Bull. Math. Soc. Sci. Math. Roumanie
Tome 66 (114), No. 3, 2023, 355–359

On correspondence between roots of polynomial congruences and degree one ideals

by
Chunlin Wang

Abstract

It is known from Kummer-Dedekind factorization theorem that roots of a polynomial congruence modulo a prime ideal are one to one correspondence to degree one prime ideals in its extension field. In this note, we give a generalization of this well known fact.

Key Words: Dedekind-Kummer Theorem, degree one ideals, polynomial congruences.
2010 Mathematics Subject Classification: Primary 11R04; Secondary 11R09.

1 Introduction

Throughout this note, let A be a Dedekind domain with fraction field K, L be a finite separable extension of K and B be the integral closure of A in L. It is well known that B is also a Dedekind domain. Suppose $L = K(\alpha)$ for some $\alpha \in B$. Let $m(x) \in A[x]$ be the monic minimal polynomial of α. Denote by $\mathfrak{F}$ the conductor of $A[\alpha]$ in B, i.e.,

$$\mathfrak{F} := \{a \in B \mid aB \in A[\alpha]\}.$$

We have the famous Kummer-Dedekind Theorem (cf. [2], Proposition 8.3, Chapter 1) for the factorization of prime ideals of A in B.

Theorem 1. *Let $\mathfrak{p}$ be a prime ideal of A such that $\mathfrak{p}B + \mathfrak{F} = B$. Assume $m(x) \equiv m_1(x)^{e_1} \cdots m_r(x)^{e_r} \mod \mathfrak{p}$, where $m_1, \ldots, m_r$ are monic polynomials in $A[x]$ whose residues mod $\mathfrak{p}$ are irreducible. Then*

$$\mathfrak{P}_i = \mathfrak{p}B + m_i(\alpha)B, \quad i = 1, \ldots, r, \tag{1.1}$$

are prime ideals of B above $\mathfrak{p}$. The inertia degree f_i of $\mathfrak{P}_i$ equals to the degree of m_i, and one has

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

Recall that $\mathfrak{P}_i$ is said to be ramified if $e_i > 1$, otherwise it is unramified, and $\mathfrak{P}_i$ is a degree one ideal if its inertia degree is one. If $\mathfrak{P}_i$ is of degree one, then (1.1) becomes $\mathfrak{P}_i = \mathfrak{p}B + (\alpha - v)B$, which is denoted by $\mathfrak{P}_i = (\alpha - v, \mathfrak{p})$ sometimes, for some $v \in A$ satisfying $m(v) \equiv 0 \mod \mathfrak{p}$. The one to one correspondence between the degree one ideals over $\mathfrak{p}$ and the roots of the polynomial congruence $m(v) \equiv 0 \mod \mathfrak{p}$ is implied in Theorem

1. The main purpose of the article is to extend this correspondence to a more general setting.

We start with a generalization of degree one prime ideals. Obviously a prime ideal $\mathfrak{P}$ of B is of degree one if and only if

$$B/\mathfrak{P} \cong A/(\mathfrak{P} \cap A).$$

This enables us to generalize the definition of degree one prime ideals. Let $\mathfrak{b}$ be any ideal of B and $\mathfrak{a} := \mathfrak{b} \cap A$. Then $A/\mathfrak{a}$ is a subring of $B/\mathfrak{b}$. We say that $\mathfrak{b}$ is of degree one if $A/\mathfrak{a} \cong B/\mathfrak{b}$. We have the following result for degree one ideals.

Theorem 2. *Let $\mathfrak{b} \subset B$ be an ideal and $\mathfrak{b} = \mathfrak{P}_1^{k_1} \cdots \mathfrak{P}_s^{k_s}$ be its unique factorization into prime ideals. Denote by $\mathfrak{p}_i = \mathfrak{P}_i \cap A$. Then $\mathfrak{b}$ is a degree one ideal if and only if all the following three are true:*

(a) *each $\mathfrak{P}_i$ is of degree one;*

(b) *$k_i = 1$ if $\mathfrak{P}_i$ is ramified;*

(c) *for each pair of i, j with $1 \leq i < j \leq s$, $\mathfrak{p}_i$ and $\mathfrak{p}_j$ are relatively prime.*

To state our main result, we introduce some notations. Let $\alpha_1, ..., \alpha_n$ be elements in B such that $L = K(\alpha_1, ..., \alpha_n)$. Denote by $g_i(x)$ the monic minimal polynomial of α_i over K. Let $\mathfrak{d}_i$ be the discriminant of g_i, i.e., $\mathfrak{d}_i$ is the discriminant of $1, \alpha_i, ..., \alpha_i^{\deg g_i - 1}$ with respect to the field extension $K(\alpha_i)/K$. Suppose that

$$[L : K] = \prod_{i=1}^{n} [K(\alpha_i) : K]. \tag{1.2}$$

Then $g_i(x)$ is again the minimal polynomial of α_i over $K(\alpha_1, ..., \hat{\alpha}_i, ..., \alpha_n)$, where $\hat{\alpha}_i$ means the term α_i is omitted.

Theorem 3. *Let α_i, g_i and $\mathfrak{d}_i$ be given as above such that (1.2) is true. For an ideal $\mathfrak{a} \subset A$ satisfying that $\mathfrak{a}A + \mathfrak{d}_i A = A$ for all $1 \leq i \leq n$, let*

$$\mathcal{R} := \{(v_1, ..., v_n) \in (A/\mathfrak{a})^n \mid g_i(v_i) \equiv 0 \mod \mathfrak{a}\}$$

and

$$\mathcal{I} := \{\mathfrak{b} \subset B \mid \mathfrak{b} \text{ is of degree one with } \mathfrak{b} \cap A = \mathfrak{a}\}.$$

Define

$$\varphi((v_1, ..., v_n)) := (\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{a}), \forall (v_1, ..., v_n) \in \mathcal{R},$$

where $(\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{a})$ denotes the ideal of B generated by $\alpha_1 - v_1, ..., \alpha_n - v_n$ and $\mathfrak{a}$. Then φ is a bijection from $\mathcal{R}$ to $\mathcal{I}$, and its inverse is

$$\psi : \mathcal{I} \to \mathcal{R},\ \psi(\mathfrak{b}) := (\alpha_1 \bmod \mathfrak{b}, ..., \alpha_n \bmod \mathfrak{b}).$$

When A is the ring of integers, it is known that (1.2) is true if $\mathfrak{d}_i, \mathfrak{d}_j$ are relatively prime for each pair of $1 \leq i < j \leq n$. The following corollary of Theorem 3 is used in [3] to study the distribution of roots of a system of polynomial congruences.

Corollary 1. *For $1 \leq i \leq n$, let $g_i(x)$ be a monic irreducible polynomial over $\mathbb{Z}$ with discriminant $\mathfrak{d}_i$, and α_i be a root of g_i in $\bar{\mathbb{Q}}$. Suppose that $(\mathfrak{d}_i, \mathfrak{d}_j) = 1$ for all $1 \leq i < j \leq n$. Then for any positive integer l with $(l, \mathfrak{d}_i) = 1$ for $1 \leq i \leq n$, each degree one ideal of $\mathbb{Q}(\alpha_1, ..., \alpha_n)$ above l can be written as $(\alpha_1 - v_1, ..., \alpha_n - v_n, l)$, where v_i satisfy $g_i(v_i) \equiv 0$ mod l and are uniquely determined up to modulo l.*

2 Proofs

Proof of Theorem 2. For any prime ideal $\mathfrak{p}$ that appears in the set $\{\mathfrak{p}_i : 1 \le i \le s\}$, we have

$$A \cap \mathfrak{b} = A \cap \Big(\prod_{\substack{1 \le i \le s \\ \mathfrak{p}_i = \mathfrak{p}}} \mathfrak{P}_i^{k_i} \cdot \prod_{\substack{1 \le i \le s \\ \mathfrak{p}_i \ne \mathfrak{p}}} \mathfrak{P}_i^{k_i} \Big) = \Big(A \cap \prod_{\substack{1 \le i \le s \\ \mathfrak{p}_i = \mathfrak{p}}} \mathfrak{P}_i^{k_i} \Big) \cdot \Big(A \cap \prod_{\substack{1 \le i \le s \\ \mathfrak{p}_i \ne \mathfrak{p}}} \mathfrak{P}_i^{k_i} \Big).$$

It is easy to see that

$$A \cap \prod_{\substack{1 \le i \le s \\ \mathfrak{p}_i = \mathfrak{p}}} \mathfrak{P}_i^{k_i} = \min_{\substack{1 \le i \le s \\ \mathfrak{p}_i = \mathfrak{p}}} \{A \cap \mathfrak{P}_i^{k_i}\},$$

where $\min_{\substack{1 \le i \le s \\ \mathfrak{p}_i = \mathfrak{p}}} \{A \cap \mathfrak{P}_i^{k_i}\}$ denotes the smallest ideal of the form $A \cap \mathfrak{P}_i^{k_i}$ with $\mathfrak{p}_i = \mathfrak{p}$. From the two equations we may conclude that there are integers $i_1, ..., i_t$ such that

$$A \cap \mathfrak{P}_1^{k_1} \cdots \mathfrak{P}_s^{k_s} = (A \cap \mathfrak{P}_{i_1}^{k_{i_1}}) \cdots (A \cap \mathfrak{P}_{i_t}^{k_{i_t}}),$$

and $A \cap \mathfrak{P}_{i_l}$ are different prime ideals in A for all $1 \le l \le t$. So $A/(A \cap \mathfrak{b})$ is a subring of $\bigoplus_{i=1}^s A/(A \cap \mathfrak{P}_i^{k_i})$. Moreover, since each $A/(A \cap \mathfrak{P}_i^{k_i})$ is a subring of $B/\mathfrak{P}_i^{k_i}$, it follows that $\bigoplus_{i=1}^s A/(A \cap \mathfrak{P}_i^{k_i})$ is a subring of $B/\mathfrak{b}$. Therefore $\mathfrak{b}$ is a degree one ideal if and only if

$$A/(A \cap \mathfrak{b}) \cong \bigoplus_{i=1}^{s} A/(A \cap \mathfrak{P}_i^{k_i}) \cong B/\mathfrak{b}.$$

The first $\cong$ happens if and only if $A \cap \mathfrak{P}_1^{k_1}, ..., A \cap \mathfrak{P}_s^{k_s}$ are pairwisely coprime. The second $\cong$ holds if and only if $A/(A \cap \mathfrak{P}_i^{k_i}) \cong B/\mathfrak{P}_i^{k_i}$ for each i, if and only if each $\mathfrak{P}_i$ is of degree one and $k_i = 1$ for ramified $\mathfrak{P}_i$. This proves Theorem 2. □

Proof of Theorem 3. Let $v_1, .., v_n$ be elements of A such that $g_i(v_i) \equiv 0 \mod \mathfrak{a}$. First we show $(\alpha_1 - v_1, \ldots, \alpha_n - v_n, \mathfrak{a}) \subset B$ is a degree one ideal.

If $\mathfrak{a}$ is a prime ideal, then $(\alpha_1 - v_1, \mathfrak{a})$ is a degree one prime ideal of $K(\alpha_1)$. By (1.2), one deduces that $g_2(x)$ is the monic minimal polynomial of α_2 over $K(\alpha_1)$. Then the discriminant of $1, \alpha_2, \alpha_2^2 ..., \alpha_2^{\deg g_2 - 1}$ with respect to the field extension $K(\alpha_1, \alpha_2)/K(\alpha_1)$ is also $\mathfrak{d}_2$. Let $B_1, B_{1,2}$ be the integral closure of A in $K(\alpha_1)$ and $K(\alpha_1, \alpha_2)$ respectively. Then the conductor of $B_1[\alpha_2]$ in $B_{1,2}$ divides $\mathfrak{d}_2$. So by $(\mathfrak{a}, \mathfrak{d}_2) = 1$, we derive that $(\alpha_1 - v_1, \alpha_2 - v_2, \mathfrak{a})$ is a degree one prime ideal of $K(\alpha_1, \alpha_2)$. Inductively we can show that $(\alpha_1 - v_1, \ldots, \alpha_i - v_i, \mathfrak{a})$ is a degree one prime ideal of $K(\alpha_1, ..., \alpha_i)$ for all i with $1 \le i \le n$. Specially, $(\alpha_1 - v_1, \ldots, \alpha_n - v_n, \mathfrak{a})$ is a degree one prime ideal of L if $\mathfrak{a}$ is a prime ideal of A. We can also see that $(v_1', \ldots, v_n', \mathfrak{a})$ is different from $(v_1, \ldots, v_n, \mathfrak{a})$ if $(v_1', \ldots, v_n')$ and $(v_1, \ldots, v_n)$ are different elements of $\mathcal{R}$.

Assume $\mathfrak{a}$ is a power of a prime ideal. Write $\mathfrak{a} = \mathfrak{p}^k$. Claim that

$$(\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{p}^k) = (\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{p})^k.$$

The ideal $(\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{p})$ has been proved to be a degree one prime ideal. On the other hand $(\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{p})$ is unramified if $\mathfrak{p}$ is relatively prime to each $\mathfrak{d}_i$. So one deduces from the claim and Theorem 2 that $(\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{p}^k)$ is a degree one ideal. We show the validity of the claim below.

Denote again by B_1 the integral closure of A in $K(\alpha_1)$ and $(\alpha_1-v_1,\mathfrak{a})$ the ideal generated by $\alpha_1 - v_1$ and $\mathfrak{a}$ in B_1. We have already known $(\alpha_1 - v_1, \mathfrak{p})$ is a prime ideal of degree one. In addition $(\alpha_1 - v_1, \mathfrak{p})$ is the only prime ideal of B_1 that divides both $\alpha_1 - v_1$ and $\mathfrak{p}B_1$. Then $\alpha_1 - v_1 = (\alpha_1 - v_1, \mathfrak{p})^l I$ for $l > 0$ and some ideal $I \subset B_1$ with $I + \mathfrak{p}B_1 = B_1$. It follows that

$$N_{B_1/A}((\alpha_1 - v_1)B_1) = g_1(v_1)A = \mathfrak{p}^l N_{B_1/A}(I),$$

where $N_{B_1/A}$ denotes the ideal norm of B_1/A and we used the fact that $N_{B_1/A}((\alpha_1 - v_1, \mathfrak{p})^l) = \mathfrak{p}^l$. From $g_1(v_1) \equiv 0 \mod \mathfrak{p}^k$ and $(N_{B_1/A}(I), \mathfrak{p}) = 1$, one induces $l \geq k$. So

$$(\alpha_1 - v_1, \mathfrak{p}^k) = (\alpha_1 - v_1, \mathfrak{p})^k.$$

Therefore

$$(\alpha_1 - v_1, \alpha_2 - v_2, \mathfrak{p}^k) = (\alpha_2 - v_2, (\alpha_1 - v_1, \mathfrak{p})^k).$$

Replacing $\mathfrak{p}$ by $(\alpha_1 - v_1, \mathfrak{p})$ and repeating above discussion, one derives that

$$(\alpha_2 - v_2, (\alpha_1 - v_1, \mathfrak{p})^k) = (\alpha_2 - v_2, \alpha_1 - v_1, \mathfrak{p})^k.$$

Continue this process by induction on n, we eventually arrived at the claimed equality.

Now we are ready to consider general ideals $\mathfrak{a}$. Write $\mathfrak{a} = \prod_{i=1}^{s} \mathfrak{p}_i^{k_i}$. We know each $(\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{p}_i^{k_i})$ is of degree one. Since

$$(\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{a}) \subset (\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{p}_i^{k_i})$$

for each i with $1 \leq i \leq s$. So

$$(\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{a}) \subset \prod_{i=1}^{s} (\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{p}_i^{k_i}).$$

By comparing the generators of each side, one is easy to see

$$\prod_{i=1}^{s} (\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{p}_i^{k_i}) \subset (\alpha_1 - v_1, ..., \alpha_n - v_n, \prod_{i=1}^{s} \mathfrak{p}_i^{k_i}).$$

That is

$$(\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{a}) = \prod_{i=1}^{s} (\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{p}_i)^{k_i}.$$

Then by Theorem 2, $(\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{a})$ is a degree one ideal. Hence φ defines a map from $\mathcal{R}$ to $\mathcal{I}$. For two different elements $(v_1, \ldots, v_n)$ and $(v_1', \ldots, v_n')$ of $\mathcal{R}$, there is at least one $\mathfrak{p_i} \mid \mathfrak{a}$ that $(v_1, \ldots, v_n, \mathfrak{p_i}^{k_i}) \neq (v_1', \ldots, v_n', \mathfrak{p_i}^{k_i})$. So $(v_1, \ldots, v_n, \mathfrak{a})$ does not coincide with $(v_1', \ldots, v_n', \mathfrak{a})$, and hence ϕ is injective.

Now it is left to show ψ is the inverse of φ. Let $\mathfrak{b}$ be any degree one ideal of B with $\mathfrak{b} \cap A = \mathfrak{a}$. Then by $B/\mathfrak{b} \cong A/\mathfrak{a}$, there are $v_1, ..., v_n \in A$ such that $\alpha_i \equiv v_i \mod \mathfrak{b}$, and v_i are uniquely determined up to modulo $\mathfrak{a}$. Since $\alpha_i, v_i \in K(\alpha_i)$, we have $\alpha_i \equiv v_i \mod \mathfrak{b} \cap K(\alpha_i)$. Denote by B_i the integral closure of A in $K(\alpha_i)$. Then

$$g_i(v_i)A = N_{B_i/A}((\alpha_i - v_i)B_i) \subset N_{B_i/A}(\mathfrak{b} \cap K(\alpha_i)) = \mathfrak{a}.$$

So $g_i(v_i) \equiv 0 \mod \mathfrak{a}$ for each i. Therefore ψ is a map from $\mathcal{I}$ to $\mathcal{R}$.

Obviously, $\psi \cdot \varphi = \mathrm{id}_{\mathcal{R}}$. For a given degree one ideal $\mathfrak{b}$ of B above $\mathfrak{a}$, let $v_1, ..., v_n \in A$ such that $\alpha_i \equiv v_i \mod \mathfrak{b}$ for each i. Then $\mathfrak{b}$ divides $\mathfrak{a}B$ and $(\alpha_i - v_i)B$ for all i. Hence

$$\mathfrak{b} \subset (\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{a}).$$

Note that both of $\mathfrak{b}$ and $(\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{a})$ are ideals of degree one above $\mathfrak{a}$. By the definition of degree one ideals over $\mathfrak{a}$ and Theorem 1.2, for each prime factor $\mathfrak{p}$ of $\mathfrak{a}$, there is exactly one prime ideal $\mathfrak{P}$ (resp. $\mathfrak{P}'$) above $\mathfrak{p}$ satisfying that $\mathfrak{P} \mid (\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{a})$ (resp. $\mathfrak{P}' \mid \mathfrak{b}$). Since $\mathfrak{b}$ contains in $(\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{a})$,$\mathfrak{P} = \mathfrak{P}'$. It then follows from $B/\mathfrak{b} \cong B/(\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{a}) \cong A/\mathfrak{a}$ that

$$\mathfrak{b} = (\alpha_1 - v_1, ..., \alpha_n - v_n, \mathfrak{a}).$$

Thus $\varphi \cdot \psi(\mathfrak{b}) = \mathfrak{b}$ for any $\mathfrak{b} \in \mathcal{I}$. That is $\varphi \cdot \psi = \mathrm{id}_{\mathcal{I}}$. This finishes the proof of Theorem 3. □

Before ending this note, we would like to recall Theorem 88 of [1] and show its relation with Theorem 3. Let L_1, L_2 be two number field with relatively prime discriminants and $L := L_1 L_2$. Let p be a prime number which factorises in L_1 as $p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ and in L_2 as $p = \mathfrak{q}_1 \cdots \mathfrak{q}_{\mathfrak{s}}$ where $\mathfrak{p}_1, ..., \mathfrak{p}_r$ and $\mathfrak{q}_1, ..., \mathfrak{q}_s$ are distinct prime ideals of L_1, L_2 respectively. Then Theorem 88 states that p factorises in L as $p = \prod_{i,j} \mathfrak{I}_{ij}^{e_i}$ where the product is taken over $i = 1, ..., r$ and $j = 1, ..., s$ and $\mathfrak{I}_{ij}$ is the greatest common divisor of $\mathfrak{p}_i$ and $\mathfrak{q}_j$ in L. The ideals $\mathfrak{I}_{ij}$ are not necessarily prime ideals in L. From Theorem 3 we know that for a large prime p, if $\mathfrak{p}_i, \mathfrak{q}_j$ are of degree one, then $\mathfrak{I}_{ij}$ is a prime ideal of degree one. Actually it is indicated in the proof of Theorem 3 that $\mathfrak{I}_{ij}$ is a prime ideal if one of $\mathfrak{p}_i, \mathfrak{q}_j$ is of degree one.

Acknowledgement *This paper is supported by the National Natural Science Foundation of China (NSFC No.11901415). The author is sincerely grateful to the referee for helpful comments and corrections that improved the paper.*

References

[1] D. Hilbert, *The theory of algebraic number fields*, Springer-Verlag Berlin Heidelberg (1998).

[2] J. Neukirch, *Algebraic number theory*, Springer-Verlag Berlin Heidelberg (1999).

[3] C. Wang, Distribution of the residues of an algebraic number modulo degree one ideals, *preprint*: https://arxiv.org/abs/2108.05496.

Received: 08.12.2021
Revised: 28.02.2022
Accepted: 08.03.2022

School of Mathematical Sciences, Sichuan Normal University, Chengdu, P. R. China
E-mail: c-l.wang@outlook.com