sciendo

uniform distribution theory

DOI: 10.2478/udt-2019–0006
Unif. Distrib. Theory **14** (2019), no.1, 87–104

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

Yoshiyuki Kitaoka

Author is retired, Asahi, JAPAN

ABSTRACT. Let $f(x)$ be a monic polynomial with integer coefficients and $0 \leq r_1 \leq \cdots \leq r_n < p$ its roots modulo a prime p. We generalize a conjecture on the distribution of roots r_i with additional congruence relations $r_i \equiv R_i \bmod L$ from the case that f has no non-trivial linear relation among roots to the case that f has a non-trivial linear relation.

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

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

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

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

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

$$f(x) \equiv \prod_{i=1}^{n}(x - r_i) \bmod p, \tag{2}$$

$$0 \leq r_1 \leq r_2 \leq \cdots \leq r_n < p. \tag{3}$$

The condition (2) is the definition of $p \in \mathrm{Spl}(f)$. We can determine local roots r_i uniquely with the global ordering (3). If $f(x), f'(x)$ are relatively prime

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

in $\mathbb{Z}/p\mathbb{Z}[x]$ and $a_0 \not\equiv 0 \bmod p$, then (3) is equivalent to $0 < r_1 < \cdots < r_n < p$. From now on, local roots r_i are supposed to satisfy conditions (2) and (3).

Let $\alpha_1, \ldots, \alpha_n \, (\in \mathbb{C})$ be roots of a polynomial f in (1) and we fix their numbering once and for all. Define a vector space LR over $\mathbb{Q}$ by

$$\mathrm{LR} := \left\{ (l_1, \ldots, l_{n+1}) \in \mathbb{Q}^{n+1} \,\middle|\, \sum_{i=1}^{n} l_i \alpha_i = l_{n+1} \right\}. \tag{4}$$

The vector $(1, \ldots, 1, -a_{n-1})$ is always in LR, hence $t := \dim_{\mathbb{Q}} \mathrm{LR} \geq 1$. We say that a polynomial f has a non-trivial linear relation among roots if $t > 1$. Put

$$\mathrm{Pr}_D(f, X) := \frac{\#\{p \in \mathrm{Spl}_X(f) \mid (r_1/p, \ldots, r_n/p) \in D\}}{\#\mathrm{Spl}_X(f)},$$
$$\mathrm{Pr}_D(f) := \lim_{X \to \infty} \mathrm{Pr}_D(f, X), \tag{5}$$

for a set $D \subset [0,1)^n$ with $D = \overline{D^\circ}$. Here we assume the existence of the limit, and so on. We stated the following Expectations 1, $1'$, $1''$, 2 in [K1] :

Expectation 1. If f has no non-trivial linear relation among roots, then

$$\mathrm{Pr}_D(f) = \frac{\mathrm{vol}\,(D \cap \hat{\mathfrak{D}}_n)}{\mathrm{vol}\,(\hat{\mathfrak{D}}_n)},$$

where

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

Here, $\hat{\mathfrak{D}}_n$ is contained in the union of hyperplanes $\{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid \sum_{i=1}^{n} x_i \in \mathbb{Z}\}$ and vol is the volume as an $(n-1)$-dimensional set. Let us consider a general polynomial, that is a polynomial which may have a non-trivial linear relation among roots, i.e. $t \geq 1$. Let

$$\hat{\boldsymbol{m}}_j := (m_{j,1}, \ldots, m_{j,n}, m_j) \ (j = 1, \ldots, t)$$

be a $\mathbb{Z}$-basis of $\mathrm{LR} \cap \mathbb{Z}^{n+1}$ and put $\boldsymbol{m}_j := (m_{j,1}, \ldots, m_{j,n})$. Since the conditions $(l_1, \ldots, l_{n+1}) \in \mathrm{LR}$ and $l_1, \ldots, l_n \in \mathbb{Z}$ imply $l_{n+1} \in \mathbb{Z}$ by roots α_i being algebraic integers, the set of vectors $\boldsymbol{m}_1, \ldots, \boldsymbol{m}_t$ is a $\mathbb{Z}$-basis of

$$\left\{ (l_1, \ldots, l_n) \in \mathbb{Z}^n \,\middle|\, \sum_{i=1}^{n} l_i \alpha_i \in \mathbb{Q} \right\}.$$

Proposition 1 in [K1] says that for a sufficiently large prime $p \in \mathrm{Spl}(f)$, there is at least one permutation $\sigma \in S_n$ dependent on p such that

$$\sum_{i=1}^{n} m_{j,i} r_{\sigma(i)} \equiv m_j \bmod p \quad (1 \leq {}^\forall j \leq t), \tag{6}$$

hence we have for some permutation σ and integers k_j $(j=1,\dots,t)$ dependent on a prime p

$$\sum_{i=1}^{n} m_{j,i} r_{\sigma(i)} = m_j + k_j p \quad (1 \le {}^{\forall} j \le t). \tag{7}$$

Once we take and fix bases $\hat{\boldsymbol{m}}_j$, the possibility of integers k_j is finite by $0 \le r_i < p$.

If f has no non-trivial linear relation, then $t=1$, $\hat{\boldsymbol{m}}_1 = (1,\dots,1,-a_{n-1})$ and (7) is, for a sufficiently large $p \in \mathrm{Spl}(f)$,

$$\sum_i r_i = -a_{n-1} + kp \quad (1 \le k < n).$$

Correlating with (6), we put, for a permutation $\sigma \in S_n$,

$$\mathrm{Spl}_X(f,\sigma) := \left\{ p \in \mathrm{Spl}_X(f) \,\middle|\, \sum_{i=1}^{n} m_{j,i} r_{\sigma(i)} \equiv m_j \bmod p \ (1 \le {}^{\forall} j \le t) \right\} \tag{8}$$

and

$$\mathfrak{D}(f,\sigma) := \left\{ (x_1 \dots, x_n) \in [0,1)^n \,\middle|\, \begin{array}{l} 0 \le x_1 \le \cdots \le x_n < 1, \\ \sum_{i=1}^{n} m_{j,i}\, x_{\sigma(i)} \in \mathbb{Z} \ (1 \le {}^{\forall} j \le t) \end{array} \right\}. \tag{9}$$

It is obvious that $\dim \mathfrak{D}(f,\sigma) \le n-t$. If f has no non-trivial linear relation among roots, then it is easy to see that $\mathrm{Spl}_X(f,\sigma) = \mathrm{Spl}_X(f)$ and $\mathfrak{D}(f,\sigma) = \hat{\mathfrak{D}}_n$ for any permutation σ. The following is a generalization of Expectation 1.

Expectation 1′.

$$\begin{aligned} \mathrm{Pr}_D(f,\sigma) :&= \lim_{X\to\infty} \frac{\#\{p \in \mathrm{Spl}_X(f,\sigma) \mid (r_1/p,\dots,r_n/p) \in D\}}{\#\mathrm{Spl}_X(f,\sigma)} \\ &= \frac{\mathrm{vol}(D \cap \mathfrak{D}(f,\sigma))}{\mathrm{vol}(\mathfrak{D}(f,\sigma))} \end{aligned} \tag{10}$$

for a permutation σ if $\dim \mathfrak{D}(f,\sigma) = n-t$, and vol is the volume as an $(n-t)$--dimensional set.

The expectation on the density of the set $\mathrm{Spl}_\infty(f,\sigma)$ is

Expectation 1″.

$$\mathrm{Pr}(f,\sigma) := \lim_{X\to\infty} \frac{\#\mathrm{Spl}_X(f,\sigma)}{\#\mathrm{Spl}_X(f)} = c^{-1} \cdot \mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big), \tag{11}$$

where the constant c is independent of σ.

The explicit value of c is given in Proposition 4 in the subsection 2.3 and by using it, Expectation 1 is generalized to a polynomial with a non-trivial linear relation among roots (see (30) in the subsection 2.4).

To state the distribution of roots r_i with congruence conditions

$$r_i \equiv R_i \bmod L \quad (i = 1, \ldots, n) \tag{12}$$

for given integers $L\,(\geq 2)$ and R_i, we introduced notations

$$\mathrm{Pr}_X(f, L, \{R_i\}) := \frac{\#\{p \in \mathrm{Spl}_X(f) \mid r_i \equiv R_i \bmod L \ (1 \leq {}^\forall i \leq n)\}}{\#\mathrm{Spl}_X(f)} \tag{13}$$

and

$$\mathrm{Pr}\,(f, L, \{R_i\}) := \lim_{X \to \infty} \mathrm{Pr}_X(f, L, \{R_i\}), \tag{14}$$

and proposed the following to a polynomial without non-trivial linear relation among roots.

Expectation 2.

$$\mathrm{Pr}\,(f, L, \{R_i\}) = \frac{1}{L^{n-1}} \sum_{k,\,q} \frac{E_n(k)}{[\mathbb{Q}(\zeta_L) : \mathbb{Q}(f) \cap \mathbb{Q}(\zeta_{L/d})]}, \tag{15}$$

where k, q run over a set of integers satisfying

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

and

$$\begin{cases} q \in (\mathbb{Z}/L\mathbb{Z})^\times, \\ a_{n-1} + \sum_{i=1}^n R_i \equiv kq \bmod L, \\ \big[[q]\big] = \big[[1]\big] \text{ on } \mathbb{Q}(f) \cap \mathbb{Q}(\zeta_{L/d}). \end{cases}$$

Here $E_n(k)$ is the volume of the set $\{\boldsymbol{x} \in [0,1)^{n-1} \mid k-1 < x_1 + \cdots + x_{n-1} \leq k\}$ and it is also given as $E_n(k) = A(n-1, k)/(n-1)!$, using Eulerian numbers $A(n, k)$ $(1 \leq k \leq n)$ defined recursively by

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

And 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 α_i of f. Lastly for an abelian field F in $\mathbb{Q}(\zeta_c)$ and an integer m relatively prime to c, $\big[[m]\big]$ denotes an automorphism of F induced by $\zeta_c \to \zeta_c^m$.

In the first section of this note, we review Expectation 2 and generalize it to a polynomial with a non-trivial linear relation among roots: Restricting a prime $p \in \mathrm{Spl}(f)$ by the condition (7), we introduce a more natural density $\mathrm{Pr}(f, \sigma, \{k_j\}, L, \{R_i\})$ than $\mathrm{Pr}(f, L, \{R_i\})$ in (14), which seems to take the same value independent of integers $\{R_i\}$ fixing a permutation σ and integers k_j in (7), if it does not vanish. In case of $\deg f = 1$, it is essentially equivalent to Dirichlet's prime number theorem on arithmetic progressions.

In the second section, we give several miscellaneous remarks on $Spl(f, \sigma)$, $\mathfrak{D}(f, \sigma)$ and the constant c in Expectation $1''$.

1.

To state the conjecture, we introduce following notations according to conditions (6), (7), (12):

$$\mathrm{Spl}_X(f, \sigma) = \left\{ p \in \mathrm{Spl}_X(f) \middle| \sum_{i=1}^{n} m_{j,i} r_{\sigma(i)} \equiv m_j \bmod p \, ({}^{\forall} j) \right\}, \quad (cf.\,(8))$$

$$\mathrm{Spl}_X(f, \sigma, \{k_j\}) := \left\{ p \in \mathrm{Spl}_X(f, \sigma) \middle| \sum_{i=1}^{n} m_{j,i} r_{\sigma(i)} = m_j + k_j p \, ({}^{\forall} j) \right\},$$

$$\mathrm{Spl}_X(f, \sigma, \{k_j\}, L, \{R_i\}) := \left\{ p \in \mathrm{Spl}_X(f, \sigma, \{k_j\}) \mid r_i \equiv R_i \bmod L \, ({}^{\forall} i) \right\},$$

$$\Pr(f, \sigma) = \lim_{X \to \infty} \frac{\# \mathrm{Spl}_X(f, \sigma)}{\# \mathrm{Spl}_X(f)}, \quad (cf.\,(11))$$

$$\Pr(f, \sigma, \{k_j\}) := \lim_{X \to \infty} \frac{\# \mathrm{Spl}_X(f, \sigma, \{k_j\})}{\# \mathrm{Spl}_X(f, \sigma)},$$

$$\Pr(f, \sigma, \{k_j\}, L, \{R_i\}) := \lim_{X \to \infty} \frac{\# \mathrm{Spl}_X(f, \sigma, \{k_j\}, L, \{R_i\})}{\# \mathrm{Spl}_X(f, \sigma, \{k_j\})},$$

where for the last two, the denominators $\# \mathrm{Spl}_X(f, \sigma), \# \mathrm{Spl}_X(f, \sigma, \{k_j\})$ of the right-hand sides are supposed to tend to the infinity.

The density $\Pr(f, \sigma)$ is given by (11), where the constant c will be given by Proposition 4 in the subsection 2.3. (11) implies that the density of $\mathrm{Spl}_\infty(f, \sigma)$ is positive if and only if the geometric condition $\dim \mathfrak{D}(f, \sigma) = n - t$ holds. It seems that two conditions $\# \mathrm{Spl}_\infty(f, \sigma) = \infty$ and $\Pr(f, \sigma) > 0$ are equivalent. What is the number of permutations σ with $\Pr(f, \sigma) > 0$ or $\dim \mathfrak{D}(f, \sigma) = n - t$?

Putting

$$D(\sigma, \{k_j\}) := \left\{ (x_1, \ldots, x_n) \middle| \left| \sum_{i=1}^{n} m_{j,i} x_{\sigma(i)} - k_j \right| \le 1/3 \, (j = 1, \ldots, t) \right\},$$

we see that for a sufficiently large $p \in \mathrm{Spl}_\infty(f, \sigma)$, the condition $(r_1/p, \ldots, r_n/p) \in D(\sigma, \{k_j\})$ is equivalent to (7). Hence the density $\Pr(f, \sigma, \{k_j\})$ is equal to the density $\Pr_D(f, \sigma)$ in Expectation $1'$ with $D = D(\sigma, \{k_j\})$, thus we have

$$\begin{aligned} \Pr(f,\sigma,\{k_j\}) &= \Pr_{D(\sigma,\{k_j\})}(f,\sigma) = \frac{\mathrm{vol}(D(\sigma,\{k_j\}) \cap \mathfrak{D}(f,\sigma))}{\mathrm{vol}(\mathfrak{D}(f,\sigma))} \\ &= \frac{\mathrm{vol}(\{(x_1,\dots,x_n) \mid 0 \le x_1 \le \cdots \le x_n < 1, \sum_i m_{j,i}x_{\sigma(i)} = k_j \ ({}^\forall j)\})}{\mathrm{vol}(\mathfrak{D}(f,\sigma))} \end{aligned} \tag{16}$$

by Expectation 1′.

Lastly, assume $\#\,\mathrm{Spl}_\infty(f,\sigma,\{k_j\}) = \infty$; then we expect that

$$\begin{aligned} &\Pr(f,\sigma,\{k_j\},L,\{R_i\}) \\ &= \begin{cases} \dfrac{1}{\#\mathfrak{R}(f,\sigma,\{k_j\},L)} & \text{if } \#\,\mathrm{Spl}_\infty(f,\sigma,\{k_j\},L,\{R_i\}) = \infty, \\ 0 & \text{otherwise,} \end{cases} \end{aligned} \tag{17}$$

where

$$\mathfrak{R}(f,\sigma,\{k_j\},L) := \big\{\{R_i\} \in [0,L-1]^n \mid \#\,\mathrm{Spl}_\infty(f,\sigma,\{k_j\},L,\{R_i\}) = \infty\big\}.$$

It is not easy to see whether $\#\,\mathrm{Spl}_\infty(f,\sigma,\{k_j\},L,\{R_i\}) = \infty$ or not. Suppose $\#\,\mathrm{Spl}_\infty(f,\sigma,\{k_j\},L,\{R_i\}) = \infty$; then there is a large prime $p \in \mathrm{Spl}(f)$ such that $\sum_i m_{j,i}r_{\sigma(i)} = m_j + k_jp$ and $r_i \equiv R_i \bmod L$, hence $\sum_i m_{j,i}R_{\sigma(i)} \equiv m_j + k_jp \bmod L$ $(j = 1,\dots,t)$. Thus the following condition (C_1) is satisfied:

> (C_1) : $(k_j, L) = (\sum_i m_{j,i}R_{\sigma(i)} - m_j, L)(= d_j$ say) and there is an integer q which is independent of j, relatively prime to L and satisfies that $\sum_i m_{j,i}R_{\sigma(i)} - m_j \equiv k_j \cdot q \bmod L$ and $[[q]] = [[1]]$ on $\mathbb{Q}(f) \cap \mathbb{Q}(\zeta_{L/d_j})$.

Data suggest that the condition (C_1) is also a sufficient condition, that is putting

$$\mathfrak{R}'(f,\sigma,\{k_j\},L) := \big\{\{R_i\} \in [0,L-1]^n \mid (C_1)\big\} \ \big(\supset \mathfrak{R}(f,\sigma,\{k_j\},L)\big),$$

we expect that

$$\mathfrak{R}(f,\sigma,\{k_j\},L) = \mathfrak{R}'(f,\sigma,\{k_j\},L) \ \text{ if } \ \#\,\mathrm{Spl}_\infty(f,\sigma,\{k_j\}) = \infty. \tag{18}$$

Example 1. Let us see the case of degree 1, i.e. $f(x) = x - a$: Then we see that the permutation σ is the identity, $t = 1$, $\hat{\boldsymbol{m}}_1 = (1,a)$, and the local root r_1 is equal to $a + k_1p$ for $k_1 = 0,1$ according to $a \ge 0$, $a < 0$ if $p > |a|$. Hence we have $\#\,\mathrm{Spl}_\infty(f,id,k_1) < \infty$ unless $k_1 = 0,1$ according to $a \ge 0$, $a < 0$. We consider only such an integer k_1 $(= 0$ or $1)$ and neglect a finite number of primes p less than or equal to $|a|$; then we see that

$$\begin{aligned} \mathrm{Spl}_X(f,id) &= \{p \le X\}, \\ \mathrm{Spl}_X(f,id,k_1) &= \{p \le X\}, \\ \mathrm{Spl}_X(f,id,k_1,L,R_1) &= \{p \le X \mid a + k_1p \equiv R_1 \bmod L\}, \end{aligned}$$

hence

$$\Pr(f, id) = \Pr(f, id, k_1) = 1$$

and

$$\Pr(f, id, k_1, L, R_1) = \begin{cases} 1 & \text{if } a \geq 0, a \equiv R_1 \bmod L, \\ 0 & \text{if } a \geq 0, a \not\equiv R_1 \bmod L, \\ \frac{1}{\varphi(L)} & \text{if } a < 0, (R_1 - a, L) = 1, \\ 0 & \text{if } a < 0, (R_1 - a, L) \neq 1 \end{cases}$$

by Dirichlet's theorem, and

$$\#\mathfrak{R}(f, id, k_1, L) = \begin{cases} 1 & \text{if } a \geq 0, \\ \varphi(L) & \text{if } a < 0. \end{cases}$$

Thus the conjecture (17) is nothing but Dirichlet's theorem. Since the condition (C_1) is : $d_1 := (R_1 - a, L) = (k_1, L) = L$ or 1 according to $a \geq 0$ or $a < 0$, and there is an integer q such that $(q, L) = 1$, $R_1 - a \equiv k_1 q \bmod L$, it is easy to see that (18) is true.

Example 2. Let us see that Expectation 2 follows from the conjectures (17), (18). Suppose that a polynomial f has no non-trivial linear relation among roots. So, we have $t = 1$, $\hat{\boldsymbol{m}}_1 = (1, \ldots, 1, -a_{n-1})$. The equation (15) in Expectation 2 is equivalent to

$$\Pr(f, L, \{R_i\}) = \frac{1}{L^{n-1}} \sum_{k_1} \frac{E_n(k_1)}{[\mathbb{Q}(\zeta_{L/d}) : \mathbb{Q}(f) \cap \mathbb{Q}(\zeta_{L/d})]}, \tag{19}$$

where k_1 satisfies that

$$1 \leq k_1 \leq n - 1,\, d := \Big(a_{n-1} + \sum R_i, L\Big) = (k_1, L),$$

and that there is an integer q such that $(q, L) = 1$, $(a_{n-1} + \sum R_i)/d \equiv k_1/d \cdot q \bmod L/d$ and $[[q]] = [[1]]$ on $\mathbb{Q}(f) \cap \mathbb{Q}(\zeta_{L/d})$, since the number of such integers q is $[\mathbb{Q}(\zeta_L) : \mathbb{Q}(\zeta_{L/d})]$ if there exists. We see that for any permutation σ

$$\begin{aligned} \mathrm{Spl}_X(f, \sigma) &= \mathrm{Spl}_X(f), \\ \mathrm{Spl}_X(f, \sigma, k_1) &= \Big\{p \in \mathrm{Spl}_X(f, \sigma) \Big| \sum r_i = -a_{n-1} + k_1 p\Big\}, \\ \mathrm{Spl}_X(f, \sigma, k_1, L, \{R_i\}) &= \Big\{p \in \mathrm{Spl}_X(f, \sigma, k_1) \mid r_i \equiv R_i \bmod L \,({}^\forall i)\Big\}. \end{aligned}$$

The identity $\Pr(f, \sigma) = 1$ is obvious. Since we know

$$\mathrm{vol}\Big(\{\boldsymbol{x} \in \hat{\mathfrak{D}}_n \big| \sum x_i = k_1\}\Big)/\mathrm{vol}(\hat{\mathfrak{D}}_n) = E_n(k_1),$$

we have

$$\Pr(f, \sigma, k_1) = E_n(k_1) \qquad \text{by (16).}$$

We see that the density in (14) is

$$\lim_{X\to\infty}\frac{\#\{p\in \mathrm{Spl}_X(f)\mid r_i\equiv R_i \bmod L\}}{\#\mathrm{Spl}_X(f)}$$

$$=\sum_{k_1=1}^{n-1}\lim_{X\to\infty}\frac{\#\{p\in \mathrm{Spl}_X(f)\mid r_i\equiv R_i \bmod L, \sum r_i=-a_{n-1}+k_1p\}}{\#\mathrm{Spl}_X(f)}$$

$$=\sum_{k_1=1}^{n-1}\lim_{X\to\infty}\frac{\#\,\mathrm{Spl}_X(f,\sigma,k_1,L,\{R_i\})}{\#\mathrm{Spl}_X(f)}$$

$$=\sum_{k_1=1}^{n-1}{}'\lim_{X\to\infty}\frac{\#\mathrm{Spl}_X(f,\sigma,k_1,L,\{R_i\})}{\#\mathrm{Spl}_X(f,\sigma,k_1)}\cdot\frac{\#\mathrm{Spl}_X(f,\sigma,k_1)}{\#\mathrm{Spl}_X(f,\sigma)}$$

where $\sum{}'$ means that k_1 satisfies the condition $\#\mathrm{Spl}_\infty(f,\sigma,k_1,L,\{R_i\})=\infty$, i.e. $\{R_i\}\in\mathfrak{R}(f,\sigma,k_1,L)$, then $\#\mathrm{Spl}_\infty(f,\sigma,k_1)=\infty$ is satisfied

$$=\sum_{k_1=1}^{n-1}{}'\mathrm{Pr}(f,\sigma,k_1,L,\{R_i\})\mathrm{Pr}(f,\sigma,k_1)$$

$$=\sum_{k_1=1}^{n-1}{}'\frac{E_n(k_1)}{\#\mathfrak{R}(f,\sigma,k_1,L)}\qquad\text{using (17).}$$

Put $d_1:=(k_1,L)$ and suppose $(\sum R_i+a_{n-1},L)=d_1$. Making use of $(\sum R_i+a_{n-1})/d_1\equiv k_1/d_1\cdot p \bmod L/d_1$, the mapping $\{R_i\}\mapsto[[p]]\in\mathrm{Gal}(\mathbb{Q}(\zeta_{L/d_1})/\mathbb{Q})$ tells us $\#\mathfrak{R}'(f,\sigma,k_1,L)=L^{n-1}[\mathbb{Q}(\zeta_{L/d_1}):\mathbb{Q}(f)\cap\mathbb{Q}(\zeta_{L/d_1})]$. Hence under the assumption (18), we obtain (15) in Expectation 2.

Putting

$$C(f,L,k):=\frac{E_n(k)}{L^{n-1}[\mathbb{Q}(\zeta_{L/d}):\mathbb{Q}(f)\cap\mathbb{Q}(\zeta_{L/d})]}\quad\big(d:=(k,L)\big),$$

we have checked for polynomials

$$x^2+1,\ x^3+2,\ x^4+x^3+x^2+x+1,\ x^5+2,\ x^6+x^5+x^4+x^3+x^2+x+1,$$

which have no non-trivial linear relation among roots that there is a large number $X(\le 10^{12})$ and $L\le 7$ such that

$$\left|\frac{\#\mathrm{Spl}_X(f,\sigma,k,L,\{R_i\})}{\#\mathrm{Spl}_X(f)}-C(f,L,k)\right|<C(f,L,k)/10$$

if $\#\mathrm{Spl}_X(f,\sigma,k,L,\{R_i\})>10$.

Example 3. Suppose that a polynomial $f(x) = (x^2 + ax)^2 + b(x^2 + ax) + c$ is irreducible. It is an irreducible polynomial of the least degree with a non-trivial linear relation. For roots β_1, β_2 of x^2+bx+c, denote roots of $x^2+ax = \beta_i$ by $\alpha_{i,j}$ $(j = 1, 2)$. Then we can take linear equations $\alpha_{i,1} + \alpha_{i,2} = -a$ $(i = 1, 2)$ as a basis of linear relations among roots of $f(x)$ ([K1]). By putting $\alpha_1 = \alpha_{1,1}, \alpha_2 = \alpha_{2,1}, \alpha_3 = \alpha_{2,2}, \alpha_4 = \alpha_{1,2}$, the relations $\alpha_1 + \alpha_4 = \alpha_2 + \alpha_3 = -a$ are a basis, hence we see that $t = 2$ and $\hat{\boldsymbol{m}}_1 = (1, 0, 0, 1, -a)$, $\hat{\boldsymbol{m}}_2 = (0, 1, 1, 0, -a)$. Let p be a large prime in $\mathrm{Spl}(f)$ and r_i local roots, which are supposed to satisfy $0 < r_1 < \cdots < r_4 < p$ by the assumption. Then, the induced local linear relations (7) among them are $r_1+r_4 = -a+p, r_2+r_3 = -a+p$ for a large prime p, hence a permutation σ with $\#\mathrm{Spl}(f, \sigma) = \infty$ satisfies $\{\sigma(1), \sigma(4)\} = \{1, 4\}$ or $\{2, 3\}$ with $k_1 = k_2 = 1$. For such permutations σ and $k_1 = k_2 = 1$, we see that $\mathrm{Spl}_X(f, \sigma, \{k_j\}) = \mathrm{Spl}_X(f)$ and $\mathrm{Spl}_X(f, \sigma, \{k_j\}, L, \{R_i\}) = \{p \in \mathrm{Spl}_X(f) \mid r_i \equiv R_i \bmod L\}$, neglecting a finite number of small primes. Our expectation with (18) is, for $\mathfrak{R}' = \mathfrak{R}'(f, \sigma, \{k_j\}, L)$

$$\Pr(f, \sigma, \{k_i\}, L, \{R_i\}) = \begin{cases} 1/\#\mathfrak{R}' & \text{if } (R_1, \ldots, R_4) \in \mathfrak{R}', \\ 0, & \text{otherwise.} \end{cases}$$

We have checked for $2 \le L \le 40$ and for polynomials in the following table below

[a,b,c]	G	Max. abelian subfield	Cond
$[10, 5, 7]$	D	$x^4 - x^2 + 1$	12
$[10, 2, 3]$	D	$x^4 + 1$	8
$[4, 4, 5]$	D	$x^4 + 3x^2 + 1$	20
$[9, -3, 3]$	D	$x^4 - x^3 - x^2 - 2x + 4$	21
$[-3, 0, 9]$	B	$x^4 - x^2 + 1$	12
$[-2, 1, 4]$	B	$x^4 - x^3 + 2x^2 + x + 1$	15
$[-4, 0, 9]$	B	$x^4 + 1$	8
$[-3, 4, 9]$	B	$x^4 + 3x^2 + 1$	20
$[0, 0, 1]$	B	$x^4 + 1$	8
$[-1, 3, 1]$	C	$x^4 - x^3 + x^2 - x + 1$	5
$[-9, 3, -9]$	C	$x^4 - x^3 - 4x^2 + 4x + 1$	15
$[-6, 8, -4]$	C	$x^4 - 5x^2 + 5$	20
$[-1, 7, 9]$	C	$x^4 - x^3 + 2x^2 + 4x + 3$	13
$[-8, -8, 8]$	C	$x^4 - 4x^2 + 2$	16
$[-6, 1, -4]$	C	$x^4 - x^3 - 6x^2 + x + 1$	17
$[-4, -2, -4]$	C	$x^4 - 10x^2 + 20$	40

that there is a number X ($\leq 10^{12}$) such that $|\mathrm{Pr}_X(f,\sigma,\{k_i\},L,\{R_i\})-1/\#\mathfrak{R}'| < 1/(10\#\mathfrak{R}')$ if $(R_1,\ldots,R_4)\in\mathfrak{R}'$. In the table, $[a,b,c]$ means a polynomial $f := (x^2+ax)^2+b(x^2+ax)+c$, and G is the Galois group $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$: D is the dihedral group of order 8, B is $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, and C means $\mathbb{Z}/4\mathbb{Z}$. "Max. abelian subfield" is a defining polynomial of the maximal abelian subfield of $\mathbb{Q}(f)$, which is of degree 4. "Cond" is its conductor.

Example 4. Let us give another example of a polynomial with a non-trivial linear relation among roots. Let

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

whose roots are

$$\begin{aligned} v =(&\zeta_7^3+\zeta_7, \quad \zeta_7^5+\zeta_7^4, \quad -\zeta_7^5-\zeta_7^4-\zeta_7^3-\zeta_7-1,\\ &\zeta_7^3+\zeta_7^2, \quad \zeta_7^5+\zeta_7, \quad -\zeta_7^5-\zeta_7^3-\zeta_7^2-\zeta_7-1)\end{aligned}$$

and the basis of linear relations among roots are $v_1+v_2+v_3=-1, v_4+v_5+v_6=-1$. Hence we have $t=2$ and (7) is

$$r_{\sigma(1)}+r_{\sigma(2)}+r_{\sigma(3)} = -1+k_1p,\ r_{\sigma(4)}+r_{\sigma(5)}+r_{\sigma(6)} = -1+k_2p.$$

We have only to consider the case $1\in\{\sigma(1),\sigma(2),\sigma(3)\}$, and then possible permutations σ and a pair $[k_1,k_2]$ of integers are following $(1),\ldots,(9.3)$:

	permutation, $[k_1,k_2]$
(1) :	$[1,2,3,4,5,6],[1,2],$
(2) :	$[1,2,4,3,5,6],[1,2],$
(3) :	$[1,2,5,3,4,6],[1,2],$
(4.1) :	$[1,2,6,3,4,5],[1,1],$
(4.2) :	$[1,2,6,3,4,5],[1,2],$
(4.3) :	$[1,2,6,3,4,5],[2,2],$
(5) :	$[1,3,4,2,5,6],[1,2],$
(6.1) :	$[1,3,6,2,4,5],[1,1],$
(6.2) :	$[1,3,6,2,4,5],[2,2],$
(7.1) :	$[1,4,5,2,3,6],[1,1],$
(7.2) :	$[1,4,5,2,3,6],[2,2],$
(8.1) :	$[1,4,6,2,3,5],[1,1],$
(8.2) :	$[1,4,6,2,3,5],[2,2],$
(9.1) :	$[1,5,6,2,3,4],[1,1],$
(9.2) :	$[1,5,6,2,3,4],[2,1],$
(9.3) :	$[1,5,6,2,3,4],[2,2],$

where a permutation σ is identified with the 6-tuple $[\sigma(1),\dots,\sigma(6)]$ of images. Then $\Pr(f,\sigma)$ is numerically 10/144, 24/144, 15/144, 13/144, 15/144, 18/144, 18/144, 18/144, 13/144 in order of permutations (1), (2), (3), (4), …, (9), and $\Pr(f,\sigma,\{k_j\})$ is 1, 1, 1, 8/13, 4/13, 1/13, 1, 2/3, 1/3, 1/2, 1/2, 1/3, 2/3, 1/13, 4/13, 8/13 in order of pairs of a permutation and $[k_1,k_2]$ (1), (2), (3), (4.1), (4.2), …, (9.3). We checked that there is a large integer $X(<10^{12})$ such that

$$\left|\frac{\#\mathrm{Spl}_X(f,\sigma,\{k_j\},L,\{R_i\})}{\#\mathrm{Spl}_X(f,\sigma)}-\frac{\Pr(f,\sigma,\{k_j\})}{\#\mathfrak{R}(f,\sigma,\{k_j\},L)}\right|<\frac{\Pr(f,\sigma,\{k_j\})}{10\#\mathfrak{R}(f,\sigma,\{k_j\},L)}$$

for $\{R_i\}$ satisfying $\#\mathrm{Spl}_X(f,\sigma,\{k_j\},L,\{R_i\})>10$ in the case of $L\le 8$. Data say that $\#\mathfrak{R}(f,\sigma,\{k_j\},8)=\#\mathfrak{R}'(f,\sigma,\{k_j\},8)=8192$ if $[k_1,k_2]=[2,2]$, otherwise 16384.

2.

Let us give several miscellaneous remarks on $\mathfrak{D}(f,\sigma)$, $\mathrm{Spl}(f,\sigma)$, the constant c in Expectation 1″ and $\Pr_D(f)$ of (5) in the case that f has a non-trivial linear relation. We put for $\boldsymbol{x}=(x_1,\dots,x_n), x\in\mathbb{R}$ and a permutation $\sigma\in S_n$

$$\sigma^{-1}(\boldsymbol{x}):=(x_{\sigma(1)},\dots,x_{\sigma(n)}),\ \sigma^{-1}((\boldsymbol{x},x)):=\big(\sigma^{-1}(\boldsymbol{x}),x\big), \tag{20}$$

2.1.

By definition (9), we see

$$\begin{aligned}&\mathfrak{D}(f,\sigma)\\&=\left\{\boldsymbol{x}=(x_1\dots,x_n)\in[0,1)^n\;\middle|\;\begin{array}{l}0\le x_1\le\dots\le x_n<1,\\ \big(\boldsymbol{m}_j,\sigma^{-1}(\boldsymbol{x})\big)\in\mathbb{Z}\text{ for }1\le{}^\forall j\le t\end{array}\right\}\\&=\left\{\boldsymbol{x}=(x_1\dots,x_n)\in[0,1)^n\;\middle|\;\begin{array}{l}0\le x_1\le\dots\le x_n<1,\\ \big(\sigma(\boldsymbol{m}_j),\boldsymbol{x}\big)\in\mathbb{Z}\text{ for }1\le{}^\forall j\le t\end{array}\right\}.\end{aligned}\tag{21}$$

The aim in this subsection is

Proposition 1. *Suppose that* $\mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big)>0$, *i.e.* $\dim\mathfrak{D}(f,\sigma)=n-t$; *then for a permutation* μ, *we have the equivalence*

$$\begin{aligned}&\mathrm{vol}\big(\mathfrak{D}(f,\sigma)\cap\mathfrak{D}(f,\mu)\big)>0\iff\mathfrak{D}(f,\sigma)=\mathfrak{D}(f,\mu)\\&\iff\langle\sigma(\boldsymbol{m}_1),\dots,\sigma(\boldsymbol{m}_t)\rangle_{\mathbb{Z}}=\langle\mu(\boldsymbol{m}_1),\dots,\mu(\boldsymbol{m}_t)\rangle_{\mathbb{Z}}\\&\iff\mu^{-1}\sigma\in G:=\{\nu\in S_n\mid\langle\nu(\boldsymbol{m}_1),\dots,\nu(\boldsymbol{m}_t)\rangle_{\mathbb{Z}}=\langle\boldsymbol{m}_1,\dots,\boldsymbol{m}_t\rangle_{\mathbb{Z}}\}.\end{aligned}$$

In particular, $\mathfrak{D}(f,\sigma)=\mathfrak{D}(f,\sigma\nu)$ *holds if and only if* $\nu\in G$.

P r o o f. Define a mapping ψ from $\mathfrak{D}(f,\sigma)$ to $\mathbb{Z}^t$ by $\psi(\boldsymbol{x})_j = \big(\sigma(\boldsymbol{m}_j), \boldsymbol{x}\big)$, and take an inverse image $\boldsymbol{x}_{\boldsymbol{k}}$ of $\boldsymbol{k}$, i.e. $\psi(\boldsymbol{x}_{\boldsymbol{k}}) = \boldsymbol{k}$. If $\psi(\boldsymbol{x}) = \psi(\boldsymbol{y})$ holds for $\boldsymbol{x}, \boldsymbol{y} \in \mathfrak{D}(f,\sigma)$, then we have $\big(\sigma(\boldsymbol{m}_j), \boldsymbol{x} - \boldsymbol{y}\big) = 0$. Therefore we have

$$\mathfrak{D}(f,\sigma) = \cup_{\boldsymbol{k}\in\psi(\mathfrak{D}(f,\sigma))} \big\{\hat{\mathfrak{D}}_n \cap \{\boldsymbol{x}_{\boldsymbol{k}} + \langle \sigma(\boldsymbol{m}_1), \dots, \sigma(\boldsymbol{m}_t)\rangle_{\mathbb{R}}^{\perp}\}\big\}. \tag{22}$$

Suppose that $\mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big) > 0$; if the property $\mathrm{vol}(\mathfrak{D}(f,\sigma) \cap \mathfrak{D}(f,\mu)) > 0$ holds, then (22) implies $\langle \sigma(\boldsymbol{m}_1), \dots, \sigma(\boldsymbol{m}_t)\rangle_{\mathbb{R}}^{\perp} = \langle \mu(\boldsymbol{m}_1), \dots, \mu(\boldsymbol{m}_t)\rangle_{\mathbb{R}}^{\perp}$, i.e.

$$\langle \sigma(\boldsymbol{m}_1), \dots, \sigma(\boldsymbol{m}_t)\rangle_{\mathbb{R}} = \langle \mu(\boldsymbol{m}_1), \dots, \mu(\boldsymbol{m}_t)\rangle_{\mathbb{R}}.$$

Since the matrix whose jth row is $\boldsymbol{m}_j$ is integral with every elementary divisor being 1, the above is equivalent to

$$\langle \sigma(\boldsymbol{m}_1), \dots, \sigma(\boldsymbol{m}_t)\rangle_{\mathbb{Z}} = \langle \mu(\boldsymbol{m}_1), \dots, \mu(\boldsymbol{m}_t)\rangle_{\mathbb{Z}}.$$

Conversely, suppose that the above is true. Then it is easy to see that

$$\boldsymbol{x} \in \mathfrak{D}(f,\sigma) \iff \boldsymbol{x} \in \mathfrak{D}(f,\mu) \qquad \text{by (21)},$$

hence $\mathfrak{D}(f,\sigma) = \mathfrak{D}(f,\mu)$. □

Remark The condition $\nu \in G$ is equivalent to

$$\begin{pmatrix} \nu^{-1}(\boldsymbol{m}_1) \\ \vdots \\ \nu^{-1}(\boldsymbol{m}_t) \end{pmatrix} = A \begin{pmatrix} \boldsymbol{m}_1 \\ \vdots \\ \boldsymbol{m}_t \end{pmatrix},$$

and if a polynomial f has no non-trivial linear relation among roots, then we have $G = S_n$ obviously.

Corollary 1. *We have*

$$\sum_{\mu\in S_n} \mathrm{vol}\big(\mathfrak{D}(f,\mu)\big) = \#G \cdot \mathrm{vol}\big(\cup_{\mu\in S_n} \mathfrak{D}(f,\mu)\big). \tag{23}$$

P r o o f. Put

$$S' := \big\{\sigma \in S_n \mid \mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big) > 0\big\}.$$

Then we have

$$\begin{aligned}\sum_{\sigma\in S_n} \mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big) &= \sum_{\sigma\in S'} \mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big) = \sum_{\mu\in S'/G} \sum_{\sigma\in\mu G} \mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big) \\ &= \#G \sum_{\mu\in S'/G} \mathrm{vol}\big(\mathfrak{D}(f,\mu)\big) = \#G \cdot \mathrm{vol}\big(\cup_{\mu\in S'/G} \mathfrak{D}(f,\mu)\big) \\ &= \#G \cdot \mathrm{vol}\big(\cup_{\mu\in S_n} \mathfrak{D}(f,\mu)\big).\end{aligned}$$

□

2.2.

Put
$$\hat{G} := \left\{ \nu \in S_n \,\middle|\, \sum_i m_{j,\nu(i)}\alpha_i = m_j \ (j = 1, \ldots, t) \right\}.$$

Since vectors $\hat{\boldsymbol{m}}_1, \ldots, \hat{\boldsymbol{m}}_n$ are a basis of linear relations LR (cf. (4)), there is an integral matrix A for $\nu \in \hat{G}$ such that, by the definition (20)

$$\begin{pmatrix} \nu^{-1}(\hat{\boldsymbol{m}}_1) \\ \vdots \\ \nu^{-1}(\hat{\boldsymbol{m}}_t) \end{pmatrix} = A \begin{pmatrix} \hat{\boldsymbol{m}}_1 \\ \vdots \\ \hat{\boldsymbol{m}}_t \end{pmatrix},$$

i.e.

$$\begin{pmatrix} m_{1,\nu(1)} & \ldots & m_{1,\nu(n)} & m_1 \\ \vdots & \ldots & \vdots & \vdots \\ m_{t,\nu(1)} & \ldots & m_{t,\nu(n)} & m_t \end{pmatrix} = A \begin{pmatrix} m_{1,1} & \ldots & m_{1,n} & m_1 \\ \vdots & \ldots & \vdots & \vdots \\ m_{t,1} & \ldots & m_{t,n} & m_t \end{pmatrix}. \tag{24}$$

Since the matrix whose jth row is $\hat{\boldsymbol{m}}_j$ is primitive, the left-hand side is also primitive, hence $A \in GL_t(\mathbb{Z})$. Conversely, (24) implies easily $\nu \in \hat{G}$. Therefore, the condition (24) is equivalent to $\nu \in \hat{G}$ and we see that

$$\hat{G} = \left\{ \nu \in S_n \mid \langle \nu(\hat{\boldsymbol{m}}_1), \ldots, \nu(\hat{\boldsymbol{m}}_t) \rangle_{\mathbb{Z}} = \langle \hat{\boldsymbol{m}}_1, \ldots, \hat{\boldsymbol{m}}_t \rangle_{\mathbb{Z}} \right\}$$

is a subgroup of G.

Remark. If $m_1 = \cdots = m_t = 0$, then $\hat{G} = G$ is obvious. If a polynomial f is irreducible, then $\sum_i m_{j,\nu(i)}\alpha_i = m_j$ implies $(\sum_i m_{j,\nu(i)})tr(\alpha_1) = nm_j$, and so the identity

$$\begin{pmatrix} m_{1,\nu(1)} & \ldots & m_{1,\nu(n)} \\ \vdots & \ldots & \vdots \\ m_{t,\nu(1)} & \ldots & m_{t,\nu(n)} \end{pmatrix} = A \begin{pmatrix} m_{1,1} & \ldots & m_{1,n} \\ \vdots & \ldots & \vdots \\ m_{t,1} & \ldots & m_{t,n} \end{pmatrix}$$

implies

$$\begin{pmatrix} m_1 \\ \vdots \\ m_t \end{pmatrix} = A \begin{pmatrix} m_1 \\ \vdots \\ m_t \end{pmatrix},$$

multiplying ${}^t(tr(\alpha_1)/n, \ldots, tr(\alpha_1)/n)$ from the right. Therefore, *if f is irreducible, then we have $\hat{G} = G$.* However, it is not necessarily true for a reducible polynomial. For example, let a polynomial f be $(x^2 + x + 1)(x^2 + 2x + 2)$ with roots $\alpha_1 = (-1+\sqrt{-3})/2, \alpha_2 = (-1-\sqrt{-3})/2, \alpha_3 = -1+\sqrt{-1}, \alpha_4 = -1-\sqrt{-1}$. Then we may choose obviously $\hat{\boldsymbol{m}}_1 = (1, 1, 0, 0, -1), \hat{\boldsymbol{m}}_2 = (0, 0, 1, 1, -2)$, thus a permutation $\nu = (1, 3)(2, 4)$ is in G, but not in $\hat{G}$.

To prove the next proposition, we introduce one more notation. For a prime $p \in \mathrm{Spl}(f)$, we take and fix a prime ideal $\mathfrak{p}$ of the field $\mathbb{Q}(f) = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ lying above p, and put

$$M_\mu := \{p \in \mathrm{Spl}(f) \mid \alpha_i \equiv r_{\mu(i)} \bmod \mathfrak{p} \ \ (i = 1, \ldots, n)\}.$$

It is clear that $\#(M_\sigma \cap M_\mu) = \infty$ implies $\alpha_{\sigma^{-1}\mu(i)} = \alpha_i$ $(i = 1, \ldots, n)$, hence $\sigma^{-1}\mu \in \hat{G}$, i.e. $\sigma\hat{G} = \mu\hat{G}$. The aim of this subsection is to show

Proposition 2. *We have*

$$\mathrm{Spl}(f, \sigma) = (\cup_\mu M_\mu) \cup T_\sigma \tag{25}$$

where μ runs over the set of permutations satisfying $\mu \in \sigma\hat{G}$ and $\#M_\mu = \infty$, and T_σ is a finite set.

Proof. Since $\mathrm{Spl}(f, \sigma) = \cup_{\mu \in S_n} \big(\mathrm{Spl}(f, \sigma) \cap M_\mu\big)$ by $\mathrm{Spl}(f) = \cup_{\mu \in S_n} M_\mu$, we have only to show that $\#\big(\mathrm{Spl}(f, \sigma) \cap M_\mu\big) = \infty$ if and only if $\mu\hat{G} = \sigma\hat{G}$ and $\#M_\mu = \infty$, and then $M_\mu \subset \mathrm{Spl}(f, \sigma)$. Suppose that $\#\big(\mathrm{Spl}(f, \sigma) \cap M_\mu\big) = \infty$. The property $\#M_\mu = \infty$ is clear. For $p \in \mathrm{Spl}(f, \sigma) \cap M_\mu$, we have

$$\sum_i m_{j,i} r_{\sigma(i)} \equiv m_j \bmod p, \ \ r_i \equiv \alpha_{\mu^{-1}(i)} \bmod \mathfrak{p},$$

which implies $\sum_i m_{j,i}\alpha_{\mu^{-1}\sigma(i)} \equiv m_j \bmod \mathfrak{p}$ for infinitely many primes in $p \in \mathrm{Spl}(f, \sigma) \cap M_\mu$, thus $\sum_i m_{j,i}\alpha_{\mu^{-1}\sigma(i)} = m_j$. It means $\mu^{-1}\sigma \in \hat{G}$, i.e. $\mu\hat{G} = \sigma\hat{G}$.

Conversely, suppose that $\mu\hat{G} = \sigma\hat{G}$ and $\#M_\mu = \infty$ hold; then we have $\sum_i m_{j,i}\alpha_{\mu^{-1}\sigma(i)} = m_j$. Hence, for $p \in M_\mu$, we see $\sum_i m_{j,i} r_{\sigma(i)} \equiv m_j \bmod \mathfrak{p}$, that is, $p \in \mathrm{Spl}(f, \sigma)$ and so $M_\mu \subset \mathrm{Spl}(f, \sigma)$, thus $\#(\mathrm{Spl}(f, \sigma) \cap M_\mu) = \infty$.

Therefore, the condition $\#\big(\mathrm{Spl}(f, \sigma) \cap M_\mu\big) = \infty$ is equivalent to $\#M_\mu = \infty$ and $\mu\hat{G} = \sigma\hat{G}$. And then, we have $M_\mu \subset \mathrm{Spl}(f, \sigma)$ as above. This completes the proof. □

Remark. The proposition says that the condition $\#\mathrm{Spl}(f, id) = \infty$ holds if and only if $\#M_\mu = \infty$ for some $\mu \in \hat{G}$. Suppose that $\mathbb{Q}(\alpha_1)$ is a Galois extension of $\mathbb{Q}$, and we take the prime ideal $\mathfrak{p} := (\alpha_1 - r_1, p)$ as a prime ideal to define the set M_μ. Using a polynomial $g_i \in \mathbb{Q}[x]$ defined by $\alpha_i = g_i(\alpha_1)$, we have $p \in M_\mu \iff g_i(r_1) \equiv r_{\mu(i)} \bmod p$.

Corollary 2. *We have*

$$\lim_{X\to\infty}\sum_{\sigma\in S_n}\frac{\#\mathrm{Spl}_X(f,\sigma)}{\#\mathrm{Spl}_X(f)}=\#\hat{G}. \tag{26}$$

P r o o f. Suppose $\#\mathrm{Spl}(f,\sigma)=\infty$. Let us see that the following three conditions are equivalent: (i) $\sigma\hat{G}=\nu\hat{G}$, (ii) there is a finite set T such that

$$\mathrm{Spl}(f,\sigma)\setminus T=\mathrm{Spl}(f,\nu)\setminus T,$$

(iii) $\#\big(\mathrm{Spl}(f,\sigma)\cap\mathrm{Spl}(f,\nu)\big)=\infty$. The condition (iii) implies that there are permutations μ_1,μ_1' such that $\mu_1\in\sigma\hat{G}$, $\mu_1'\in\nu\hat{G}$ and $\#(M_{\mu_1}\cap M_{\mu_1'})=\infty$, which implies $\mu_1\hat{G}=\mu_1'\hat{G}$, hence $\sigma\hat{G}=\nu\hat{G}$, i.e. (i). Suppose (i); then (ii) holds for $T=T_\sigma\cup T_\nu$. (ii) implies obviously (iii). Thus we have

$$\begin{aligned}&\lim_{X\to\infty}\sum_{\sigma\in S_n}\frac{\#\mathrm{Spl}_X(f,\sigma)}{\#\mathrm{Spl}_X(f)}\\&=\#\hat{G}\lim_{X\to\infty}\sum_{\sigma\in S_n/\hat{G}}\frac{\#\mathrm{Spl}_X(f,\sigma)}{\#\mathrm{Spl}_X(f)}\\&=\#\hat{G}\lim_{X\to\infty}\frac{\#(\cup_{\sigma\in S_n/\hat{G}}\mathrm{Spl}_X(f,\sigma))}{\#\mathrm{Spl}_X(f)}\\&=\#\hat{G}.\end{aligned}$$

□

Proposition 3. *Let σ,ν be permutations, and suppose that $\nu\in\hat{G}$. Then we have, neglecting a finite set of primes*

$$\mathrm{Spl}(f,\sigma)=\mathrm{Spl}(f,\sigma\nu^{-1}),$$

$$\mathrm{Spl}(f,\sigma,\{k_j\})=\mathrm{Spl}(f,\sigma\nu^{-1},\{k_j'\}), \tag{27}$$

$$\mathrm{Spl}(f,\sigma,\{k_j\},L,\{R_j\})=\mathrm{Spl}(f,\sigma\nu^{-1},\{k_j'\},L,\{R_j\}), \tag{28}$$

where ${}^t(k_1',\dots,k_t'):=A\cdot{}^t(k_1,\dots,k_t)$ *for the integral matrix* $A=(a_{ij})\in GL_t(\mathbb{Z})$ *given at* (24). *In particular, we have*

$$\mathrm{Pr}(f,\sigma)=\mathrm{Pr}(f,\sigma\nu^{-1}),$$

$$\mathrm{Pr}(f,\sigma,\{k_j\})=\mathrm{Pr}(f,\sigma\nu^{-1},\{k_j'\}),$$

$$\mathrm{Pr}(f,\sigma,\{k_j\},L,\{R_i\})=\mathrm{Pr}(f,\sigma\nu^{-1},\{k_j'\},L,\{R_i\}).$$

P r o o f. The first equation follows from the equivalence in the proof of the corollary above. Let p be a prime in $\mathrm{Spl}(f,\sigma,\{k_j\})$; then we see

$$\sum_i m_{j,i} r_{\sigma(i)} = m_j + k_j p \quad \text{and so} \quad \sum_j a_{l,j} \sum_i m_{j,i} r_{\sigma(i)} = \sum_j a_{l,j} m_j + \sum_j a_{l,j} k_j p,$$

that is,

$$\sum_i m_{l,\nu(i)} r_{\sigma(i)} = m_l + k_l' p,$$

which implies

$$p \in \mathrm{Spl}(f, \sigma\nu^{-1}, \{k_j'\}),$$

that is, $\mathrm{Spl}(f,\sigma,\{k_j\})$ is included in $\mathrm{Spl}(f,\sigma\nu^{-1},\{k_j'\})$. Since A^{-1} is also integral, we have the converse inclusion

$$\mathrm{Spl}(f,\sigma\nu^{-1},\{k_j'\}) \subset \mathrm{Spl}(f,\sigma,\{k_j\})$$

similarly, hence (27), (28). □

2.3.

We give the constant c in (11) explicitly.

Proposition 4.

$$c = [G : \hat{G}] \cdot \mathrm{vol}\big(\cup_{\sigma\in S_n} \mathfrak{D}(f,\sigma)\big).$$

P r o o f. Suppose that (11) is true; then we have

$$\lim_{X\to\infty} \sum_{\sigma\in S_n} \frac{\#\mathrm{Spl}_X(f,\sigma)}{\#\mathrm{Spl}_X(f)} = c^{-1} \sum_{\sigma\in S_n} \mathrm{vol}\big(\mathfrak{D}(f,\sigma)\big), \tag{29}$$

Applying Corollary 1, 2, we see

$$c = [G : \hat{G}] \cdot \mathrm{vol}\big(\cup_{\sigma\in S_n} \mathfrak{D}(f,\sigma)\big). \qquad \square$$

2.4.

If a polynomial f may have a non-trivial linear relation, then Expectation 1 is generalized as follows:

For a subset $D = \overline{D^\circ} \subset [0,1)^n$, we have

$$\mathrm{Pr}_D(f) = \frac{1}{\#G} \sum_{\sigma\in S_n} \frac{\mathrm{vol}(D \cap \mathfrak{D}(f,\sigma))}{\mathrm{vol}(\cup_{\sigma\in S_n} \mathfrak{D}(f,\sigma))}. \tag{30}$$

Because, we see that $\mathrm{Pr}_D(f)$ is, by definition (5) equal to

$$\lim_{X\to\infty}\frac{\#\{p\in \mathrm{Spl}_X(f)\mid (r_1/p,\dots,r_n/p)\in D\}}{\#\mathrm{Spl}_X(f)}$$

$$=\frac{1}{\#\hat{G}}\lim\sum_{\sigma\in S_n}{}'\frac{\#\{p\in \mathrm{Spl}_X(f,\sigma)\mid (r_1/p,\dots,r_n/p)\in D\}}{\#\mathrm{Spl}_X(f)}$$

$$=\frac{1}{\#\hat{G}}\lim\sum{}'\frac{\#\mathrm{Spl}_X(f,\sigma)}{\#\mathrm{Spl}_X(f)}\cdot\frac{\#\{p\in \mathrm{Spl}_X(f,\sigma)\mid (r_1/p,\dots,r_n/p)\in D\}}{\#\mathrm{Spl}_X(f,\sigma)}$$

$$=\frac{1}{\#\hat{G}}\lim\sum{}'\frac{\mathrm{vol}(\mathfrak{D}(f,\sigma))}{c}\cdot\frac{\mathrm{vol}(D\cap\mathfrak{D}(f,\sigma))}{\mathrm{vol}(\mathfrak{D}(f,\sigma))}\quad \text{by (11), (10)}$$

$$=\frac{1}{\#G}\frac{\sum_{\sigma\in S_n}\mathrm{vol}(D\cap\mathfrak{D}(f,\sigma))}{\mathrm{vol}(\cup_{\sigma\in S_n}\mathfrak{D}(f,\sigma))},$$

where $\sum'$ means that permutations $\sigma\in S_n$ with $\#\mathrm{Spl}_\infty(f,\sigma)<\infty$ are omitted.

Applicaton 1. Let us consider the case of a decomposable polynomial of degree 4. Let a polynomial $f(x)=(x^2+ax)^2+b(x^2+ax)+c$ be irreducible. Referring to Example 3 in the previous section, we see that

$$\{\sigma\mid \#\mathrm{Spl}(f,\sigma)=\infty\}=\big\{\sigma\mid \{\sigma(1),\sigma(4)\}=\{1,4\}\quad\text{or}\quad\{2,3\}\big\}=\hat{G}=G.$$

Only for such permutations, $\mathfrak{D}(f,\sigma)>0$ and $\mathfrak{D}(f,\sigma)=\mathfrak{D}(f,id)$ are easy, hence we have, by (30)

$$\mathrm{Pr}_D(f)=\frac{\mathrm{vol}(D\cap\mathfrak{D}(f,id))}{\mathrm{vol}(\mathfrak{D}(f,id))}. \tag{31}$$

Let us see that this implies the traditional equi-distribution of the sequence of $r_1/p,\dots,r_4/p$ in $[0,1)$. (cf. [K2] in the case that there is no non-trivial linear relation.)

Because, we have only to show

$$\frac{\sum_{p\in\mathrm{Spl}_X(f)}\#\{1\le i\le 4\mid r_i/p\le A\}}{4\#\mathrm{Spl}_X(f)}\to A\quad (0\le A<1).$$

By putting $D_i:=\{(x_1,\dots,x_4)\mid x_i\le A\}\cap\mathfrak{D}(f,id)$, (31) tells us that the left-hand side tends to

$$\sum_{i=1}^{4}\frac{1}{4}\frac{\mathrm{vol}(D_i)}{\mathrm{vol}(\mathfrak{D}(f,id))}, \tag{32}$$

using $\mathrm{Spl}_X(f) = \mathrm{Spl}_X(f, id)$. By $\mathfrak{D}(f, id) = \{(x_1, \ldots, x_4) \mid 0 \le x_1 \le \ldots \le x_4 < 1 \mid x_1 + x_4 = 1, x_2 + x_3 = 1\}$ we have

$$\mathfrak{D}(f, id) = \{(x_1, x_2, 1 - x_2, 1 - x_1) \mid 0 \le x_1 \le x_2 < 1/2\},$$

$$D_1 = \{(x_1, x_2, 1 - x_2, 1 - x_1) \mid 0 \le x_1 \le x_2 < 1/2, x_1 \le A\},$$

$$D_2 = \{(x_1, x_2, 1 - x_2, 1 - x_1) \mid 0 \le x_1 \le x_2 < \min(1/2, A)\},$$

$$D_3 = \{(x_1, x_2, 1 - x_2, 1 - x_1) \mid 0 \le x_1 \le x_2 < 1/2, 1 - x_2 \le A\},$$

$$D_4 = \{(x_1, x_2, 1 - x_2, 1 - x_1) \mid 0 \le x_1 \le x_2 < 1/2, 1 - x_1 \le A\},$$

and projecting them on the (x_1, x_2)-plane, we see

$$\mathrm{vol}\Big(\mathrm{pr}\big(\mathfrak{D}(f, id)\big)\Big) = 1/8,$$

$$\mathrm{vol}\big(\mathrm{pr}(D_1)\big) = \begin{cases} A/2 - A^2/2 & \text{if } A \le 1/2, \\ 1/8 & \text{if } A \ge 1/2, \end{cases}$$

$$\mathrm{vol}\big(\mathrm{pr}(D_2)\big) = \begin{cases} A^2/2 & \text{if } A \le 1/2, \\ 1/8 & \text{if } A \ge 1/2, \end{cases}$$

$$\mathrm{vol}\big(\mathrm{pr}(D_3)\big) = \begin{cases} 0 & \text{if } A \le 1/2, \\ (A - 1/2)/2 - (A - 1/2)^2/2 & \text{if } A \ge 1/2, \end{cases}$$

$$\mathrm{vol}\big(\mathrm{pr}(D_4)\big) = \begin{cases} 0 & \text{if } A \le 1/2, \\ (A - 1/2)^2/2 & \text{if } A \ge 1/2. \end{cases}$$

Thus we see that (32) is equal to A.

REFERENCES

[K1] KITAOKA, Y.: Notes on the distribution of roots modulo a prime of a polynomial, Unif. Distrib. Theory **12** (2017), no. 2, 91–116.

[K2] ______ *Statistical distribution of roots of a polynomial modulo primes III*, Int. J. Statist. Probab. **7** (2018), 115–124.

Received March 16, 2018
Accepted August 28, 2018

Yoshiyuki Kitaoka
Author is retired,
Asahi
JAPAN
E-mail: kitaoka@meijo-u.ac.jp