_1x$, that is decomposable.

The following is an easy corollary.

Corollary 1. *Let f be a polynomial of degree less than 6 and suppose that f has a non-trivial liner relation among roots. Then f is reducible or decomposable.*

Proposition 4. *Let $f = (x^2+ax)^2+b(x^2+ax)+c$ $(a, b, c \in \mathbb{Q})$ be an irreducible and decomposable polynomial, and put*

$$x^2 + bx + c = (x - \beta_1)(x - \beta_2), \quad x^2 + ax - \beta_i = (x - \alpha_{i,1})(x - \alpha_{i,2}).$$

Then equations $\alpha_{i,1} + \alpha_{i,2} = -a$ $(i = 1, 2)$ are a basis of linear relations (3) *among roots of f.*

Proof. Let

$$m_{1,1}\alpha_{1,1} + m_{1,2}\alpha_{1,2} + m_{2,1}\alpha_{2,1} + m_{2,2}\alpha_{2,2} = m \quad (m_{i,j}, m \in \mathbb{Q})$$

be a linear relation. Using $\alpha_{i,1} + \alpha_{i,2} = -a$, we may suppose

$$m_{1,2}\alpha_{1,2} + m_{2,2}\alpha_{2,2} = m.$$

We have only to show $m_{2,2} = 0$, which implies $m_{1,2} = 0$, hence we complete the proof. Suppose that $m_{2,2} \neq 0$, and dividing $m_{2,2}$, we may assume

$$\alpha_{2,2} = m_1\alpha_{1,2} + m_2 \quad (m_1, m_2 \in \mathbb{Q}).$$

Hence $\alpha_{1,2}$ is a root of $g(x) = x^2 + ax - \beta_1$ and $h(x) = (m_1x + m_2)^2 + a(m_1x + m_2) - \beta_2 = (m_1x + m_2)^2 + a(m_1x + m_2) + b + \beta_1$, which are polynomials over a quadratic field $\mathbb{Q}(\beta_1)$. Since $g(x)$ is irreducible in $\mathbb{Q}(\beta_1)[x]$, we have $h(x) = m_1^2 g(x)$, hence comparing constant terms $m_2^2 + am_2 + b + \beta_1 = -m_1^2\beta_1$. Thus we find a contradiction that β_1 is rational. □

Let us give $\mathfrak{D}(f, \sigma)$ explicitly for a polynomial of degree 4. In case that f is irreducible and indecomposable, there is only a trivial relation, hence

$$\mathfrak{D}(f, \sigma) = \hat{\mathfrak{D}}_n.$$

In case that f is irreducible and decomposable, by using Proposition 4, we find, with $\dim \mathfrak{D}(f, \sigma) = 2$

$$\mathfrak{D}(f, \sigma) = \left\{ (x_1, x_2, x_3, x_4) \;\middle|\; \begin{array}{l} 0 \le x_1 \le x_2 \le x_3 \le x_4 \le 1, \\ x_{\sigma(1)} + x_{\sigma(2)} \in \mathbb{Z}, x_{\sigma(3)} + x_{\sigma(4)} \in \mathbb{Z} \end{array} \right\}$$

$$= \{(x_1, x_2, 1 - x_2, 1 - x_1) \mid 0 \le x_1 \le x_2 \le 1 - x_2 \le 1 - x_1 < 1\},$$

which is parametrized by $0 \le x_1 \le x_2 \le 1/2$. The dimension of a domain corresponding to $\{\sigma(1), \sigma(2)\} \neq \{1, 4\}, \{2, 3\}$ is less than 2. To confirm Expectation $1'$, i.e., (8), what we can do now is an approximate calculation by computer. The right hand of (8) is a ratio, hence we do not need to look for volumes themselves. By using a projection to (x_1, x_2)-plane, we can approximate the right hand of (8) by the Monte Carlo method.

In case that f is a product of two irreducible quadratic polynomials with distinct fundamental discriminants, relations are similar to the previous case and hence $\mathfrak{D}(f,\sigma)$ is the same.

In case that two irreducible quadratic factors have the same fundamental discriminant D, e.g., $f(x) = (x^2 - D)\big((x-1)^2 - 4D\big)$, put

$$\alpha_1 = \sqrt{D}, \quad \alpha_2 = -\sqrt{D}, \quad \alpha_3 = 1 + 2\sqrt{D}, \quad \alpha_4 = 1 - 2\sqrt{D}.$$

A basis of linear relations (3) among roots are

$$\alpha_1 + \alpha_2 = 0, \quad 2\alpha_1 - \alpha_3 = -1, \quad 2\alpha_1 + \alpha_4 = 1,$$

hence hyperplanes necessary in $[0,1)^4$ in question are

$$x_1 + x_2, \quad 2x_1 - x_3, \quad 2x_1 + x_4 \in \mathbb{Z}$$

and its permutations of indexes.

Thus we see that $\mathfrak{D}(f,\sigma)$ of dim 1 is one of

$$\big\{(x, 2x, 1-2x, 1-x) \mid \ 0 \ \le x < 1/4\big\} \text{ for } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix},$$

$$\big\{(x, 1-2x, 2x, 1-x) \mid 1/4 \le x < 1/3\big\} \text{ for } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix},$$

$$\big\{(1-2x, x, 1-x, 2x) \mid 1/3 \le x < 1/2\big\} \text{ for } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Let us see that Expectation $1''$ is true in this case. It is easy to see that lengths are, in order $\sqrt{10}/4$, $\sqrt{10}/12$, $\sqrt{10}/6$. For densities of $\mathrm{Spl}\,(f,\sigma)$, we invoke [1], [9], that is for an irreducible quadratic polynomial, $r_1/p, r_2/p$ are equi-distributed. Let r be a root of $r^2 \equiv D \bmod p$ with $0 < r < p/2$. Then other roots of $f(x) \equiv 0 \bmod p$ are $-r, 1 \pm 2r \bmod p$, and it is easy to see except for finitely many primes local roots $r_1, \dots, r_4$ are in order

$$(r_1, \dots, r_4) = \begin{cases} (r, 1+2r, p+1-2r, p-r) & \text{if} \quad r/p \in [0, 1/4), \\ (r, p+1-2r, 1+2r, p-r) & \text{if} \quad r/p \in [1/4, 1/3), \\ (p+1-2r, r, p-r, 1+2r) & \text{if} \quad r/p \in [1/3, 1/2). \end{cases}$$

The uniformity of r/p implies that densities are proportional to

$$1/4, 1/3 - 1/4 = 1/12, 1/2 - 1/3 = 1/6.$$

Hence the constant c in Expectation $1''$ is independent of σ.

In case that a polynomial f is a product of irreducible quadratic polynomials with the same fundamental discriminant, Expectation $1', 1''$ should be reduced to [1], [9].

In case that $f(x) = \prod_{i=1}^{a}(x-\alpha_i)\cdot g(x)$, where α_i's are all rational integer roots of f with $\alpha_1 \le \dots \alpha_t < 0 \le \alpha_{t+1} \le \dots \alpha_a$ It is easy to see that

$$r_1 = \alpha_{t+1}, \dots, r_{a-t} = \alpha_a,\ r_{n+1-t} = p + \alpha_t, \dots, r_n = p + \alpha_1$$

for any prime $p \in \mathrm{Spl}\,(f)$ except finitely many primes. Linear relations among roots are reduced to relations of g. Therefore the projection of $\mathfrak{D}(f,\sigma)$ to a hyperplane defined by

$$x_1 = \cdots = x_a = 0 \quad \text{with} \quad \sigma(i) = i \quad (1 \le i \le a)$$

is $\mathfrak{D}(g, \sigma_{|\{a+1,\dots,n\}})$ modulo a lower dimensional set, hence the problem is reduced to that of a polynomial $g(x)$ as expected.

Before we discuss the case of degree six, let us introduce a notion "type". For an irreducible polynomial f of degree 6, we define its type number $2, 3$ temporarily as follows:

Denote a root of f by α. The type number of f is 2 if $\mathbb{Q}(\alpha)$ contains a quadratic subfield M_2 such that the trace of α to M_2 is rational.

The type number of f is 3 if $\mathbb{Q}(\alpha)$ contains a cubic subfield M_3 such that the discriminant D of the monic minimal quadratic polynomial $g_2(x)$ of α over M_3 is rational.

We note that the type number is independent of the choice of a root α of f, and type numbers of $f(x), f(x+a)$ $(a \in \mathbb{Q})$ are equal.

Proposition 5. *Let $f = x^6 + a_5x^5 + \cdots + a_0$ be an irreducible polynomial of degree 6 with roots $\alpha_1, \dots, \alpha_6$ and suppose that there is a non-trivial relation (3). Then we have:*

(i) *The extension degree $[\mathbb{Q}(f) : \mathbb{Q}]$ is not divisible by 5.*

(ii) *If $\mathbb{Q}(\alpha_1)$ is an abelian extension, then f is either of type 2 or 3, or decomposable.*

(iii) *If $\mathbb{Q}(\alpha_1)$ is an S_3 Galois extension, then f is either of type 2 or 3, decomposable or there are a rational number c, two distinct roots α, α' of f, and a cubic subfield M_3 such that $\mathrm{tr}_{K/M_3}(\alpha) + c\cdot \mathrm{tr}_{K/M_3}(\alpha') \in \mathbb{Q}$ and α, α' are not conjugate over M_3.*

Proof. Let (3) be a non-trivial relation.

(i) Suppose that the extension degree $[\mathbb{Q}(f) : \mathbb{Q}]$ is divisible by 5; then there is an automorphism σ of order 5 in $\mathrm{Gal}\,(\mathbb{Q}(f)/\mathbb{Q})$, which acts faithfully on a set $\{\alpha_1, \dots, \alpha_6\}$, hence we may assume that

$$\sigma(\alpha_i) = \alpha_{i+1} \ \ (i = 1,2,3,4), \qquad \sigma(\alpha_5) = \alpha_1 \quad \text{and} \quad \sigma(\alpha_6) = \alpha_6.$$

Adding a trivial relation, we may assume $\sum_{i=1}^{5} m_i \neq 0$

$$\begin{pmatrix} m_1 & m_2 & m_3 & m_4 & m_5 \\ m_5 & m_1 & m_2 & m_3 & m_4 \\ m_4 & m_5 & m_1 & m_2 & m_3 \\ m_3 & m_4 & m_5 & m_1 & m_2 \\ m_2 & m_3 & m_4 & m_5 & m_1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \end{pmatrix} = (m - m_6\alpha_6) \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

If the determinant of the coefficient matrix does not vanish, then $\alpha_1, \ldots, \alpha_5$ are in $\mathbb{Q}(\alpha_6)$, hence $\mathbb{Q}(\alpha_6) = \mathbb{Q}(\{\alpha_1, \ldots, \alpha_6\}) = \mathbb{Q}(f)$ is a Galois extension of degree 6. This contradicts the assumption. Thus the determinant vanishes, hence there is a fifth root ζ of unity satisfying $\sum_{i=1}^{5} m_i \zeta^{i-1} = 0$, i.e., $m_1 = \cdots = m_5$. Thus (3) implies $m_1(\mathrm{tr}\,(f) - \alpha_6) + m_6\alpha_6 = m$, which implies $m_1 = m_6$, that is (3) is a trivial relation, contradicting the assumption. This completes the proof of (i). $\square$

(ii) Suppose that $\mathbb{Q}(\alpha_1)$ is an abelian extension, hence the Galois group is generated by an automorphism σ of order 6. We may assume that $\sigma(\alpha_i) = \alpha_{i+1}$, where $\alpha_j = \alpha_k$ if $j \equiv k \bmod 6$. Otherwise, there is a fixed root α_i by σ. Let $\zeta = (1 + \sqrt{-3})/2$ be a primitive sixth root of unity, which satisfies $\zeta^2 - \zeta + 1 = 0$ and $\zeta^3 = -1$, and consider central idempotents

$$\chi_i = 6^{-1} \sum_{j \bmod 6} \zeta^{ij} \sigma^j,$$

which satisfies

$$\sum_{i \bmod 6} \chi_i = 1, \; \chi_i \chi_j = \delta_{i,j} \chi_j.$$

The equation (3) is equivalent to $\chi_i(m) = \chi_i(\sum_k m_k \alpha_k)$, hence

$$0 = \chi_i(m) = \left(\sum_{k \bmod 6} \zeta^{-ik} m_k \right) \left(\sum_{l \bmod 6} \zeta^{il} \alpha_l \right) \quad (i \not\equiv 0 \bmod 6),$$

using $\chi_i(\alpha_k) = 6^{-1} \zeta^{-ki} \sum_{l \bmod 6} \zeta^{li} \alpha_l$. Thus for

$$i \not\equiv 0 \bmod 6, \quad \sum_{k \bmod 6} \zeta^{ik} m_k = 0 \quad \text{or} \quad \sum_{l \bmod 6} \zeta^{il} \alpha_l = 0 \quad \text{occurs.}$$

If $\sum_{l \bmod 6} \zeta^{il} \alpha_l = 0$ holds for every $i = 1, \ldots, 5$, then we have

$$\begin{aligned} 0 = \sum_{i=1}^{5} \left(\sum_{l \bmod 6} \zeta^{il} \alpha_l \right) &= 5\alpha_6 + \sum_{l=1}^{5} \left(\sum_{i=1}^{5} \zeta^{il} \right) \alpha_l \\ &= 5\alpha_6 - \sum_{l=1}^{5} \alpha_l = 6\alpha_6 - \mathrm{tr}\,(f), \end{aligned}$$

which implies a contradiction $\alpha_6 \in \mathbb{Q}$. Hence, we have $\sum_{l \bmod 6} \zeta^{il}\alpha_l \neq 0$ for some $i \not\equiv 0 \bmod 6$, i.e.,

$$\zeta^{-i}\sum_{k=1}^{6}\zeta^{ik}m_k = m_1 + \zeta^i m_2 + \zeta^{2i}m_3 + \cdots + \zeta^{5i}m_6 = 0. \tag{17}$$

By expressing the above as a linear form of ζ and 1, the equation (17) is

$$\begin{cases} m_1 - m_3 - m_4 + m_6 = m_2 + m_3 - m_5 - m_6 = 0 & (i = 1, 5), \\ m_1 - m_2 + m_4 - m_5 = m_2 - m_3 + m_5 - m_6 = 0 & (i = 2, 4), \\ m_1 + m_3 + m_5 = m_2 + m_4 + m_6 & (i = 3). \end{cases}$$

Suppose that (17) is true for both $i = 1$ and $i = 2$: Then we have

$$m_1 = m_3 = m_5 \quad \text{and} \quad m_2 = m_4 = m_6.$$

If (17) is true for $i = 3$ moreover, then (3) is a trivial relation, which is a contradiction. Thus (17) is false for $i = 3$, hence $\sum_{l \bmod 6} \zeta^{3l}\alpha_l = 0$ follows, that is $\alpha_1 + \alpha_3 + \alpha_5 = \alpha_2 + \alpha_4 + \alpha_6$. Putting $g = (x - \alpha_1)(x - \alpha_3)(x - \alpha_5)$ and $h = (x - \alpha_2)(x - \alpha_4)(x - \alpha_6)$, coefficients of polynomials g, h are in a quadratic subfield M_2 fixed by σ^2 and their second leading coefficient $\alpha_1 + \alpha_3 + \alpha_5 = \alpha_2 + \alpha_4 + \alpha_6 = \mathrm{tr}\,(f)/2$ is rational, hence f is of type 2.

Suppose that (17) is true for $i = 1$, but false for $i = 2, 4$: Hence we have $\sum_{l \bmod 6} \zeta^{il}\alpha_l = 0$ for $i = 2, 4$, which implies two equations

$$(\alpha_1 - \alpha_2 + \alpha_4 - \alpha_5)\sqrt{-3} + (-\alpha_1 - \alpha_2 + 2\alpha_3 - \alpha_4 - \alpha_5 + 2\alpha_6) = 0,$$
$$-(\alpha_1 - \alpha_2 + \alpha_4 - \alpha_5)\sqrt{-3} + (-\alpha_1 - \alpha_2 + 2\alpha_3 - \alpha_4 - \alpha_5 + 2\alpha_6) = 0,$$

hence $\alpha_1 + \alpha_4 = \alpha_2 + \alpha_5 = \alpha_3 + \alpha_6$. Thus f is a polynomial in $x^2 + (\alpha_1 + \alpha_4)x$, that is decomposable.

Finally, we assume that (17) is false for $i = 1$ hence for $i = 5$; similarly to the above, we have $\alpha_1 + \alpha_2 - \alpha_4 - \alpha_5 = 0$, i.e., $\alpha_1 - \alpha_4 = \alpha_5 - \alpha_2$. Hence we see that the discriminant $(\alpha_1 - \alpha_4)^2$ of a polynomial $(x - \alpha_1)(x - \alpha_4)$ fixed by σ^3 is fixed by σ, hence rational, that is f is of type 3.

(iii) Suppose that $K = \mathbb{Q}(\alpha_1)$ is an S_3-extension: Then there are automorphisms σ, μ and a numbering $\beta_{i,j}$ $(i = 1, 2,\ j = 1, 2, 3)$ of roots α_i of f such that $\sigma^3 = \eta^2 = 1, \eta\sigma\eta = \sigma^2$ and

$$\sigma(\beta_{i,1}) = \beta_{i,2}, \sigma(\beta_{i,2}) = \beta_{i,3}, \sigma(\beta_{i,3}) = \beta_{i,1} \quad (i = 1, 2)$$
$$\eta(\beta_{1,1}) = \beta_{2,1},\ \eta(\beta_{1,2}) = \beta_{2,3},\ \eta(\beta_{1,3}) = \beta_{2,2},$$

noting that σ, η have no fixed root. We divide a proof to several parts.

Lemma 1.

(1) *If* $\sum_j \beta_{1,j}$ *is rational, then* f *is of type* 2.

(2) *If one of* $(\beta_{1,1}-\beta_{2,1})^2$,$(\beta_{1,2}-\beta_{2,3})^2$,$(\beta_{1,3}-\beta_{2,2})^2$ *is fixed by* σ*, then* f *is of type* 3.

Proof.
Suppose that $\sum_i \beta_{1,j} \in \mathbb{Q}$, and decompose f as $f = gh$ with $g = \prod(x-\beta_{1,j})$, $h = \prod(x-\beta_{2,j}) \in M_2[x]$, where M_2 is a quadratic subfield fixed by σ. Therefore f is of type 2. Since polynomials $(x-\beta_{1,1})(x-\beta_{2,1})$, $(x-\beta_{1,2})(x-\beta_{2,3})$ and $(x-\beta_{1,3})(x-\beta_{2,2})$ are fixed by η, their discriminants are also fixed by η. Therefore, if the discriminant is fixed by σ, it is a rational number, that is, f is of type 3. □

Lemma 2. *If there is a non-trivial relation*

$$\sum_j m_{1,j}\beta_{1,j} + \sum_j m_{2,j}\beta_{2,j} = m \quad (m_{i,j}, m \in \mathbb{Q}), \tag{18}$$

then f *is of type* 2*, or there are rational numbers* m_1, m_2, m_3 *with* $m_i \neq m_j$ *for some* i, j *and* $m_1 + m_2 + m_3 = 0$ *such that*

$$m_1(\beta_{1,1}+\beta_{2,1}) + m_2(\beta_{1,2}+\beta_{2,3}) + m_3(\beta_{1,3}+\beta_{2,2}) = 0. \tag{19}$$

Proof. We may suppose that $m = 0$ in (18) by the remark at the beginning of this section, and acting $id, \sigma, \sigma^2, \eta, \eta\sigma, \eta\sigma^2$ in order, we have

$$m_{1,1}\beta_{1,1} + m_{1,2}\beta_{1,2} + m_{1,3}\beta_{1,3} + m_{2,1}\beta_{2,1} + m_{2,2}\beta_{2,2} + m_{2,3}\beta_{2,3} = 0, \tag{20}$$
$$m_{1,3}\beta_{1,1} + m_{1,1}\beta_{1,2} + m_{1,2}\beta_{1,3} + m_{2,3}\beta_{2,1} + m_{2,1}\beta_{2,2} + m_{2,2}\beta_{2,3} = 0, \tag{21}$$
$$m_{1,2}\beta_{1,1} + m_{1,3}\beta_{1,2} + m_{1,1}\beta_{1,3} + m_{2,2}\beta_{2,1} + m_{2,3}\beta_{2,2} + m_{2,1}\beta_{2,3} = 0, \tag{22}$$
$$m_{2,1}\beta_{1,1} + m_{2,3}\beta_{1,2} + m_{2,2}\beta_{1,3} + m_{1,1}\beta_{2,1} + m_{1,3}\beta_{2,2} + m_{1,2}\beta_{2,3} = 0, \tag{23}$$
$$m_{2,3}\beta_{1,1} + m_{2,2}\beta_{1,2} + m_{2,1}\beta_{1,3} + m_{1,3}\beta_{2,1} + m_{1,2}\beta_{2,2} + m_{1,1}\beta_{2,3} = 0, \tag{24}$$
$$m_{2,2}\beta_{1,1} + m_{2,1}\beta_{1,2} + m_{2,3}\beta_{1,3} + m_{1,2}\beta_{2,1} + m_{1,1}\beta_{2,2} + m_{1,3}\beta_{2,3} = 0. \tag{25}$$

Equations (20)+(23), (21)+(24), (22)+(25) are

$$\begin{pmatrix} m_{1,1}+m_{2,1} & m_{1,2}+m_{2,3} & m_{1,3}+m_{2,2} \\ m_{1,3}+m_{2,3} & m_{1,1}+m_{2,2} & m_{1,2}+m_{2,1} \\ m_{1,2}+m_{2,2} & m_{1,3}+m_{2,1} & m_{1,1}+m_{2,3} \end{pmatrix} \begin{pmatrix} \beta_{1,1}+\beta_{2,1} \\ \beta_{1,2}+\beta_{2,3} \\ \beta_{1,3}+\beta_{2,2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}. \tag{26}$$

If entries in each row of the coefficient matrix in (26) are the same, that is

$$\begin{cases} m_{1,1}+m_{2,1}=m_{1,2}+m_{2,3}=m_{1,3}+m_{2,2}:=a \text{ (say)},\\ m_{1,3}+m_{2,3}=m_{1,1}+m_{2,2}=m_{1,2}+m_{2,1}:=b,\\ m_{1,2}+m_{2,2}=m_{1,3}+m_{2,1}=m_{1,1}+m_{2,3}:=c, \end{cases}$$

then we have

$$\begin{cases} m_{2,3}=a-m_{1,2}=b-m_{1,3}=c-m_{1,1},\\ m_{2,2}=a-m_{1,3}=b-m_{1,1}=c-m_{1,2},\\ m_{2,1}=a-m_{1,1}=b-m_{1,2}=c-m_{1,3}, \end{cases}$$

hence

$$m_{1,3}=m_{1,1}+b-c=m_{1,1}+a-b=m_{1,1}-a+c,$$

which imply

$$b-c=a-b=-a+c, \quad \text{hence} \quad a=b=c.$$

Therefore, we get $m_{1,1}=m_{1,2}=m_{1,3}$ and $m_{2,1}=m_{2,2}=m_{2,3}$. The non-triviality of (20) implies $m_{1,1}\neq m_{2,1}$, hence comparing it with trivial relation $\sum_i \beta_{1,i}+\sum_i \beta_{2,i}=\mathrm{tr}\,(f)$, we see $\sum_i \beta_{1,i}\in\mathbb{Q}$. By lemma 1, f is of type 2.

If there are distinct entries in some row of the coefficient matrix in (26), then putting entries of the row by m_1, m_2, m_3, we have

$$m_1(\beta_{1,1}+\beta_{2,1})+m_2(\beta_{1,2}+\beta_{2,3})+m_3(\beta_{1,3}+\beta_{2,2})=0.$$

If $\mathrm{tr}\,(f)\neq 0$, then taking the trace, we have $(m_1+m_2+m_3)\mathrm{tr}\,(f)=0$, which implies $m_1+m_2+m_3=0$. If $\mathrm{tr}\,(f)=0$, then we have only to replace m_i by $m_i-(m_1+m_2+m_3)/3$.

Thus we have, by (19)

$$m_1(\beta_{1,1}+\beta_{2,1}-\beta_{1,3}-\beta_{2,2})+m_2(\beta_{1,2}+\beta_{2,3}-\beta_{1,3}-\beta_{2,2})=0,$$

where $m_1=m_2=0$ does not hold.

We divide the proof to several cases:

(I) Case of $m_1=0$ and $m_2\neq 0$: We have $\beta_{1,2}+\beta_{2,3}-\beta_{1,3}-\beta_{2,2}=0$, and $\beta_{1,3}+\beta_{2,1}-\beta_{1,1}-\beta_{2,3}=0$, acting σ. Therefore we find that $\beta_{1,1}-\beta_{2,1}=\beta_{1,3}-\beta_{2,3}=\beta_{1,2}-\beta_{2,2}$, which is σ-invariant, hence by Lemma 1, f is of type 3.

(II) Case of $m_1\neq 0$ and $m_2=0$: We have $\sigma(\beta_{1,1}+\beta_{2,1}-\beta_{1,3}-\beta_{2,2})=\beta_{1,2}+\beta_{2,2}-\beta_{1,1}-\beta_{2,3}=0$, and $\beta_{2,3}+\beta_{1,3}-\beta_{2,1}-\beta_{1,2}=0$, acting η. Hence, we find that $\sigma(\beta_{1,2}-\beta_{2,3})^2-(\beta_{1,2}-\beta_{2,3})^2=(\beta_{1,3}-\beta_{2,1}+\beta_{1,2}-\beta_{2,3})(\beta_{1,3}-\beta_{2,1}-\beta_{1,2}+\beta_{2,3})=0$ and so by Lemma 1, f is of type 3.

(III) Case of $m_1m_2\neq 0$: Dividing by m_2, we may suppose $m_2=1$, that is

$$m_1(\beta_{1,1}+\beta_{2,1}-\beta_{1,3}-\beta_{2,2})+(\beta_{1,2}+\beta_{2,3}-\beta_{1,3}-\beta_{2,2})=0 \qquad (27)$$

Suppose that $m_1 = 1$: Adding $3(\beta_{1,3} + \beta_{2,2})$ to the above, we have $\mathrm{tr}\,(f) = 3(\beta_{1,3}+\beta_{2,2})$. Acting σ, we have $\beta_{1,3}+\beta_{2,2} = \beta_{1,1}+\beta_{2,3} = \beta_{1,2}+\beta_{2,1} = \mathrm{tr}\,(f)/3$. Therefore, $f = (x-\beta_{1,3})(x-\beta_{2,2})\cdot(x-\beta_{1,1})(x-\beta_{2,3})\cdot(x-\beta_{1,2})(x-\beta_{2,1})$ is a polynomial in $x^2 - \mathrm{tr}\,(f)/3\cdot x$, that is decomposable.

Finally, we assume that $m_1 \neq 1$. Substituting $\beta_{1,2} + \beta_{2,3} = -(\beta_{1,1} + \beta_{2,1} + \beta_{1,3} + \beta_{2,2}) + \mathrm{tr}\,(f)$ to (27), we get

$$(m_1-1)(\beta_{1,1}+\beta_{2,1}) - (m_1+2)(\beta_{1,3}+\beta_{2,2}) = -\mathrm{tr}\,(f).$$

By denoting a cubic subfield fixed by η by M_3, it means

$$(m_1-1)\mathrm{tr}_{K/M_3}(\beta_{1,1}) - (m_1+2)\mathrm{tr}_{K/M_3}(\beta_{1,3}) = -\mathrm{tr}\,(f),$$

which completes the proof, putting

$$c = -(m_1+2)/(m_1-1), \quad \alpha = \beta_{1,1}, \quad \alpha' = \beta_{1,3}. \qquad \square$$

In [3], there are examples of a polynomial of type $2, 3$, but at that time the author did not recognize any S_3-type polynomial satisfying the last condition in Proposition 5. In the next section, we give examples.

Let us give a basis of linear relations of an irreducible abelian polynomial of degree 6 without proof to describe a set $\mathfrak{D}(f,\sigma)$.

Proposition 6. *Let f be an irreducible polynomial of degree 6 with a root α_1 and suppose that $\mathbb{Q}(\alpha_1)/\mathbb{Q}$ is an abelian extension of $\mathbb{Q}$ and let σ be an automorphism satisfying $\sigma(\alpha_i)=\alpha_{i+1}$ ($\alpha_i=\alpha_j$ for $i\equiv j \bmod 6$) for roots α_i of f. Then a basis of linear relations among roots are:*

(a) *In case that f is indecomposable and neither of type 2 nor of type 3.*

$$\sum_{i=1}^{6} \alpha_i = \mathrm{tr}\,(f).$$

(b) *in case that f is indecomposable and of type 2,*

$$\alpha_1+\alpha_3+\alpha_5 = \alpha_2+\alpha_4+\alpha_6 = \mathrm{tr}\,(f)/2.$$

(c) *In case that f is indecomposable and of type 3,*

$$\sum \alpha_i = \mathrm{tr}\,(f),\ \alpha_1+\alpha_2-(\alpha_4+\alpha_5)=0,\ \alpha_2+\alpha_3-(\alpha_5+\alpha_6)=0.$$

(d) *In case that $f(x) = g\big(h(x)\big)$ is possible for a cubic polynomial g, but impossible for a quadratic polynomial g,*

$$\alpha_1+\alpha_4 = \alpha_2+\alpha_5 = \alpha_3+\alpha_6 = \mathrm{tr}\,(f)/3.$$

(e) *In case that* $f(x) = g\bigl(h(x)\bigr)$ *is possible for a quadratic polynomial* g, *but impossible for a cubic polynomial* g,

$$\alpha_1 + \alpha_3 + \alpha_5 = \alpha_2 + \alpha_4 + \alpha_6 = \mathrm{tr}\,(f)/2.$$

(f) *In case that* f *is decomposable and* $f(x) = g\bigl(h(x)\bigr)$ *is possible for both* $\deg g = 2, 3$,

$$\alpha_1 + \alpha_4 = \alpha_2 + \alpha_5 = \alpha_3 + \alpha_6 = \mathrm{tr}\,(f)/3,\ \alpha_1 - \alpha_2 + \alpha_3 = \mathrm{tr}\,(f)/6.$$

Except this abelian case, even the classification of non-trivial relations is incomplete.

2. Expectation 2 for a polynomial of degree 6

We have no data to deny Expectation 2 for an irreducible and indecomposable polynomial f in the case of degree ≤ 5, but it fails in the case of degree 6. The two conditions irreducibility and indecomposability are equivalent to having no non-trivial linear relations among roots in the case of degree ≤ 5 as in the previous section. Data in [2] are less accurate in the case of degree 6, that is X in (11) was too small to guess the precise limit. We improve a method to guess the limit from approximate values.

Suppose that the limit in (11) exists and every $\mathrm{Pr}\,(f, L, \{R_i\})$ is rational: Then for the common denominator b, we see that

$$\sum_{\{R_i\}} \mathrm{Pr}\,(f, L, \{R_i\}) \cdot b = b,\ \mathrm{gcd}\left(\mathrm{gcd}_{\{R_i\}} \bigl(\mathrm{Pr}\,(f, L, \{R_i\}) \cdot b\bigr), b \right) = 1.$$

Supposing that b is less than 30000 and taking the above into account, let us consider integers d with $1 \leq d \leq 30000$, which satisfies

$$\sum_{\{R_i\}} r\bigl(\mathrm{Pr}_X(f, L, \{R_i\}) \cdot d\bigr) = d,\ \mathrm{gcd}\left(\mathrm{gcd}_{\{R_i\}} \Bigl(r\bigl(\mathrm{Pr}_X(f, L, \{R_i\}) \cdot d\bigr)\Bigr), d \right) = 1, \quad (28)$$

where $r(x)$ is an integer closest to x. Because, they must be satisfied if d is the common denominator of $\mathrm{Pr}\,(f, L, \{R_i\})$ and an approximation by $\mathrm{Pr}_X(f, L, \{R_i\})$ is sufficiently well. We consider the following four measures, abbreviating $\mathrm{Pr}_X(f, [3]L, \{R_i\})$ to Pr_{X,R_i}:

$$er_1 := \max_{\{R_i\}} \Bigl| \mathrm{Pr}_{X,R_i} \cdot d - r(\mathrm{Pr}_{X,R_i} \cdot d) \Bigr|,$$

$$er_2 := \sum_{\{R_i\}} \Bigl| \mathrm{Pr}_{X,R_i} \cdot d - r(\mathrm{Pr}_{X,R_i} \cdot d) \Bigr|^2,$$

$$er_3 := \max_{\{R_i\}} \left| \mathrm{Pr}_{X,R_i} - r(\mathrm{Pr}_{X,R_i} \cdot d)/d \right|,$$
$$er_4 := \sum_{\{R_i\}} \left| \mathrm{Pr}_{X,R_i} - r(\mathrm{Pr}_{X,R_i} \cdot d)/d \right|^2.$$

If $\mathrm{Pr}_X(f, L, \{R_i\})$ approximates a rational number a/b well, they are close to 0 for $d = b$. So, we can find the conjectural denominator b of $\mathrm{Pr}\,(f, L, \{R_i\})$ by checking that there is a large number X satisfying that there is an integer d with $1 \le d \le 30000$ which gives the common minimum for four measures above. The first two d-adic measures er_1, er_2 seem to be more appropriate.

We put

$$\begin{aligned}
f_1 &:= x^6 + 2x^5 + 4x^4 + x^3 + 2x^2 - 3x + 1,\\
f_2 &:= x^6 + 4x^5 + 16x^4 + 22x^3 + 39x^2 + 16x + 29,\\
f_3 &:= x^6 + 5x^5 + 11x^4 + 13x^3 + 23x^2 + 31x + 43,\\
f_4 &:= x^6 + 8x^5 + 43x^4 + 134x^3 + 372x^2 + 596x + 953.
\end{aligned}$$

They are irreducible and indecomposable and define the same cyclotomic field $\mathbb{Q}(\zeta_7)$, and the type of f_1, f_2 is 2 and that of f_3, f_4 is 3.

Let $L = 2$. A 6-tuple $(R_1, \ldots, R_6)$ with $0 \le R_i \le L - 1$ corresponds to an integer r with $1 \le r \le L^6$ by

$$r = 1 + \sum_{i=1}^{6} R_i L^{i-1}.$$

(I) The case that there is no non-trivial linear relation among roots:
For a polynomial $f = x^6 + 5x^5 + 1$ in [2], data were insufficient. Wrong values $7/512 = 0.0136\ldots, 9/512 = 0.0175\ldots$ on p.87 in [2] are close to the conjectural values $13/960 = 0.0135\ldots, 17/960 = 0.0177\ldots$ on p.84 respectively. The common denominator for four measures above is 960 for $X = 1.36 \cdot 10^{12}$ and the density matches with the conjecture (12). The density in (12) for $L = 2$ is given explicitly by

$$\mathrm{Pr}\,(f, 2, \{R_i\}) = \begin{cases} 13/960 & \text{if} \quad \mathrm{tr}\,(f) + \sum R_i \equiv 0 \bmod 2, \\ 17/960 & \text{if} \quad \mathrm{tr}\,(f) + \sum R_i \equiv 1 \bmod 2. \end{cases} \tag{29}$$

(II) Case that f is irreducible and indecomposable, and the type number is 2. For $f = f_1, f_2$, the common denominator of $\mathrm{Pr}_X(f, 2, \{R_i\})$ for four measures is 2304, which is attained for $X = 2 \cdot 10^{11}$. The following table of densities is arranged in the order of r above. For example, $(R_1, \ldots, R_6) = (0, \ldots, 0)$ corresponds to $r = 1$, and hence the density $\mathrm{Pr}\big(f_1, 2, (0, \ldots, 0)\big)$ is the first entry $36/2304$.

$$\begin{aligned}\Pr(f_1, 2, \{R_i\}) = [\,&36,\ \ 4, 15, 43, 43, 42, 23, 62, 29, 30, 35, 48, 36, 38, 49, 43,\\ &57, 29, 36, 38, 37, 40, 29, 42, 49, 54, 43, 30, 23, 29, 36,\ \ 4,\\ &68, 36, 43, 49, 42, 29, 18, 23, 30, 43, 32, 35, 34, 36, 43, 15,\\ &29, 23, 34, 36, 24, 37, 42, 43, 10, 49, 30, 29, 29, 57, 68, 36\,]/2304,\end{aligned}$$

$$\begin{aligned}\Pr(f_2, 2, \{R_i\}) = [\,&36, 68, 57, 29, 29, 30, 49, 10, 43, 42, 37, 24, 36, 34, 23, 29,\\ &15, 43, 36, 34, 35, 32, 43, 30, 23, 18, 29, 42, 49, 43, 36, 68,\\ &\ \ 4, 36, 29, 23, 30, 43, 54, 49, 42, 29, 40, 37, 38, 36, 29, 57,\\ &43, 49, 38, 36, 48, 35, 30, 29, 62, 23, 42, 43, 43, 15,\ \ 4, 36\,]/2304.\end{aligned}$$

Errors are

$$er_1(f_1) = 0.019615,\ er_1(f_2) = 0.026945.$$

The density of another polynomial f of type 2 for $L = 2$ seems to be given by the above according to $\operatorname{tr}(f) \bmod 4$. ($\operatorname{tr}(f)$ is an even integer in this case.) Let $f(x)$ be of type 2; then a polynomial $f(x-1)$ is also of type 2 and

$$\operatorname{tr}\bigl(f(x-1)\bigr) \equiv \operatorname{tr}\bigl(f(x)\bigr) + 2 \bmod 4 \quad \text{is easy.}$$

If $r_1, \dots, r_6$ are local roots with $r_i \equiv R_i \bmod 2$, then $r'_1 := r_1 + 1, \dots, r'_6 := r_6 + 1$ are also local roots of $f(x-1)$ with $r'_i \equiv R_i + 1 \bmod 2$. It is the reason why the densities $\Pr(f_1, 2, \{R_i\}), \Pr(f_2, 2, \{R_i\})$ are anti-symmetric. Some properties of $f = f_1, f_2$ are for $R = (R_1, \dots, R_6)$, $R' = (R'_1, \dots, R'_6)$,

(1) if $R_i + R'_i = 1$ for $1 \le {}^{\forall} i \le 6$, then $\Pr(f, 2, \{R_i\}) + \Pr(f, 2, \{R'_i\}) = 72/2304 = 1/32$,
(2) $\sum_{\sum R_i \equiv 0 \bmod 2} \Pr(f, 2, \{R_i\}) = \sum_{\sum R_i \equiv 1 \bmod 2} \Pr(f, 2, \{R_i\}) = 1/2$,
(3) if $R_i = 1 - R'_{7-i}$ for $1 \le {}^{\forall} i \le 6$, then $\Pr(f, 2, \{R_i\}) = \Pr(f, 2, \{R'_i\})$.

The third property is explained as follows: If we have $f(x) \equiv \prod(x - r_i) \bmod p$, then $f(-x) \equiv \prod(x - r'_i) \bmod p$ with $r'_i = p - r_{7-i}$ is easy to see. Hence the condition $r_i \equiv R_i \bmod 2$ implies $r'_i \equiv 1 - R_{7-i} \bmod 2$ for an odd prime p.
The author does not know how to give densities directly from $\{R_i\}$.

A basis of linear relations of $f = f_1,\ f_2$ with an appropriate numbering is

$$\alpha_1 + \alpha_3 + \alpha_5 = \alpha_2 + \alpha_4 + \alpha_6 = \operatorname{tr}(f)/2.$$

(III) The case that f is irreducible and indecomposable, and the type number is 3. For $f = f_3, f_4$, the common denominator of $\Pr_X(f, 2, \{R_i\})$ for four measures is 15120, which is attained for $X = 2 \cdot 10^{11}$. The following table of densities is arranged in the order of r as above.

$$\begin{aligned}\Pr(f_3, 2, \{R_i\}) = [&525, 189, 63, 414, 63, 229, 176, 159, 63, 224, 288, 172,\\ &544, 125, 204, 414, 63, 153, 394, 125, 288, 320, 300, 229,\\ &176, 401, 300, 224, 204, 153, 189, 189, 189, 189, 153, 204,\\ &224, 300, 401, 176, 229, 300, 320, 288, 125, 394, 153, 63,\\ &414, 204, 125, 544, 172, 288, 224, 63, 159, 176, 229, 63,\\ &414, 63, 189, 525]/15120,\end{aligned}$$

$$\begin{aligned}\Pr(f_4, 2, \{R_i\}) = [&420, 288, 180, 279, 162, 157, 140, 336, 162, 110, 174, 229,\\ &343, 176, 273, 279, 180, 84, 247, 176, 174, 485, 405, 157,\\ &140, 602, 405, 110, 273, 84, 42, 288, 288, 42, 84, 273,\\ &110, 405, 602, 140, 157, 405, 485, 174, 176, 247, 84, 180,\\ &279, 273, 176, 343, 229, 174, 110, 162, 336, 140, 157, 162,\\ &279, 180, 288, 420]/15120.\end{aligned}$$

Errors are

$$er_1(f_3) = 0.16450, er_1(f_4) = 0.16892.$$

We note that $\mathrm{tr}\,(f_3)$ is odd and $\mathrm{tr}\,(f_4)$ is even, and the density of another polynomial of type 3 for $L = 2$ seems to be given by the above according to $\mathrm{tr}\,(f) \bmod 2$.

A basis of linear relations of $f = f_3,\ f_4$ is

$$\sum \alpha_i = \mathrm{tr}\,(f),\ \alpha_1 + \alpha_2 = \alpha_4 + \alpha_5,\ \alpha_2 + \alpha_3 = \alpha_5 + \alpha_6.$$

(IV) The case that $K = \mathbb{Q}(\alpha_1)$ is an S_3-extension and there are a rational number c, two distinct roots α, α' of f, and a cubic subfield M_3 such that $\mathrm{tr}_{K/M_3}(\alpha) + c \cdot \mathrm{tr}_{K/M_3}(\alpha') \in \mathbb{Q}$. Let us give two examples:

The first example is $f = x^6 + 3$. Putting $y := \sqrt[6]{-3}$ with $y^3 = \sqrt{-3}$, roots are

$$\beta_{1,1} = y, \quad \beta_{1,2} = (-1 + \sqrt{-3})/2 \cdot y, \quad \beta_{1,3} = -(1 + \sqrt{-3})/2 \cdot y,$$

$$\beta_{2,1} = -y, \quad \beta_{2,2} = (1 - \sqrt{-3})/2 \cdot y, \quad \beta_{2,3} = (1 + \sqrt{-3})/2 \cdot y.$$

Automorphisms η, σ in the proof of Proposition 5 are given by $y \mapsto -y$, $y \mapsto (-1 + \sqrt{-3})/2 \cdot y$, respectively. A basis of linear relations is four equations

$$\beta_{1,2} = -\beta_{1,1} + \beta_{2,3}, \quad \beta_{1,3} = -\beta_{2,3}, \quad \beta_{2,1} = -\beta_{1,1}, \quad \beta_{2,2} = \beta_{1,1} - \beta_{2,3}.$$

The inclusion $\mathrm{tr}_{K/M_3}(\alpha) + c \cdot \mathrm{tr}_{K/M_3}(\alpha') \in \mathbb{Q}$ is obvious for $\alpha = y, c = 0$. Densities $\Pr(f, 2, \{R_i\})$ for $[R_1, \ldots, R_6]$ are given by:

$$\begin{cases} 1/16 & \text{for} \quad [1,1,1,0,0,0],\ [1,0,0,1,1,0],\ [0,1,0,1,0,1],\ [0,0,1,0,1,1], \\ 3/16 & \text{for} \quad [1,1,0,1,0,0],\ [1,0,1,0,1,0],\ [0,1,1,0,0,1],\ [0,0,0,1,1,1], \\ 0 & \text{otherwise.} \end{cases}$$

Since $-r$ is also a root for a local root r, a relation $r_i = p - r_{7-i}$ should hold for $i = 1, 2, 3$, hence $R_i + R_{7-i} \equiv 1 \bmod 2$, i.e., $R_i + R_{7-i} = 1$. This elucidates the cases of density 0.

The second example is $f = x^6 + 100x^4 - 168x^3 + 5200x^2 + 16800x + 26256$, and let β be a root. Then we see that roots $\alpha_1, \ldots, \alpha_6$ of f are in order $-1/2122960$ times -2122960β,

$$\begin{array}{rrrrrr}
-1757\beta^5 & +2758\beta^4 & -189756\beta^3 & +699188\beta^2 & -11117792\beta & -\ 9582496, \\
-1463\beta^5 & +\ 182\beta^4 & -158004\beta^3 & +159292\beta^2 & -\ 8902208\beta & -22357664, \\
125\beta^5 & +\ 710\beta^4 & +\ 13500\beta^3 & +131500\beta^2 & +\ 2458400\beta & +\ 6844000, \\
1088\beta^5 & -2312\beta^4 & +117504\beta^3 & -553792\beta^2 & +\ 7895888\beta & +\ 1825664, \\
2007\beta^5 & -1338\beta^4 & +216756\beta^3 & -436188\beta^2 & +11788672\beta & +23270496.
\end{array}$$

The polynomial f is irreducible, indecomposable and not of type $2, 3$, and we see

$$\alpha_1 + \alpha_6 + 3(\alpha_2 + \alpha_5) = 0$$

and

$$(\alpha_1 + \alpha_6)^3 = 756 = 28 \cdot 3^3$$

and

$$(\alpha_1 + \alpha_5)^3 = -224 = -28 \cdot 2^3.$$

Hence $\alpha_1 + \alpha_6$ is a trace to a cubic subfield defined by $x^3 - 756 = 0$, hence

$$\mathrm{tr}_{K/M_3}(\alpha) + c \cdot \mathrm{tr}_{K/M_3}(\alpha') \in \mathbb{Q} \quad \text{for} \quad \alpha = \alpha_1, \quad c = 3, \quad \alpha' = \alpha_2.$$

A basis of linear relations is three equations

$$\sum_i \alpha_i = 0,\ \alpha_1 + \alpha_6 + 3(\alpha_2 + \alpha_5) = 0,\ \ \alpha_1 + \alpha_5 - 2(\alpha_3 + \alpha_6) = 0.$$

And we see $(\alpha_3 + \alpha_6)^3 = -28$. The speed of convergence is slow,

$$er_1(f) > 0.3 \quad \text{even for} \quad X = 4 \cdot 10^{13}.$$

The author checked the following: Let us consider following 16 polynomials

$$\begin{array}{ll}
x^6 - 9x^4 - 4x^3 + 9x^2 + 3x - 1, & x^6 - 2x^3 + 9x^2 + 6x + 2, \\
x^6 - 7x^3 - 6x^2 - 9x - 3, & x^6 - 10x^4 - 4x^3 + 10x^2 - 1, \\
x^6 - 9x^4 - 8x^3 + 6x^2 + 6x + 1, & x^6 - 10x^4 - 7x^3 + 10x^2 - 1, \\
x^6 - 7x^4 + 8x^2 - 10x + 1, & x^6 - x^4 - 2x^3 + 7x^2 + x + 10, \\
x^6 - 8x^4 - 10x^3 - 3x^2 + 2x + 6, & x^6 - 5x^4 - 7x^3 - 3x^2 - x + 3, \\
x^6 - 10x^4 - 10x^3 - 10x^2 + 1, & x^6 - 9x^4 - 10x^3 - 2x^2 - 1,
\end{array}$$

$$x^6 - 10x^4 - 10x^3 - 10x^2 - 7, \qquad x^6 - 10x^4 - 8x^3 - 4x^2 + 8x - 2,$$
$$x^6 - 10x^4 - 10x^3 + 5x^2 - 2x + 9, \quad x^6 - 10x^4 - 10x^3 - 10x^2 - 10x - 10$$

which exhaust all types of Galois closure, checked by pari/gp. Take a root α of one of them and a polynomial f whose root is

$$\sum_{i=1}^{6} c_i \alpha^{i-1} \quad \text{with} \quad -1 \le c_i \le 1.$$

We consider irreducible and indecomposable ones of degree 6 only. We checked densities $\Pr_X(f, 2, \{R_i\})$ approximate well densities of special polynomials f_1, f_2, f_3, f_4 or (29), where we say that for a rational number a/b and a real number x, x approximates well a/b if the nearest integer $r(bx)$ to bx is a, i.e., $r(bx) = a$.

For a polynomial $f = x^6 - 3x^5 + 6x^4 + 3x^3 - 9x^2 - 18x + 36$ of type 3 and $\mathrm{tr}\,(f) \equiv 1 \bmod 2$, which is given in [2, (5) on p.87], $\Pr_X(f, 2, \{R_i\})$ $(X \le 10^{11})$ approximates well densities given above and the densities on p.87 in [2] should be corrected by the above.

REFERENCES

[1] DUKE, W.—FRIEDLANDER, J. B.—IWANIEC, H.: *Equidistribution of roots of a quadratic congruence to prime moduli*, Ann. of Math. (2) **141** (1995), no. 2, 423–441.

[2] HADANO, T.—KITAOKA, Y.—KUBOTA, T.—NOZAKI, M.: *Densities of sets of primes related to decimal expansion of rational numbers.* (W. Zhang and Y. Tanigawa, eds.) In: Number Theory: Tradition and Modernization, The 3rd China-Japan seminar on number theory, Xi'an, China, February 12–16, 2004. Developments. Math. Vol. 15, 2006, Springer, New York, pp. 67–80,

[3] KITAOKA, Y.: *A statistical relation of roots of a polynomial in different local fields*, Math. Comput. **78** (2009), no. 265, 523–536.

[4] ______ *A statistical relation of roots of a polynomial in different local fields II*, (Aoki, Takashi ed. et al.) In: Number Theory: Dreaming in Dreams, Proceedings of The 5th China-Japan seminar, Higashi-Osaka, Japan, August 27–31, 2008. Ser. Number Theory Appl. Vol. 6, 2010, World Sci. Publ., Hackensack, NJ, pp. 106–126.

[5] ______ *A statistical relation of roots of a polynomial in different local fields III*, Osaka J. Math. **49** (2012), 393–420.

[6] ______ *Statistical distribution of roots of a polynomial modulo prime powers*, In: Number Theory: Plowing and Starring through High Wave Forms, Ser. Number Theory Appl. Vol. 11, 2015, World Sci. publ., Hackensack, NJ, pp. 75–94.

[7] ______ *Statistical distribution of roots of a polynomial modulo primes*, (submitted).

[8] Y. KITAOKA: *Statistical distribution of roots of a polynomial modulo primes II*, Unif. Distrib. Theory **12** (2017), no. 1, 109–122.

[9] TÓTH, T. Á.: *Roots of Quadratic congruences*, Internat. Math. Res. Notices **2000**, no. 14, (2000) 719–739.

Received October 5, 2016
Accepted January 19, 2017

Yoshiyuki Kitaoka
Uzunawa 1085-10,
Asahi-cho,
Mie, 510-8104
JAPAN
E-mail: kitaoka@meijo-u.ac.jp