An analogy of Euler primes for a polynomial ring over a field

Morizono, Akinori
Graduate School of Mathematics, Kyushu University

An analogy of Euler primes for a polynomial ring over a field

指導教員: 竹田 雄一郎 准教授
論文提出者: 森園 明範

論文提出日: 平成 29 年 2 月 1 日

An analogy of Euler primes for a polynomial ring over a field

Akinori Morizono*

February 1, 2017

Abstract

Euler primes have been actively studied as special prime numbers, and their properties are deeply related to the class number of the corresponding quadratic field. A univariate polynomial ring over a field has a similar algebraic structure to the ring of rational integers. For a quadratic extension of a univariate rational function field, its class number is defined. Then, by investigating class numbers, we consider that we can construct polynomials which have certain similar properties to Euler primes. In this paper, we analogically give a formulation of Euler primes for a univariate polynomial ring over a field, and give special polynomials which are viewed as such Euler primes.

Contents

*E-mail: k1755282@gmail.com

1 Introduction

Throughout, let $\mathbb{Z}$ denote the ring of rational integers. For a field F, we denote by $F[t]$ the univariate polynomial ring with an indeterminate t over F. The finite field with q elements is denoted by $\mathbb{F}_q$. There is a deep analogy between $\mathbb{Z}$ and $F[t]$, e.g., both $\mathbb{Z}$ and $F[t]$ are Euclidean domains. So far, special numbers in $\mathbb{Z}$ have been actively researched (e.g., Fermat primes, Mersenne primes). As one of special prime numbers, we take up Euler primes. An Euler prime is of the form

$$x^2 + x + 41, \quad x \in \mathbb{Z}_{\geq 0}. \tag{1.1}$$

If $x = 0, 1, \ldots, 39$, then (1.1) is a prime. Their property is related to the fact that the integer ring

$$\mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{-163}}{2}\right) \;\middle|\; a, b \in \mathbb{Z}\right\} \tag{1.2}$$

has class number 1. Here are more general facts.

Theorem 1.1 *For $q \in \mathbb{Z}_{\geq 2}$, the following are equivalent:*

(i) *$1 - 4q$ is square free, and the integer ring*

$$\mathcal{O} := \left\{a + b\left(\frac{1+\sqrt{1-4q}}{2}\right) \;\middle|\; a, b \in \mathbb{Z}\right\}$$

has class number 1.

(ii) *For any $n \in \mathbb{Z}$ with $0 \leq n \leq q-2$, the integer $n^2 + n + q$ is a prime.*

Frobenius was the first to show that (i) implies (ii) in [1]. After that, Rabinovitch proved the equivalence of (i) and (ii) in [2]. The imaginary number $\sqrt{-163}$ appears in the following factorization of (1.1):

$$\left(x + \frac{1+\sqrt{-163}}{2}\right)\left(x + \frac{1-\sqrt{-163}}{2}\right).$$

Note that $\alpha := (1+\sqrt{-163})/2$ is equal to the conjugate of $\alpha^* := (1-\sqrt{-163})/2$. Recall here that the univariate polynomial ring $F[t]$ over a field F has a similar algebraic structure to $\mathbb{Z}$, and let us give questions: Are Euler primes defined over $F[t]$? If so, how is the definition (and properties) stated? What kind of examples do we have? From this, our aim is to find an analogy of Euler primes for the polynomial ring $F[t]$. Euler primes for $\mathbb{Z}$ have the following property:

> For $\alpha = (1/2) + (1/2)\sqrt{-163}$ and $\alpha^* = (1/2) - (1/2)\sqrt{-163}$, the *integer* $x^2 + x + 41 = (x+\alpha)(x+\alpha^*)$ is *prime* for $x \in \mathbb{Z}$ with $0 \leq x < \alpha\alpha^* - 1 (= 40)$.

Therefore, considering the correspondence between $\mathbb{Z}$ and $F[t]$ as Euclidian domains, an analogy of Euler primes for $F[t]$ is given by the following property:

There exist $A_1, A_2, D \in F[t]$, $B_1, B_2 \in F[t] \setminus \{0\}$ such that for $\alpha := (A_1/B_1) + (A_2/B_2)\sqrt{D}$ and $\alpha^* := (A_1/B_1) - (A_2/B_2)\sqrt{D}$, the *polynomial* $(X+\alpha)(X+\alpha^*)$ is *irreducible* for $X \in F[t]$ with $\deg X < \deg \alpha\alpha^*$.

We here give a method to find polynomials that are analogues of Euler primes:

Theorem 1.2 *Assume that the characteristic of F is not equal to 2. Let $D \in F[t]$ be a polynomial with an odd degree, and put $g := (\deg D - 1)/2$. For $X \in F[t]$, put*

$$f(X) := X^2 - D.$$

The following are equivalent:

(i) *The polynomial D is square free, and the ring*

$$F[t, \sqrt{D}] := \{A + B\sqrt{D} \mid A, B \in F[t]\}$$

has class number 1.

(ii) *For any $A \in F[t]$ with $\deg A \leq 2g$, the polynomial $f(A) \in F[t]$ is irreducible.*

(iii) *For any $A \in F[t]$ with $\deg A < g$, the polynomial $f(A) \in F[t]$ is irreducible.*

The above main theorem in this paper gives an analogy of Theorem 1.1. In particular, "the relationship between $F[t, \sqrt{D}]$ with class number 1 and the irreducible polynomial $X^2 - D$ in Theorem 1.2" corresponds to "the relationship between the integer ring $\mathcal{O}$ with class number 1 and the prime number $x^2 + x + q$ in Theorem 1.1". We prove Theorem 1.2 in a similar way to the Theorem 1.1 in [3]. By applying Theorem 1.2 to the case of $F = \mathbb{F}_3$, we can give an analogy of Euler primes for the polynomial ring $\mathbb{F}_3[t]$.

Example 1.3 Consider the following univariate polynomial over $\mathbb{F}_3[t]$ with the indeterminate X:

$$f(X) := X^2 - t^3 + t + 1. \tag{1.3}$$

Then, for any $A \in \mathbb{F}_3[t]$ with $\deg A \leq 2$, the polynomial $f(A) \in \mathbb{F}_3[t]$ is irreducible.

The factorization of (1.3) is given by

$$f(X) = \left(X + \sqrt{t^3 - t - 1}\right)\left(X - \sqrt{t^3 - t - 1}\right).$$

In this paper, we describe how Example 1.3 is related to the fact that the ring

$$\mathbb{F}_3\left[t, \sqrt{t^3 - t - 1}\right] := \left\{A + B\sqrt{t^3 - t - 1} \;\middle|\; A, B \in \mathbb{F}_3[t]\right\}$$

has class number 1.

This paper is organized as follows: In Section 2, we collect some known facts on quadratic extensions of rational function fields. In Section 3, we prove Theorem 1.2. In Section 4, we introduce an analogue of Theorem 1.2 in characteristic 2. In Section 5, we directly compute Example 1.3 (cf. the claim is immediately derived from our main theorem).

2 Preliminaries

In this section, we collect some known facts on quadratic extensions of rational function fields.

Notation

Throughout Section 2, let F be a field with $\mathrm{char}(F)$[1] $\neq 2$. Let $F[t]$ be the univariate polynomial ring with an indeterminate t over F, and $F(t)$ the univariate rational function field of F. If the leading cofficient of $X \in F[t]$ equals 1, the polynomial X is said to be monic or a monic polynomial. It is straightforward that there exists $D \in F[t]$ such that

$$\deg D \text{ is odd.} \tag{2.1}$$
$$D \text{ is square free.} \tag{2.2}$$

We put $g := (\deg D - 1)/2$. Consider the following sets:

$$F(t, \sqrt{D}) := \{A + B\sqrt{D} \mid A, B \in F(t)\},$$
$$F[t, \sqrt{D}] := \{A + B\sqrt{D} \mid A, B \in F[t]\}.$$

Note that $F(t, \sqrt{D})$ is a quadratic extension of $F(t)$. For $\alpha := A + B\sqrt{D} \in F(t, \sqrt{D})$ with $A, B \in F(t)$, we define its conjugate α^*, its trace $Tr(\alpha)$ and its norm $N(\alpha)$ as follows:

$$\alpha^* := A - B\sqrt{D},$$
$$Tr(\alpha) := \alpha + \alpha^* = 2A, \tag{2.3}$$
$$N(\alpha) := \alpha\alpha^* = A^2 - B^2 D. \tag{2.4}$$

Recall that D is a polynomial with an odd degree. Since B^2D and A^2 have different degrees ($\deg B^2D$ is odd whereas $\deg A^2$ is even), one of their leading coefficients remains in (2.4). Therefore, the following are satisfied:

$$\deg N(\alpha) = \deg (A^2 - B^2 D) = \max\{\deg A^2, \deg B^2 D\}. \tag{2.5}$$

For $\alpha_1, \ldots, \alpha_r \in R := F[t, \sqrt{D}]$, we put

$$(\alpha_1, \ldots, \alpha_r) := \{\alpha_1\xi_1 + \cdots + \alpha_r\xi_r \in R \mid \xi_1, \ldots, \xi_r \in R\},$$
$$[\alpha_1, \ldots, \alpha_r] := \{\alpha_1 X_1 + \cdots + \alpha_r X_r \in R \mid X_1, \ldots, X_r \in F[t]\}.$$

Note that $(\alpha_1, \ldots, \alpha_r)$ is an ideal of R while $[\alpha_1, \ldots, \alpha_r]$ is an $F[t]$-submodule of R.

2.1 The integral closures of $F[t]$ in $F(t, \sqrt{D})$

In this section, we prove $F[t, \sqrt{D}]$ is the integral closure of $F[t]$ in $F(t, \sqrt{D})$. First, we give an elementary property of a principal ideal domain.

Lemma 2.1.1 *Let $D \in F[t]$ be a polynomial which is square free. If $X \in F(t)$ satisfies $DX^2 \in F[t]$, then X is in $F[t]$.*

[1] Let $\mathrm{char}(F)$ denote the characteristic of a field F.

Proof. We put $C := DX^2$ and write $X = A/B$ ($A, B \in F[t]$ such that A and B are co-prime, and $B \neq 0$). We have $B^2C = DA^2$. Let us assume $\deg B > 0$. Let $P \in F[t]$ be an irreducible polynomial dividing B. It follows that P^2 is a divisor of DA^2. Since A and B are co-prime, the polynomial P is not a divisor of A. Hence, the polynomial P^2 is not a divisor of A^2 and thus P^2 is a divisor of D. However, this contradicts that D is square free. Therefore, we obtain $X \in F[t]$ since B is a constant.

Theorem 2.1.2 ([4], Theorem 10.4) *Let $D \in F[t]$ be a polynomial satisfying* (2.1) *and* (2.2)*, and we put $R := F[t, \sqrt{D}]$. For $\alpha \in F(t, \sqrt{D})$, the following are equivalent:*

(i) $\alpha \in R$.

(ii) $Tr(\alpha), N(\alpha) \in F[t]$.

(iii) *There exist $A, B \in F[t]$ such that $\alpha^2 + A\alpha + B = 0$.*

Proof. We put $\alpha := X + Y\sqrt{D}$ with $X, Y \in F(t)$.
(i) $\Rightarrow$ (ii) It follows from $X, Y \in F[t]$, (2.3) and (2.4) that $Tr(\alpha), N(\alpha) \in F[t]$.

(ii) $\Rightarrow$ (i) Putting $S := Tr(\alpha) = 2X$ and $T := N(\alpha) = X^2 - Y^2D$, suppose that $S, T \in F[t]$. We have $X = (1/2)S \in F[t]$. In addition, we have $DY^2 = X^2 - T \in F[t]$ and (2.2), and hence $Y \in F[t]$ by Lemma 2.1.1.

(ii) $\Rightarrow$ (iii) Putting $A := -Tr(\alpha)$ and $B := N(\alpha)$, we have $\alpha^2 + A\alpha + B = 0$.

(iii) $\Rightarrow$ (ii) Consider the case of $\alpha \in F(t)$. Since $F[t]$ is an integrally closed domain and since $F(t)$ is the quotient field of $F[t]$, we have $\alpha \in F[t]$. In the case of $\alpha \notin F[t]$, the polynomial Y is not equal to 0. In addition, we have $(\alpha^*)^2 + A\alpha^* + B = 0$ by the hypothesis (iii). Thus, the elements α and α^* are the different roots of the equation $t^2 + At + B = 0$, say $t^2 + At + B = (t - \alpha)(t - \alpha^*)$. Therefore, it follows that $Tr(\alpha) = \alpha + \alpha^* = -A \in F[t]$ and $N(\alpha) = \alpha\alpha^* = B \in F[t]$. We have proved (ii). □

By Theorem 2.1.2, it follows that $R := F[t, \sqrt{D}]$ is the integral closure of $F[t]$ in $F(t, \sqrt{D})$. We claim that R is a Dedekind domain since $F[t]$ is a principal ideal domain. (More generally, for the quotient field K of a principal ideal domain A, the integral closure of A in a finite extension field of K is a Dedekind domain.) This fact will be used in Section 2.3 to define the *ideal class group* of R.

2.2 The canonical basis and the norm of an ideal of $F[t, \sqrt{D}]$

In this section, we introduce the canonical basis and the norm of an ideal of $F[t, \sqrt{D}]$.

Proposition 2.2.1 ([4], Proposition 10.8) *Let $D \in F[t]$ be a polynomial satisfying* (2.1) *and* (2.2)*, and we put $R := F[t, \sqrt{D}]$. For an $F[t]$-submodule $\mathcal{I} := [A, B + C\sqrt{D}]$ with $A, B \in F[t]$ and $C \in F[t] \setminus \{0\}$, the following are equivalent:*

(i) *$\mathcal{I}$ is an ideal of R, and we have $\mathcal{I} = (A, B + C\sqrt{D})$.*

(ii) *A and B are divisible by C and $(B^2/C) - CD$ is divisible by A.*

Proof. Note that (i) is equivalent to $A\sqrt{D}$, $(B+C\sqrt{D})\sqrt{D} \in \mathcal{I}$. On the other hand, we can write

$$A\sqrt{D} = -\frac{B}{C}\,A + \frac{A}{C}(B+C\sqrt{D}),$$
$$(B+C\sqrt{D})\sqrt{D} = -\left(\frac{B^2}{C} - CD\right) + \frac{B}{C}(B+C\sqrt{D}).$$

The set $\{A, B+C\sqrt{D}\}$ is a basis of the $F[t]$-submodule $\mathcal{I}$. Hence the condition that $A\sqrt{D}$ and $(B+C\sqrt{D})\sqrt{D}$ are in $\mathcal{I}$ is equivalent to (ii). □

Proposition 2.2.2 ([4], Proposition 10.9) *Let $D \in F[t]$ be a polynomial satisfying* (2.1) *and* (2.2)*, and we put $R := F[t, \sqrt{D}]$. For any ideal $\mathcal{I} \subset R$ with $\mathcal{I} \neq (0)$, there exist unique $A, B, C \in F[t]$ such that*

$$\mathcal{I} \cap F[t] = [A], \tag{2.6}$$
$$\mathcal{I} = [A, B+C\sqrt{D}] = (A, B+C\sqrt{D}), \tag{2.7}$$
$$A \text{ and } B \text{ are divisible by } C, \tag{2.8}$$
$$B^2/C - CD \text{ is divisible by } A, \tag{2.9}$$
$$A \text{ and } C \text{ are monic}, \tag{2.10}$$
$$\deg A > \deg B. \tag{2.11}$$

Proof. First, for $\alpha \in \mathcal{I}$ with $\alpha \neq 0$, we have $N(\alpha) \neq 0$ and $N(\alpha) \in \mathcal{I} \cap F[t]$, and therefore $\mathcal{I} \cap F[t] \neq [0]$. Thus, there exists a monic polynomial $A \in F[t] \setminus \{0\}$ such that $\mathcal{I} \cap F[t] = [A]$. We define an ideal I of $F[t]$ as follows:

$$I := \{Y \in F[t] \mid \text{there exists } X \in F[t] \text{ such that } X + Y\sqrt{D} \in \mathcal{I}\}. \tag{2.12}$$

Note that I is a non-zero ideal since $A \in I$. Let C be a monic generator of I, say $I = [C]$. Putting $\mathcal{A}_C := \{X \in F[t] \mid X + C\sqrt{D} \in \mathcal{I}\}$, we take $B \in \mathcal{A}_C$ so that $\deg B = \min\{\deg X \mid X \in \mathcal{A}_C\}$. Here, we suppose $\deg A \leq \deg B$. We write

$$A = t^m + a_1 t^{m-1} + \cdots + a_{m-1}t + a_m,$$
$$B = b_1 t^n + b_2 t^{n-1} + \cdots + b_n t + b_{n+1}$$
$$(a_1, \ldots, a_m, b_1, \ldots, b_{n+1} \in F,\ b_1 \neq 0, m := \deg A, n := \deg B).$$

For any $X \in F[t]$, we have $XA+B+C\sqrt{D} \in \mathcal{I}$ because XA, $B+C\sqrt{D} \in \mathcal{I}$. In particular, taking $-b_1 t^{n-m}$ as X, we have $-b_1 t^{n-m}A + B \in \mathcal{A}_C$. Putting $S := -b_1 t^{n-m}A + B$, we have

$$\begin{aligned} S &= -b_1 t^{n-m}(t^m + a_1 t^{m-1} + \cdots + a_m) + b_1 t^n + b_2 t^{n-1} + \cdots + b_{n+1} \\ &= -b_1 t^n - b_1 t^{n-m}(a_2 t^{m-2} + \cdots + a_m) + b_1 t^n + b_2 t^{n-1} + \cdots + b_{n+1} \\ &= -b_1 t^{n-m}(a_1 t^{m-1} + \cdots + a_m) + b_2 t^{n-1} + \cdots + b_{n+1} \\ &= (b_2 - b_1 a_1)t^{n-1} + \cdots + (b_{m+1} - b_1 a_m)t^{n-m} + b_{m+2}t^{n-m-1} + \cdots + b_{n+1}. \end{aligned}$$

Thus, we obtain $\deg S < \deg B$. This contradicts the minimality of $\deg B$. Therefore, the polynomials A and B satisfy (2.11). Here, we show (2.7). Since A and $B + C\sqrt{D}$

are elements of $\mathcal{I}$, we have $[A, B+C\sqrt{D}] \subset (A, B+C\sqrt{D}) \subset \mathcal{I}$. Let $\alpha = X + Y\sqrt{D}$ be an arbitrary element of $\mathcal{I}$. The polynomial Y satisfies $Y \in I = [C]$, and thus we write $Y = CT$ for some $T \in F[t]$. Since α, $B + C\sqrt{D} \in \mathcal{I}$ and since

$$X - TB = X + Y\sqrt{D} - T(B + C\sqrt{D}) = \alpha - T(B + C\sqrt{D}),$$

we have $X - TB \in \mathcal{I} \cap F[t] = [A]$. Hence, there exists $U \in F[t]$ such that $X - TB = AU$. Therefore, we have $\alpha = X + Y\sqrt{D} = AU + T(B + C\sqrt{D}) \in [A, B + C\sqrt{D}]$. We have shown (2.7). Moreover, the polynomials A, $B \in F[t]$ and $C \in F[t] \setminus \{0\}$ satisfy (2.8) and (2.9) by Proposition 2.2.1. From this, the polynomials A, B and $C \in F[t]$ satisfy (2.6)–(2.11). Finally, we show that these polynomials are determined uniquely. The polynomial A is determined uniquely by (2.6) and (2.10). Assume that $B', C' \in F[t]$ satisfy the following:

$$\mathcal{I} = [A, B' + C'\sqrt{D}] = (A, B' + C'\sqrt{D}), \tag{2.13}$$
$$A \text{ and } B' \text{ are divisible by } C', \tag{2.14}$$
$$(B')^2/C' - C'D \text{ is divisible by } A, \tag{2.15}$$
$$C' \text{ is monic}, \tag{2.16}$$
$$\deg A > \deg B'. \tag{2.17}$$

By (2.13), for any $Y \in I$ with $X + Y\sqrt{D} \in \mathcal{I}$ ($X \in F[t]$), the polynomial Y is divisible by C', and hence $I = [C']$. Here I is a non-zero ideal of $F[t]$ defined in (2.12). We obtain $C' = C$ by (2.16). We suppose that $B' \neq B$. We may assume $\deg B \geq \deg B'$. By $B + C\sqrt{D}$, $B' + C\sqrt{D} \in \mathcal{I}$ and $B - B' \in (\mathcal{I} \cap F[t]) \setminus \{0\}$, we have $B - B' = XA$ for some $X \in F[t] \setminus \{0\}$. Hence, we have

$$\deg (B - B') = \deg X + \deg A \geq \deg A.$$

This contradicts $\deg A > \deg B \geq \deg (B - B')$. We have shown the uniqueness. □

Definition 2.2.3 In Proposition 2.2.2, the set $\{A, B + C\sqrt{D}\}$ is called the *canonical basis* of $\mathcal{I}$. If $C = 1$, then $\mathcal{I}$ is called a *primitive ideal* of R.

Remark 2.2.4 By Proposition 2.2.2, there exist polynomials $A', B' \in F[t]$ such that $A = A'C$ and $B = B'C$, where A' is monic. Then, we have $\mathcal{I} = C(A', B' + \sqrt{D})$. Moreover, we claim that the canonical basis of the ideal $\mathcal{I}' := (A', B' + \sqrt{D})$ is $\{A', B' + \sqrt{D}\}$. Indeed, it follows from (2.9) that $(B')^2 - D$ is divisible by A'. Thus, we obtain $\mathcal{I}' = [A', B' + \sqrt{D}]$ by Proposition 2.2.1. In addition, we have $\deg A' > \deg B'$ by (2.11). It is clear that $\mathcal{I}' \cap F[t] = [A']$. From this, $\{A', B' + \sqrt{D}\}$ satisfies (2.6)–(2.11), which means $\{A', B' + \sqrt{D}\}$ is the canonical basis of $\mathcal{I}$. We also note that the ideal $\mathcal{I}'$ of R is a primitive ideal.

Proposition 2.2.5 ([4], Proposition 10.10) *Let $D \in F[t]$ be a polynomial satisfying* (2.1) *and* (2.2)*, and we put $R := F[t, \sqrt{D}]$. Then for ideals $\mathcal{I}, \mathcal{I}' \subset R$ with $\mathcal{I}, \mathcal{I}' \neq (0)$, the following are satisfied:*

(i) *$\mathcal{I}^* := \{\alpha^* \mid \alpha \in \mathcal{I}\}$ is an ideal of R.*

(ii) *There exists a unique polynomial $N \in F[t]$ such that N is monic and $\mathcal{I}\mathcal{I}^* = (N)$. The polynomial $N(\mathcal{I}) := N$ is called the norm of the ideal $\mathcal{I}$.*

(iii) $N(\mathcal{I})N(\mathcal{I}') = N(\mathcal{I}\mathcal{I}')$.

(iv) *If there exists* $\alpha \in R$ *such that* $\mathcal{I} = (\alpha)$, *then* $(N(\mathcal{I})) = (N(\alpha))$ *and* $\deg N(\mathcal{I}) = \deg N(\alpha)$. *In addition,* $\mathcal{I} = (1)$ *and* $N(\mathcal{I}) = 1$ *are equivalent each other.*

(v) *Writing* $\mathcal{I} = [A, B + C\sqrt{D}]$ *by its canonical basis* $\{A, B + C\sqrt{D}\}$, *we have* $N(\mathcal{I}) = AC$.

Proof. (i) Straightforward.

(ii) By Proposition 2.2.2, the ideal $\mathcal{I}$ is generated by two elements. Writing $\mathcal{I} = (\alpha, \beta)$ with $\alpha, \beta \in \mathcal{I}$, one has $\mathcal{I}^* = (\alpha^*, \beta^*)$, and thus $\mathcal{I}\mathcal{I}^* = (\alpha\alpha^*, \alpha\beta^*, \alpha^*\beta, \beta\beta^*)$. We put $A := \alpha\alpha^*$, $B := \alpha\beta^* + \alpha^*\beta$ and $C := \beta\beta^*$. Since $\alpha\alpha^* = N(\alpha)$, $\alpha\beta^* + \alpha^*\beta = Tr(\alpha\beta^*)$ and $\beta\beta^* = N(\beta)$, it follows from Theorem 2.1.2 that A, B and C are in $F[t]$. For the ideal $[A, B, C]$ of $F[t]$, there exists a unique polynomial such that N is monic and $[A, B, C] = [N]$. By $[N] = [A, B, C] \subset (A, B, C) \subset \mathcal{I}\mathcal{I}^*$, we have $(N) \subset \mathcal{I}\mathcal{I}^*$. We show $(N) \supset \mathcal{I}\mathcal{I}^*$. We put $\gamma := (\alpha\beta^*/N)$. Then, we have $\gamma + \gamma^* = (B/N) \in F[t]$ and $\gamma\gamma^* = (AC/N^2) \in F[t]$, and thus we have $\gamma, \gamma^* \in R$ by Theorem 2.1.2. Therefore, we obtain

$$\mathcal{I}\mathcal{I}^* = (\alpha\alpha^*, \alpha\beta^*, \alpha^*\beta, \beta\beta^*) = (A, N\gamma, N\gamma^*, C) \subset (N).$$

We have shown $\mathcal{I}\mathcal{I}^* = (N)$. The uniqueness of the norm of $\mathcal{I}$ follows from the choice of N.

(iii) It is straightforward that

$$\begin{aligned}(\mathcal{I}\mathcal{I}')^* &= \left\{ \left(\sum \alpha\beta \right)^* \,\middle|\, \alpha \in \mathcal{I}, \beta \in \mathcal{I}' \right\} \\ &= \left\{ \sum \alpha^*\beta^* \,\middle|\, \alpha \in \mathcal{I}, \beta \in \mathcal{I}' \right\} \\ &= \left\{ \sum \gamma\delta \,\middle|\, \gamma \in \mathcal{I}^*, \delta \in (\mathcal{I}')^* \right\} = \mathcal{I}^*(\mathcal{I}')^*,\end{aligned}$$

and hence we have

$$(N(\mathcal{I}\mathcal{I}')) = (\mathcal{I}\mathcal{I}')(\mathcal{I}\mathcal{I}')^* = \mathcal{I}\mathcal{I}'\mathcal{I}^*(\mathcal{I}')^* = \mathcal{I}\mathcal{I}^*\mathcal{I}'(\mathcal{I}')^* = (N(\mathcal{I}))(N(\mathcal{I}')) = (N(\mathcal{I})N(\mathcal{I}')).$$

Thus, we have shown $N(\mathcal{I}\mathcal{I}') = N(\mathcal{I})N(\mathcal{I}')$ by the uniqueness of the norm of an ideal.

(iv) First, we show $(N(\mathcal{I})) = (N(\alpha))$. We have $(N(\mathcal{I})) = \mathcal{I}\mathcal{I}^* = (\alpha)(\alpha^*) = (\alpha\alpha^*) = (N(\alpha))$. From this, we obtain $\deg N(\mathcal{I}) = \deg N(\alpha)$. Next, we show that $\mathcal{I} = (1)$ and $N(\mathcal{I}) = 1$ are equivalent each other. Suppose $\mathcal{I} = (1)$. Then, it follows that $\mathcal{I}\mathcal{I}^* = (1)(1^*) = (1)$, and thus $N(\mathcal{I}) = 1$. If $N(\mathcal{I}) = 1$, the ideal $\mathcal{I}$ equals (1) since $(1) = \mathcal{I}\mathcal{I}^* \subset \mathcal{I}$.

(v) First, consider the case that $\mathcal{I}$ is a primitive ideal, that is, $C = 1$. We put $N := N(\mathcal{I})$, $X := (B^2 - D)/A$ and $\mathcal{J} := (A, B + \sqrt{D}, B - \sqrt{D}, X)$. Note that X is in $F[t]$ by the definition of the canonical basis. Then, we have

$$\begin{aligned}(N) = \mathcal{I}\mathcal{I}^* &= (A, B + \sqrt{D})(A, B - \sqrt{D}) \\ &= (A^2, A(B + \sqrt{D}), A(B - \sqrt{D}), B^2 - D) = A\mathcal{J}.\end{aligned}$$

Now, we show $\mathcal{J} = (1)$. By $N \in A\mathcal{J}$, there exists $\alpha \in \mathcal{J} \subset R$ such that $N = A\alpha$. Since $F(t) \ni N/A = \alpha \in R$, the element N/A is in $F(t) \cap R = F[t]$. Here, we put $N_1 := N/A$. Then, we have $\mathcal{J} = (N_1)$, and N_1 is monic since N and A are monic. By $B + \sqrt{D} \in \mathcal{J} = (N_1)$, there exist $X, Y \in F[t]$ such that $B + \sqrt{D} = N_1(X + Y\sqrt{D}) = N_1X + N_1Y\sqrt{D}$, and hence $N_1 = 1$. Therefore, we have $(N) = A\mathcal{J} = A(N_1) = A(1) = (A)$. Since A is monic, we have $N(\mathcal{I}) = N = A$. Next, consider the case that $\mathcal{I}$ is not necessarily a primitive ideal. There exist polynomials $A', B' \in F[t]$ such that A is monic and $A = A'C$ and $B = B'C$ by (2.8). For the ideal $\mathcal{I}' := (A', B' + \sqrt{D})$, its canonical basis is $\{A', B' + \sqrt{D}\}$ by Remark 2.2.4. Now $\mathcal{I}'$ is a primitive ideal, and thus $N(\mathcal{I}') = A'$ by using the result of the above case. In addition, we have $N((C)) = N(C)$ by (iv). Therefore, it follows from (iii) that

$$N(\mathcal{I}) = N((A'C, B'C + C\sqrt{D})) = N((C)\mathcal{I}') = N((C))N(\mathcal{I}') = C^2A' = AC.$$

□

Remark 2.2.6 Proposition 2.2.5 (v) is proved by using only (2.8)–(2.10). Therefore, for $A, B, C \in F[t]$ satisfying (2.8)–(2.10), by Proposition 2.2.1, the $F[t]$-submodule $\mathcal{I} := [A, B + C\sqrt{D}]$ of R is an ideal of R, and we have $N(\mathcal{I}) = AC$. (In this case, the set $\{A, B + C\sqrt{D}\}$ is not necessarily the canonical basis of $\mathcal{I}$).

Lemma 2.2.7 *Let $D \in F[t]$ be a polynomial satisfying* (2.1) *and* (2.2)*, and we put $R := F[t, \sqrt{D}]$. Then for any ideal $\mathcal{I} \subset R$ with $\mathcal{I} \neq (0)$, the following are satisfied:*

(i) $\mathcal{I} = (\mathcal{I}^*)^*$.

(ii) $N(\mathcal{I}) = N(\mathcal{I}^*)$.

Proof. (i) Straightforward.

(ii) It follows from (i) that $\mathcal{I}^*(\mathcal{I}^*)^* = \mathcal{I}^*\mathcal{I} = \mathcal{I}\mathcal{I}^*$. By Proposition 2.2.5 (ii), we obtain $\mathcal{I}\mathcal{I}^* = (N(\mathcal{I}))$, and thus $\mathcal{I}^*(\mathcal{I}^*)^* = (N(\mathcal{I}))$. By the uniqueness of the norm of an ideal, it follows that $N(\mathcal{I}^*) = N(\mathcal{I})$. □

Proposition 2.2.8 ([4], Proposition 10.11 (ii)) *Let $D \in F[t]$ be a polynomial satisfying* (2.1) *and* (2.2)*, and put $R := F[t, \sqrt{D}]$. Then for ideals $\mathcal{I}, \mathcal{J} \subset R$ with $\mathcal{I}, \mathcal{J} \neq (0)$, the following are equivalent:*

(a) $\mathcal{J} \subset \mathcal{I}$.

(b) *There exists an ideal $\mathcal{I}' \subset R$ such that $\mathcal{I}\mathcal{I}' = \mathcal{J}$.*

Proof. It is clear that (b) ⇒ (a). We prove that (a) implies (b). Suppose $\mathcal{J} \subset \mathcal{I}$. Then, we have $\mathcal{J}\mathcal{I}^* \subset \mathcal{I}\mathcal{I}^* = (N(\mathcal{I}))$. We put $N := N(\mathcal{I})$. The subset $\mathcal{I}' := \{\alpha/N \mid \alpha \in \mathcal{J}\mathcal{I}^*\}$ is an ideal of R. Here, we show $\mathcal{I}\mathcal{I}' = \mathcal{J}$. First, let $\gamma \in \mathcal{J}$. Writing $N = \sum_{i=1}^{n} \alpha_i\beta_i$ ($\alpha_i \in \mathcal{I}, \beta_i \in \mathcal{I}^*$ for each $i = 1, \cdots, n$), we have

$$\gamma = \frac{1}{N}N\gamma = \frac{1}{N}\left(\sum_{i=1}^{n} \alpha_i\beta_i\right)\gamma = \sum_{i=1}^{n} \alpha_i\left(\frac{1}{N}\beta_i\gamma\right).$$

Therefore, we obtain $\gamma \in \mathcal{I}\mathcal{I}'$ by $\alpha_i \in \mathcal{I}$ and $(1/N)\beta_i\gamma \in \mathcal{I}'$. Next, we show $\mathcal{J} \supset \mathcal{I}\mathcal{I}'$. Let $\alpha\alpha'$ be an arbitrary element of $\mathcal{I}\mathcal{I}'$ with $\alpha \in \mathcal{I}$ and $\alpha' \in \mathcal{I}'$. We write $\alpha' = (1/N)\sum_{i=1}^{n} \gamma_i\delta_i$ ($\gamma_i \in \mathcal{J}, \delta_i \in \mathcal{I}^*$ for each $i = 1, \cdots, n$). Then, we have $\alpha\alpha' = (1/N)\sum_{i=1}^{n} \alpha\delta_i\gamma_i$. In addition, it follows that $\alpha\delta_i \in \mathcal{I}\mathcal{I}^* = (N)$, and thus $\alpha\alpha' \in \mathcal{J}$. Therefore, we obtain $\mathcal{J} \supset \mathcal{I}\mathcal{I}'$. We have proved the claim. □

Lemma 2.2.9 *Let $D \in F[t]$ be a polynomial satisfying* (2.1) *and* (2.2)*, and we put $R := F[t, \sqrt{D}]$. For a monic irreducible polynomial $P \in F[t]$ such that the ideal (P) of R is not a prime ideal, there exists a prime ideal $\mathcal{P}$ such that $(P) = \mathcal{P}\mathcal{P}^*$, where $\mathcal{P}^* := \{\alpha^* \mid \alpha \in \mathcal{P}\}$.*

Proof. We suppose that (P) is not a prime ideal. Then, there exists a maximal ideal $\mathcal{P}$ of R such that $(P) \subsetneq \mathcal{P}$ (since the ideal (P) is not a maximal ideal). By Proposition 2.2.8, there exists an ideal $\mathcal{I}$ of R such that $(P) = \mathcal{P}\mathcal{I}$. It follows from Proposition 2.2.5 (iv) that $(N((P))) = (N(P)) = (P^2)$, where P^2 is monic. By the definition of the norm of an ideal, the polynomial $N((P))$ is monic too. Thus, we have $N((P)) = P^2$. Moreover, we have $N(\mathcal{P}\mathcal{I}) = N(\mathcal{P})N(\mathcal{I})$ by Proposition 2.2.5 (iii). From this, it follows that

$$P^2 = N((P)) = N(\mathcal{P}\mathcal{I}) = N(\mathcal{P})N(\mathcal{I}).$$

Therefore, the norm $N(\mathcal{P})$ is equal to P or P^2. Let us assume $N(\mathcal{P}) = P^2$. In this case, we have $N(\mathcal{I}) = 1$. By Proposition 2.2.5 (iv), we have $\mathcal{I} = (1)$ and thus $(P) = \mathcal{P}\mathcal{I} = \mathcal{P}$. This contradicts that the ideal (P) is not a prime ideal. Therefore, we have $N(\mathcal{P}) = P$. By the definition of the norm of an ideal, it follows that $(P) = \mathcal{P}\mathcal{P}^*$. □

Lemma 2.2.10 ([4], Lemma 10.16 (i)) *Let $D \in F[t]$ be a polynomial satisfying* (2.1) *and* (2.2)*, and we put $R := F[t, \sqrt{D}]$. For an ideal $\mathcal{P} \subset R$ with $\mathcal{P} \neq (0)$ such that $N(\mathcal{P})$ is a monic irreducible polynomial, the following are satisfied:*

(a) *$\mathcal{P}$ is a prime ideal.*

(b) *When the prime ideal $\mathcal{P}$ is written as $\mathcal{P} = [P, B + C\sqrt{D}]$ by its canonical basis with $P, B, C \in F[t]$, we have $P = N(\mathcal{P})$ and $C = 1$.*

Proof. (a) It suffices to show that $\mathcal{P}$ is maximal. Assume an ideal $\mathcal{I}$ with $\mathcal{I} \neq (1)$ such that $\mathcal{I}$ contains $\mathcal{P}$. By Proposition 2.2.8, there exists an ideal $\mathcal{I}'$ such that $\mathcal{P} = \mathcal{I}\mathcal{I}'$. By Proposition 2.2.5 (iii), we have $N(\mathcal{P}) = N(\mathcal{I}\mathcal{I}') = N(\mathcal{I})N(\mathcal{I}')$. The polynomials $N(\mathcal{I})$ and $N(\mathcal{I}')$ are monic by the definition of the norm of an ideal. The norm $N(\mathcal{P})$ is irreducible. Hence, we obtain $N(\mathcal{I}) = 1$ or $N(\mathcal{I}') = 1$. Since $\mathcal{I} \neq (1)$, we have $N(\mathcal{I}) \neq 1$ by Proposition 2.2.5 (iv), and thus $N(\mathcal{I}') = 1$. Therefore, it follows from Proposition 2.2.5 (iv) that $\mathcal{I}' = (1)$, and thus $\mathcal{P} = \mathcal{I}$.

(b) By Proposition 2.2.5 (v), we obtain $N(\mathcal{P}) = PC$. Since $N(\mathcal{P})$ is irreducible, and since P and C are monic, we have $P = 1$ or $C = 1$. If $P = 1$, then we have $\mathcal{P} = [1, B + C\sqrt{D}] = (1, B + C\sqrt{D}) = (1)$, and this contradicts that $\mathcal{P}$ is a prime ideal. From this, we have shown that $C = 1$ and $P = N(\mathcal{P})$. □

Lemma 2.2.11 *Let $D \in F[t]$ be a polynomial satisfying* (2.1) *and* (2.2)*, and we put $R := F[t, \sqrt{D}]$. By* Proposition 2.2.2*, for any ideal $\mathcal{I} \subset R$ with $\mathcal{I} \neq (0)$, there exist A,*

B, $C \in F[t]$ such that (2.7)–(2.10) are satisfied. Consider the case of $C = 1$, that is, let $\mathcal{I}$ be an ideal of R such that there exist $A, B \in F[t]$ satisfying

$$\mathcal{I} = [A, B + \sqrt{D}] = (A, B + \sqrt{D}), \tag{2.18}$$

$$B^2 - D \text{ is divisible by } A, \tag{2.19}$$

$$A \text{ is monic.} \tag{2.20}$$

If A is factored into $A = A_1 \cdots A_r$ by monic polynomials $A_i \in F[t]$ with $1 \leq i \leq r$, then for $i = 1, \ldots, r$, the $F[t]$-submodule $\mathcal{I}_i := [A_i, B + \sqrt{D}]$ of R is an ideal of R, and

$$\mathcal{I}_i = (A_i, B + \sqrt{D}),$$
$$N(\mathcal{I}_i) = A_i.$$

In addition, the ideal $\mathcal{I}$ is factored into

$$\mathcal{I} = \mathcal{I}_1 \cdots \mathcal{I}_r.$$

Proof. Assume that the polynomial $A \in F[t]$ is factored into $A = A_1 \cdots A_r$ by $A_i \in F[t]$ with $1 \leq i \leq r$. We prove the statement by induction on r. First in the case of $r = 1$, the statement is clear. Next, we show Lemma 2.2.11 in the case of $r = 2$. We suppose that by monic polynomials A_1 and A_2, the polynomial A is factored into $A = A_1 A_2$. Since A is a divisor of $B^2 - D$, the polynomials A_1 and A_2 are divisors of $B^2 - D$. Therefore, by Proposition 2.2.1, $F[t]$-submodules $\mathcal{I}_1 := [A_1, B + \sqrt{D}]$ and $\mathcal{I}_2 := [A_2, B + \sqrt{D}]$ of R are ideals of R, and we have

$$\mathcal{I}_1 = (A_1, B + \sqrt{D}), \text{ and } \mathcal{I}_2 = (A_2, B + \sqrt{D}).$$

Since A_1 and A_2 are monic divisors of $B^2 - D$ (i.e., A_1 and A_2 satisfy (2.8)–(2.10)), we have $N(\mathcal{I}_1) = A_1$ and $N(\mathcal{I}_2) = A_2$ by Remark 2.2.6. Here, we show $\mathcal{I} = \mathcal{I}_1 \mathcal{I}_2$. Put $\alpha := B + \sqrt{D}$. Since $\mathcal{I}_1 \mathcal{I}_2 \subset \mathcal{I}$, there exists an ideal $\mathcal{I}'$ such that $\mathcal{I}\mathcal{I}' = \mathcal{I}_1 \mathcal{I}_2$ by Proposition 2.2.8. By Proposition 2.2.5 (iii), we have

$$N(\mathcal{I})N(\mathcal{I}') = N(\mathcal{I}_1)N(\mathcal{I}_2). \tag{2.21}$$

In addition, by (2.19) and (2.20), the polynomials $A, B \in F[t]$ and $C = 1 \in F[t]$ satisfy (2.8)–(2.10). From this, we have

$$N(\mathcal{I}) = A = A_1 A_2 = N(\mathcal{I}_1)N(\mathcal{I}_2) \tag{2.22}$$

by Remark 2.2.6. Therefore, we have $N(\mathcal{I}') = 1$ by (2.21) and (2.22). By Proposition 2.2.5 (iii), we have $\mathcal{I}' = R$, and thus we have proved $\mathcal{I} = \mathcal{I}_1 \mathcal{I}_2$.
Next, we show Lemma 2.2.11 in the case of $r > 2$. We suppose that by monic polynomials $A_i \in F[t]$ with $1 \leq i \leq r$, the polynomial $A \in F[t]$ is factored into $A = A_1 \cdots A_r = (A_1 \cdots A_{r-1})(A_r)$. By the hypothesis of induction, $F[t]$-submodules $\mathcal{I}' := [A_1 \cdots A_{r-1}, B + \sqrt{D}]$ and $\mathcal{I}_r := [A_r, B + \sqrt{D}]$ of R are ideals of R, and they satisfy

$$\mathcal{I}' = (A_1 \cdots A_{r-1}, B + \sqrt{D}), \text{ and } \mathcal{I}_r = (A_r, B + \sqrt{D}).$$

In addition, we have $N(\mathcal{I}_r) = A_r$ and $\mathcal{I}$ is factored into

$$\mathcal{I} = \mathcal{I}'\mathcal{I}_r. \tag{2.23}$$

Here the polynomial A is a divisor of $B^2 - D$. Thus, the polynomial $A_1 \cdots A_{r-1}$ is a divisor of $B^2 - D$. Moreover, $A_1 \cdots A_{r-1}$ is monic. From this, the ideal $\mathcal{I}'$ satisfies (2.18)–(2.20). Therefore, by the hypothesis of induction, for each $i = 1, \ldots, r-1$, $F[t]$-submodule $\mathcal{I}_i := [A_i, B + \sqrt{D}]$ of R is an ideal of R, and we have $\mathcal{I}_i = (A_i, B + \sqrt{D})$ and $N(\mathcal{I}_i) = A_i$. In addition, the ideal $\mathcal{I}'$ is factored into

$$\mathcal{I}' = \mathcal{I}_1 \cdots \mathcal{I}_{r-1}. \tag{2.24}$$

By (2.23) and (2.24), the ideal $\mathcal{I}$ is factored into

$$\mathcal{I} = \mathcal{I}_1 \cdots \mathcal{I}_r.$$

We have proved Lemma 2.2.11. □

Corollary 2.2.12 *Let $D \in F[t]$ be a polynomial satisfying* (2.1) *and* (2.2)*, and we put $R := F[t, \sqrt{D}]$. We write a primitive ideal $\mathcal{I} = [A, B + \sqrt{D}]$ by its canonical basis with $A, B \in F[t]$. If A is factored into $A = P_1 \cdots P_r$ by monic irreducible polynomials $P_i \in F[t]$ $(i = 1, \ldots, r)$, then for $i = 1, \ldots, r$, the $F[t]$-submodule $\mathcal{P}_i := [P_i, B + \sqrt{D}]$ of R is an ideal of R satisfies $\mathcal{P}_i = (P_i, B + \sqrt{D})$ and $N(\mathcal{P}_i) = P_i$. In addition, the ideal $\mathcal{I}$ is factored into*

$$\mathcal{I} = \mathcal{P}_1 \cdots \mathcal{P}_r. \tag{2.25}$$

Moreover, the ideal $\mathcal{P}_i$ is a prime ideal (*therefore, the right hand side of* (2.25) *gives a factorization of $\mathcal{I}$ by prime ideals*)*.*

Proof. It follows from Lemmas 2.2.10 and 2.2.11. □

2.3 The ideal class group of $F[t, \sqrt{D}]$

In this section, we describe some basic properties of the ideal class groups of $F[t, \sqrt{D}]$.

Definition 2.3.1 ([4], Definition 10.20) Let $D \in F[t]$ be a polynomial satisfying (2.1) and (2.2), and we put $R := F[t, \sqrt{D}]$. Consider the following set:

$$\mathrm{Id}(R) := \{\mathcal{I} \mid \mathcal{I} \neq (0) \text{ is an ideal of } R\}.$$

(i) For $\mathcal{I}, \mathcal{I}' \in \mathrm{Id}(R)$, we write $\mathcal{I} \sim \mathcal{I}'$ if there exist $\alpha, \alpha' \in R \setminus \{0\}$ such that $\alpha\mathcal{I} = \alpha'\mathcal{I}'$.

(ii) For $\mathcal{I} \in \mathrm{Id}(R)$, we put

$$[\mathcal{I}]_\sim := \{\mathcal{J} \in \mathrm{Id}(R) \mid \mathcal{J} \sim \mathcal{I}\},$$
$$\mathrm{Cl}(R) := \{[\mathcal{I}]_\sim \mid \mathcal{I} \in \mathrm{Id}(R)\}.$$

The set Cl(R) has the structure of a commutative group by the product $[\mathcal{I}]_\sim[\mathcal{J}]_\sim := [\mathcal{I}\mathcal{J}]_\sim$ (note that the product $[\mathcal{I}]_\sim[\mathcal{J}]_\sim := [\mathcal{I}\mathcal{J}]_\sim$ is well-defined). Here the unit element is $[(1)]_\sim$. For $[\mathcal{J}]_\sim \in \mathrm{Cl}(R)$, its inverse of is given by $[\mathcal{J}^*]_\sim$, where $\mathcal{J}^* := \{\alpha^* \mid \alpha \in \mathcal{J}\}$. The commutative group $\mathrm{Cl}(R)$ is called the *ideal class group* of R.

(iii) If the ideal class group $\mathrm{Cl}(R)$ is finite, then its order is called the *class number* of R. In particular, the ring R has class number 1 if and only if R is a principal ideal domain.

Theorem 2.3.2 ([4], Theorem 10.21) *Let $D \in F[t]$ be a polynomial satisfying* (2.1) *and* (2.2)*, and we put $R := F[t, \sqrt{D}]$ and $g := (\deg D - 1)/2$. For $\mathcal{C} \in \mathrm{Cl}(R)$, there exist $A, B \in F[t]$ such that*

$$(A, B + \sqrt{D}) \in \mathcal{C}, \tag{2.26}$$

$$A \text{ is monic}, \tag{2.27}$$

$$\deg A > \deg B, \tag{2.28}$$

$$g \geq \deg A. \tag{2.29}$$

Proof. For $\mathcal{C} \in \mathrm{Cl}(R)$, consider $\mathcal{I} \in \mathcal{C}$ satisfying $\deg N(\mathcal{I}) = \min\{\deg N(\mathcal{J}) \mid \mathcal{J} \in \mathcal{C}\}$. We write $\mathcal{I} = [A, B + C\sqrt{D}]$ by its canonical basis with $A, B, C \in F[t]$. By Proposition 2.2.5 (v), we have $\deg N(\mathcal{I}) = \deg AC$. Assume $\deg C > 0$. By the definition of the canonical basis, there exist polynomials $A', B' \in F[t]$ such that $A = A'C$ and $B = B'C$, where A' is monic. Putting $\mathcal{I}' := (A', B' + \sqrt{D})$, we have $\mathcal{I} = C\mathcal{I}'$, and thus $\mathcal{I} \sim \mathcal{I}'$. By Remark 2.2.4, the canonical basis of the ideal $\mathcal{I}'$ is $\{A', B' + \sqrt{D}\}$. By Proposition 2.2.5 (v), we have $N(\mathcal{I}') = A'$, and thus $\deg N(\mathcal{I}') = \deg A'$. Therefore, we obtain

$$\deg N(\mathcal{I}) = \deg AC = \deg A'C^2 > \deg A' = \deg N(\mathcal{I}').$$

This contradicts the minimality of the degree of $N(\mathcal{I})$. We have shown $C = 1$, and thus $\mathcal{I} = (A, B + \sqrt{D})$. The polynomials A and B satisfy (2.26)–(2.28). We show that A satisfies (2.29). By Proposition 2.2.8, there exists an ideal $\mathcal{J}$ of R such that $(B + \sqrt{D}) = \mathcal{I}\mathcal{J}$ since $(B + \sqrt{D}) \subset \mathcal{I}$. Note that $\deg N((B + \sqrt{D})) = \deg N(B + \sqrt{D}) = \deg (B^2 - D)$ by Proposition 2.2.5 (iv). In addition $N(\mathcal{I}\mathcal{J}) = N(\mathcal{I})N(\mathcal{J})$ by Proposition 2.2.5 (iii). Thus we have

$$\begin{aligned} \deg (B^2 - D) &= \deg N((B + \sqrt{D})) = \deg N(\mathcal{I}\mathcal{J}) \\ &= \deg N(\mathcal{I}) + \deg N(\mathcal{J}) = \deg A + \deg N(\mathcal{J}). \end{aligned} \tag{2.30}$$

Since $\mathcal{I}\mathcal{J} = (B + \sqrt{D})$ is a principal ideal of R, we have $\mathcal{J}^* \in [\mathcal{J}^*]_\sim = [\mathcal{J}]_\sim^{-1} = [\mathcal{I}]_\sim = \mathcal{C}$. By the minimality of $\deg N(\mathcal{I})$, together with Lemma 2.2.7 (ii), we have

$$\deg N(\mathcal{J}) = \deg N(\mathcal{J}^*) \geq \deg N(\mathcal{I}) = \deg A. \tag{2.31}$$

By (2.30) and (2.31), we obtain

$$\deg (B^2 - D) \geq 2\deg A. \tag{2.32}$$

We have $\deg (B^2 - D) = \max\{2\deg B, \deg D\}$ by (2.5). If $\deg (B^2 - D) = 2\deg B$, then $\deg A \leq \deg B$, which contradicts (2.28). Hence, it follows that

$$\deg (B^2 - D) = \deg D = 2g + 1. \tag{2.33}$$

By (2.32) and (2.33), A satisfies (2.29). From this, the polynomials A and B satisfy (2.26)–(2.29). □

In the above proof, $\mathcal{I}$ is a primitive ideal of R, see Definition 2.2.3. Therefore, we have the following.

Corollary 2.3.3 *Let $D \in F[t]$ be a polynomial satisfying (2.1) and (2.2), and we put $R := F[t, \sqrt{D}]$ and $g := (\deg D - 1)/2$. For any $\mathcal{C} \in \mathrm{Cl}(R)$, there exists a primitive ideal $\mathcal{I} \in \mathcal{C}$ with its canonical basis $\{A, B + \sqrt{D}\}$ such that $g \geq \deg A$.*

Lemma 2.3.4 *Let $D \in F[t]$ be a polynomial satisfying (2.1) and (2.2), and we put $R := F[t, \sqrt{D}]$ and $g := (\deg D - 1)/2$. We define S_R as the set of polynomials $P \in F[t]$ such that*

$$P \text{ is a monic irreducible polynomial}, \tag{2.34}$$
$$g \geq \deg P, \tag{2.35}$$
$$(P) \text{ is not a prime ideal of } R. \tag{2.36}$$

We define T_R as the set of elements $[\mathcal{P}]_\sim \in \mathrm{Cl}(R)$ such that

$$\mathcal{P} \text{ is a prime ideal of } R, \tag{2.37}$$
$$\text{There exists } P \in S_R \text{ satisfying } P \in \mathcal{P}. \tag{2.38}$$

Then, the ideal class group $\mathrm{Cl}(R)$ is generated by T_R. In particular, if $S_R = \emptyset$, then we have $T_R = \emptyset$, and thus

$$\mathrm{Cl}(R) = \langle\, T_R \,\rangle = \langle\, \emptyset \,\rangle = \{\ [(1)]_\sim\},$$

that is, R has class number 1.

Proof. We prove $\mathrm{Cl}(R) \subset \langle\, T_R \,\rangle$. Suppose that $\mathcal{C} \in \mathrm{Cl}(R)$. There exists a primitive ideal $\mathcal{I} := (A, B + \sqrt{D}) \in \mathcal{C}$ such that $g \geq \deg A$ by Corollary 2.3.3, where $\{A, B + \sqrt{D}\}$ is the canonical basis of $\mathcal{I}$ with $A, B \in F[t]$. First let us assume $\deg A = 0$. In this case, we have $\mathcal{I} = (1)$ since $A \in F^\times$. The unit element of the ideal class group Cl(R) is $[(1)]_\sim$, see Definition 2.3.1 (ii). From this, since $\mathcal{C}$ is a set containing (1), the element $\mathcal{C}$ equals the unit element $[(1)]_\sim \in \mathrm{Cl}(R)$. Here $\langle\, T_R \,\rangle$ is a subgroup of Cl(R), and thus $\mathcal{C} = [(1)]_\sim \in \langle\, T_R \,\rangle$. Next, we show Lemma 2.3.4 in the case of $\deg A > 0$. The polynomial A is factored into $A = P_1 \cdots P_r$ by monic irreducible polynomials. By Corollary 2.2.12, the following are satisfied for each $i = 1, \ldots, r$:

> The $F[t]$-submodule $\mathcal{P}_i := [P_i, B + \sqrt{D}]$ is a prime ideal of R. In addition, we have $\mathcal{P}_i = (P_i, B + \sqrt{D})$ and $N(\mathcal{P}_i) = P_i$.

Moreover, $\mathcal{I}$ is factored into

$$\mathcal{I} = \mathcal{P}_1 \cdots \mathcal{P}_r \tag{2.39}$$

by Corollary 2.2.12. Note that $(P_i) \subset (P_i, B + \sqrt{D}) = \mathcal{P}_i$. If $(P_i) = \mathcal{P}_i$, then

$$(N(\mathcal{P}_i)) = (N((P_i))) = (N(P_i)) = (P_i^2)$$

by Proposition 2.2.5 (iv). On the other hand, we have $(N(\mathcal{P}_i)) = (P_i)$, and thus the above equalities contradict $(P_i) \neq (P_i^2)$. We have $(P_i) \subsetneq \mathcal{P}_i$, and thus the ideal (P_i) is not a

maximal ideal. Since R is Dedekind domain, the ideal (P_i) is not a prime ideal. (More generally, any non-zero maximal ideal of a Dedekind domain is a prime ideal.) In addition, we have $\deg P_i \leq g$ since P_i is a prime factor of A and since $\deg A \leq g$. From this, the polynomial P_i satisfies (2.34), (2.35) and (2.36). Thus, we have $P_i \in S_R$. In addition, it follows from (2.39) that

$$\mathcal{C} = [\mathcal{I}]_{\sim} = [\mathcal{P}_1 \cdots \mathcal{P}_r]_{\sim} = [\mathcal{P}_1]_{\sim} \cdots [\mathcal{P}_r]_{\sim}.$$

Note that a representative $\mathcal{P}_i$ of $[\mathcal{P}_i]_{\sim}$ satisfies (2.37) and (2.38) for each $i = 1, \ldots, r$. Therefore, we have $[\mathcal{P}_i]_{\sim} \in T_R$, and thus we have $\mathcal{C} \in \langle T_R \rangle$. We have proved $\mathrm{Cl}(R) \subset \langle T_R \rangle$. □

3 The proof of the main theorem in characteristic not 2

In this section, we prove Theorem 1.2. First, let us recall Theorem 1.2.

Theorem 1.2 *Let F be a field with $\mathrm{char}(F) \neq 2$. Let $D \in F[t]$ be a polynomial with an odd degree, and put $g := (\deg D - 1)/2$. For $X \in F[t]$, put*

$$f(X) := X^2 - D.$$

The following are equivalent:

(i) *The polynomial D is square free, and the ring*

$$F[t, \sqrt{D}] := \{A + B\sqrt{D} \mid A, B \in F[t]\}$$

has class number 1.

(ii) *For any $A \in F[t]$ with $\deg A \leq 2g$, the polynomial $f(A) \in F[t]$ is irreducible.*

(iii) *For any $A \in F[t]$ with $\deg A < g$, the polynomial $f(A) \in F[t]$ is irreducible.*

Proof. (i) ⇒ (ii) Assume (i), and there exists $A \in F[t]$ satisfying $\deg A \leq 2g$ such that $f(A)$ is reducible over F. By a constant $c \in F$ and monic irreducible polynomials $P_i \in F[t]$ with $1 \leq i \leq r$, the polynomial $f(A)$ is factored into

$$f(A) = cP_1 \cdots P_r,$$

where we admit that $P_i = P_j$ for $1 \leq i < j \leq r$. By our hypothesis, we have $r \geq 2$. We may assume $\deg P_{r-1} \leq \deg P_i$ for all $1 \leq i \leq r$, and put $P := P_{r-1}$. It follows that

$$\deg P^2 = \deg P_{r-1}^2 \leq \deg (P_1 \cdots P_{r-1} P_{r-1}) \leq \deg (P_1 \cdots P_{r-1} P_r) = \deg f(A),$$

and therefore

$$\deg P^2 \leq \deg f(A).$$

Here, we have $\deg f(A) = \deg(A^2 - D) = \max\{\deg A^2, \deg D\}$ by (2.5). Now, we show $\deg P < \deg D$. First, in the case of $\deg f(A) = \deg D$, we have $\deg P < \deg f(A) = \deg D$ since P is a divisor of $f(A)$ with $\deg P \geq 1$. Next, assume $\deg f(A) = \deg A^2$. By our hypothesis, we have $\deg A \leq 2g$ and thus

$$2\deg P = \deg P^2 \leq \deg f(A) = \deg A^2 \leq 4g = 4\left(\frac{\deg D - 1}{2}\right) = 2(\deg D - 1) < 2\deg D.$$

Therefore, it follows that $\deg P < \deg D$. Now, we lead to a contradiction by proving $\deg P \geq \deg D$. The polynomial P is a divisor of $f(A) = A^2 - D$. Thus, it follows from Proposition 2.2.1 that the $F[t]$-submodule $\mathcal{I} := [P, A + \sqrt{D}]$ of R is an ideal of R, and we have $P \in \mathcal{I}$. Moreover, the polynomial P is monic, and thus P and A satisfy (2.8)–(2.10). From this, we have $N(\mathcal{I}) = P$ by Remark 2.2.6. There exists $\alpha = A' + B'\sqrt{D}$ with $A', B' \in F[t]$ such that $\mathcal{I} = (\alpha)$ since R has class number 1 by our hypothesis, see Definition 2.3.1 (iii). Here, suppose $B' = 0$. Since $(\alpha) = (A')$, we have

$$(N((\alpha))) = (N(A')) = ((A')^2), \text{ and } (N((\alpha))) = (N(\mathcal{I})) = (P)$$

by Proposition 2.2.5 (iv). Hence we have $((A')^2) = (P)$. Therefore, there exists $X + Y\sqrt{D} \in R$ with $X, Y \in F[t]$ such that $P = (X + Y\sqrt{D})(A')^2$. If $A' = 0$, then $P = 0$ and this contradicts that P is monic. Next, let us assume $A' \neq 0$. Since P is an element of $F[t]$, we have $Y = 0$, and thus $P = X(A')^2$. If A' is a constant, we have $(P) = ((A')^2) = (1)$, and this contradicts that P is irreducible. Otherwise, the polynomial P is divisible by A' which is not a constant. There is a contradiction in each case. Therefore, it follows that $B' \neq 0$. Now, we have $N(\alpha) = (A')^2 - (B')^2 D$, and thus

$$\deg N(\alpha) = \max\{\deg (A')^2, \deg (B')^2 D\} \geq \deg D$$

by (2.5). In addition, it follows from Proposition 2.2.5 (iv) that $\deg N(\alpha) = \deg N((\alpha))$. From this, we have

$$\deg D \leq \deg N(\alpha) = \deg N((\alpha)) = \deg N(\mathcal{I}) = \deg P,$$

which contradicts $\deg P < \deg D$.

(ii) $\Rightarrow$ (iii) Straightforward.

(iii) $\Rightarrow$ (i) First we claim that D is square free. Indeed, since $\deg 0 < g$, it follows from our assumption that $0^2 - D = -D$ is irreducible. Let S_R be the set defined in Lemma 2.3.4. We next prove that R has class number 1. By Lemma 2.3.4, it suffices to show $S_R = \emptyset$. We suppose that $S_R \neq \emptyset$, that is, there exists a monic irreducible polynomial $P \in F[t]$ with $\deg P \leq g$ such that the ideal (P) of R is not a prime ideal. Then, there exists a prime ideal $\mathcal{P} \subset R$ such that $(P) = \mathcal{P}\mathcal{P}^*$ by Lemma 2.2.9, where we put $\mathcal{P}^* := \{\alpha^* \mid \alpha \in \mathcal{P}\}$. By the same argument in the proof of Lemma 2.2.9, we have $N(\mathcal{P}) = P$. The prime ideal $\mathcal{P}$ is written as $\mathcal{P} = [P', A + C\sqrt{D}]$ by its canonical basis $\{P', A + C\sqrt{D}\}$ with $P', A, C \in F[t]$. By Lemma 2.2.10, we have $P' = N(P)$ and $C = 1$, and hence $P' = P$. By Proposition 2.2.2, the following are satisfied:

$$A^2 - D\ (= f(A)) \textit{ is divisible by } P, \text{ and } \deg A < \deg P.$$

Here, it follows from (2.5) that

$$\deg f(A) = \max\{\deg A^2, \deg D\} \geq \deg D.$$

Note that $\deg P \leq g$, and thus

$$\deg P \leq g < 2g + 1 = \deg D.$$

Therefore, we obtain $\deg f(A) > \deg P$, and hence P is a non-trivial divisor of $f(A)$. Thus, the polynomial $f(A)$ is reducible. Now, we have $\deg A < g$ since $\deg P \leq g$ and $\deg A < \deg P$. This is a contradiction. □

4 The case of characteristic 2

In this section, we give an analogue of Theorem 1.2 for a polynomial ring over a field with characteristic 2.

Notation

Throughout Section 4, let F be a field with $\mathrm{char}(F) = 2$. Let $F[t]$ be the univariate polynomial ring with an indeterminate t over F, and $F(t)$ the univariate rational function field over F. If the leading cofficient of $X \in F[t]$ equals 1, the polynomial X is said to be monic or a monic polynomial. It is straightforward that there exists $D \in F[t]$ such that

$$\deg D \text{ is odd}, \tag{4.1}$$
$$A^2 + A + D \neq 0 \text{ for any } A \in F(t). \tag{4.2}$$

We fix such a $D \in F[t]$ throughout this notation paragraph. We put $g := (\deg D - 1)/2$. Let $\overline{F(t)}$ denote the algebraic closure of $F(t)$, and we fix $\omega_D \in \overline{F(t)}$ satisfying

$$\omega_D{}^2 + \omega_D + D = 0.$$

Consider the following sets:

$$F(t, \omega_D) := \{A + B\omega_D \mid A, B \in F(t)\},$$
$$F[t, \omega_D] := \{A + B\omega_D \mid A, B \in F[t]\}.$$

Note that $F(t, \omega_D)$ is a quadratic extension of $F(t)$. For $\alpha := A + B\omega_D \in F(t, \omega_D)$ with $A, B \in F(t)$, we define its conjugate α^*, its trace $Tr(\alpha)$ and its norm $N(\alpha)$ as follows:

$$\alpha^* := A + B(\omega_D + 1) = A + B + B\omega_D,$$
$$Tr(\alpha) := \alpha + \alpha^* = B,$$
$$N(\alpha) := \alpha\alpha^* = A^2 + AB + B^2D. \tag{4.3}$$

Here, we claim

$$\deg N(\alpha) = \deg (A^2 + AB + B^2D) = \max\{\deg A^2, \deg B^2D\}.$$

First, we suppose $\deg A^2 \leq \deg AB$. Then we have $\deg A \leq \deg B$. In addition, we have $\deg D \geq 1$ by (4.1), and thus $\deg B^2 < \deg B^2 D$. Therefore, it follows that

$$\deg A^2 \leq \deg AB \leq \deg B^2 < \deg B^2 D,$$

and hence $\deg N(\alpha) = \deg B^2 D$. Next, we suppose $\deg A^2 > \deg AB$. Then $\deg(A^2 + AB) = \deg A^2 = 2\deg A$ is even. On the other hand, D is a polynomial with an odd degree. Since $B^2 D$ and A^2 have different degrees, one of their leading coefficients remains in (4.3). Therefore, we obtain $\deg N(\alpha) = \max\{\deg A^2, \deg B^2 D\}$. For $\alpha_1, \ldots, \alpha_r \in R := F[t, \omega_D]$, we put

$$(\alpha_1, \ldots, \alpha_r) := \{\alpha_1 \xi_1 + \cdots + \alpha_r \xi_r \in R \mid \xi_1, \ldots, \xi_r \in R\},$$
$$[\alpha_1, \ldots, \alpha_r] := \{\alpha_1 X_1 + \cdots + \alpha_r X_r \in R \mid X_1, \ldots, X_r \in F[t]\}.$$

Note that $(\alpha_1, \ldots, \alpha_r)$ is an ideal of R while $[\alpha_1, \ldots, \alpha_r]$ is an $F[t]$-submodule of R.

4.1 The integral closures of $F[t]$ in $F(t, \omega_D)$

In this section, we prove $F[t, \omega_D]$ is the integral closure of $F[t]$ in $F(t, \omega_D)$. First, we give one of elementary properties of a principal ideal domain.

Lemma 4.1.1 *Consider polynomials A and $B \in F[t]$ with $B \neq 0$ such that A and B are co-prime. If A^2 is divisible by B, then $B \in F^\times$.*

Proof. Since A and B are co-prime, there exist X, $Y \in F[t]$ such that $AX + BY = 1$. By multiplying both sides of this equality by A, we have $A^2 X + ABY = A$. Moreover, there exists $C \in F[t]$ such that $A^2 = BC$ because A^2 is divisible by B. Hence, we obtain

$$A = A^2 X + ABY = BCX + ABY = B(CX + AY).$$

Therefore, A is divisible by B. Since A and B are co-prime, we have $B \in F^\times$. □

Theorem 4.1.2 *Let $D \in F[t]$ be a polynomial satisfying* (4.1) *and* (4.2)*, and we put $R := F[t, \omega_D]$. For $\alpha \in F(t, \omega_D)$, the following are equivalent:*

(i) $\alpha \in R$.

(ii) $Tr(\alpha), N(\alpha) \in F[t]$.

(iii) *There exist $A, B \in F[t]$ such that $\alpha^2 + A\alpha + B = 0$.*

Proof. We prove (ii) ⇒ (i). Putting $\alpha := X + Y\omega_D$ with $X, Y \in F(t)$, we show $X, Y \in F[t]$. It is straightforward that $Y = Tr(\alpha) \in F[t]$. Assume $X \neq 0$. We write $X = A/B$ ($A, B \in F[t]$ with $B \neq 0$ such that A and B are co-prime). Here, we show that $B \in F^\times$. By our hypothesis, there exists $S \in F[t]$ such that

$$S = N(\alpha) = X^2 + XY + Y^2 D = \frac{A^2}{B^2} + Y\frac{A}{B} + Y^2 D.$$

Hence, we obtain the equation $A^2 = (BS + AY + BY^2 D)B$, which shows that A^2 is divisible by B. Thus, we have $B \in F^\times$ by Lemma 4.1.1. We prove (i) ⇒ (ii), (ii) ⇒ (iii) and (iii) ⇒ (ii) similarly to Theorem 2.1.2. □

It follows from Theorem 4.1.2 that $R := F[t, \omega_D]$ is the integral closure of $F[t]$ in $F(t, \omega_D)$. Hence R is a Dedekind domain by the same argument in the case of $\mathrm{char}(F) \neq 2$, see the last paragraph of Section 2.1.

4.2 The canonical basis of an ideal of $F[t, \omega_D]$

In this section, we introduce the canonical basis of an ideal of $F[t, \omega_D]$.

Proposition 4.2.1 *Let $D \in F[t]$ be a polynomial satisfying* (4.1) *and* (4.2)*, and we put $R := F[t, \omega_D]$. For $A, B, C \in F[t]$ with $C \neq 0$, the following are equivalent:*

(i) *The $F[t]$-submodule $\mathcal{I} := [A, B + C\omega_D]$ of R is an ideal of R, and we have $\mathcal{I} = (A, B + C\omega_D)$.*

(ii) *A and B are divisible by C and $(B(B + C)/C) + CD$ is divisible by A.*

Proof. Similarly to the proof of Proposition 2.2.1. □

Proposition 4.2.2 *Let $D \in F[t]$ be a polynomial satisfying* (4.1) *and* (4.2)*, and we put $R := F[t, \omega_D]$. For any ideal $\mathcal{I} \subset R$ with $\mathcal{I} \neq (0)$, there exist unique $A, B, C \in F[t]$ such that*

$$\mathcal{I} \cap F[t] = [A], \tag{4.4}$$
$$\mathcal{I} = [A, B + C\omega_D] = (A, B + C\omega_D), \tag{4.5}$$
$$A \text{ and } B \text{ are divisible by } C, \tag{4.6}$$
$$(B(B + C)/C) + CD \text{ is divisible by } A, \tag{4.7}$$
$$A \text{ and } C \text{ are monic}, \tag{4.8}$$
$$\deg A > \deg B. \tag{4.9}$$

Proof. Similarly to the proof of Proposition 2.2.2. □

Definition 4.2.3 In Proposition 4.2.2, the set $\{A, B + C\omega_D\}$ is called the *canonical basis* of $\mathcal{I}$. If $C = 1$, then $\mathcal{I}$ is called a *primitive ideal* of R.

4.3 The main theorem in characteristic 2

We prove the following theorem similarly to the proof of Theorem 1.2.

Theorem 4.3.1 *Let F be a field with $\mathrm{char}(F) = 2$. Let $D \in F[t]$ be a polynomial satisfying* (4.1) *and* (4.2)*, and put $g := (\deg D - 1)/2$. For $X \in F[t]$, put*

$$f(X) := X^2 + X + D.$$

The following are equivalent:

(i) *The ring*

$$F[t, \omega_D] := \{A + B\omega_D \mid A, B \in F[t]\}$$

has class number 1*.*

(ii) *For any $A \in F[t]$ with $\deg A \leq 2g$, the polynomial $f(A) \in F[t]$ is irreducible.*

(iii) *For any $A \in F[t]$ with $\deg A < g$, the polynomial $f(A) \in F[t]$ is irreducible.*

5 The computation of an example

In this section, we check that Example 1.3 satisfies the conditions stated in Theorem 1.2. Let us recall Example 1.3.

Example 1.3 Consider the following univariate polynomial over $\mathbb{F}_3[t]$ with the indeterminate X:

$$f(X) := X^2 - t^3 + t + 1.$$

Then, for any $A \in \mathbb{F}_3[t]$ with $\deg A \leq 2$, the polynomial $f(A) \in \mathbb{F}_3[t]$ is irreducible.

Moreover, we introduce an analogue of Euler primes for $\mathbb{F}_4[t]$.

Example 5.1 Consider the following univariate polynomial over $\mathbb{F}_4[t]$ with the indeterminate X:

$$f(X) := X^2 + X + t^3 + \alpha,$$

where $\alpha \in \mathbb{F}_4$ is a generator of $\mathbb{F}_4^\times$. Then, for any $A \in \mathbb{F}_4[t]$ with $\deg A \leq 2$, the polynomial $f(A) \in \mathbb{F}_4[t]$ is irreducible.

We check that Example 5.1 satisfies the conditions stated in Theorem 4.3.1 too. First, the following is already known. See [5] for details.

Theorem 5.2 ([5], Theorem 1.1 (vi), (vii)) *The rings* $\mathbb{F}_3[t, \sqrt{t^3 - t - 1}]$ *and* $\mathbb{F}_4[t, \omega_{t^3+\alpha}]$ *have class number* 1*, where* $\alpha \in \mathbb{F}_4$ *is a generator of* $\mathbb{F}_4^\times$*.*

According to Theorem 1.2 (resp. Theorem 4.3.1), the claim in Example 1.3 (resp. Example 5.1) follows from Theorem 5.2. We check directly the claim in Example 1.3: for any $A \in \mathbb{F}_3[t]$ with $\deg A \leq 2$, the polynomial $A^2 - t^3 + t + 1 \in \mathbb{F}_3[t]$ is irreducible. Polynomials of the form $A^2 - t^3 + t + 1 \in \mathbb{F}_3[t]$ ($A \in \mathbb{F}_3[t]$ with $\deg A \leq 2$) are the following:

$$t^4 + 2t^3 + 2t^2 + t + 2, \tag{5.1}$$
$$t^4 + 2t^3 + t^2 + t + 2, \tag{5.2}$$
$$t^4 + 2t^3 + t + 1, \tag{5.3}$$
$$t^4 + t^3 + 2t^2 + 2t + 2, \tag{5.4}$$
$$t^4 + t^3 + t^2 + t + 1, \tag{5.5}$$
$$t^4 + t^3 + 2, \tag{5.6}$$
$$t^4 + 2t^2 + 2, \tag{5.7}$$
$$t^4 + t^2 + t + 1, \tag{5.8}$$
$$t^4 + 2t + 2, \tag{5.9}$$
$$2t^3 + t^2 + 2t + 2, \tag{5.10}$$
$$2t^3 + t^2 + t + 1, \tag{5.11}$$
$$2t^3 + t^2 + 2, \tag{5.12}$$
$$2t^3 + t + 2, \tag{5.13}$$
$$2t^3 + t + 1. \tag{5.14}$$

We show that (5.1)–(5.14) are irreducible. Substituting all elements of $\mathbb{F}_3$ into the polynomials (5.1)–(5.14), one can check that they have no roots in $\mathbb{F}_3$. Thus, (5.1)–(5.14) have no linear factors. Therefore, the cubic polynomials (5.10)–(5.14) are irreducible, and (5.1)–(5.9) are not factored into a product of linear and cubic polynomials. Next, we suppose that one of (5.1)–(5.9)

$$t^4 + s_3t^3 + s_2t^2 + s_1t + s_0, \quad s_0, s_1, s_2, s_3 \in \mathbb{F}_3$$

is factored into

$$t^4 + s_3t^3 + s_2t^2 + s_1t + s_0 = (t^2 + s_5t + s_4)(t^2 + s_7t + s_6) \tag{5.15}$$

for $s_4, s_5, s_6, s_7 \in \mathbb{F}_3$. The right hand side of (5.15) is expanded into

$$t^4 + (s_5 + s_7)t^3 + (s_4 + s_5s_7 + s_6)t^2 + (s_4s_7 + s_5s_6)t + s_4s_6. \tag{5.16}$$

By comparing coefficients in (5.15) and (5.16), we obtain

$$\begin{cases} s_3 = s_5 + s_7, \\ s_2 = s_4 + s_5s_7 + s_6, \\ s_1 = s_4s_7 + s_5s_6, \\ s_0 = s_4s_6. \end{cases} \tag{5.17}$$

However, one can check that the system (5.17) has no solution for any coefficients (s_0, s_1, s_2, s_3) in (5.1)–(5.9). Therefore, (5.1)–(5.9) are irreducible. We check directly the claim in Example 5.1 similarly to the claim in Example 1.3. Polynomials of the form $A^2+A+t^3+\alpha \in \mathbb{F}_4[t]$ ($A \in \mathbb{F}_4[t]$ with $\deg A \leq 2$) are the following:

$$\alpha^2t^4 + t^3 + \alpha^2t^2 + t + \alpha^2, \tag{5.18}$$
$$\alpha^2t^4 + t^3 + \alpha^2t^2 + t + \alpha, \tag{5.19}$$
$$\alpha^2t^4 + t^3 + \alpha t^2 + \alpha^2, \tag{5.20}$$
$$\alpha^2t^4 + t^3 + \alpha t^2 + \alpha, \tag{5.21}$$
$$\alpha^2t^4 + t^3 + t^2 + \alpha t + \alpha^2, \tag{5.22}$$
$$\alpha^2t^4 + t^3 + t^2 + \alpha t + \alpha, \tag{5.23}$$
$$\alpha^2t^4 + t^3 + \alpha^2t + \alpha^2, \tag{5.24}$$
$$\alpha^2t^4 + t^3 + \alpha^2t + \alpha, \tag{5.25}$$
$$\alpha t^4 + t^3 + \alpha^2t^2 + \alpha^2, \tag{5.26}$$
$$\alpha t^4 + t^3 + \alpha^2t^2 + \alpha, \tag{5.27}$$
$$\alpha t^4 + t^3 + \alpha t^2 + t + \alpha^2, \tag{5.28}$$
$$\alpha t^4 + t^3 + \alpha t^2 + t + \alpha, \tag{5.29}$$
$$\alpha t^4 + t^3 + t^2 + \alpha^2t + \alpha^2, \tag{5.30}$$
$$\alpha t^4 + t^3 + t^2 + \alpha^2t + \alpha, \tag{5.31}$$
$$\alpha t^4 + t^3 + \alpha t + \alpha^2, \tag{5.32}$$
$$\alpha t^4 + t^3 + \alpha t + \alpha, \tag{5.33}$$
$$t^4 + t^3 + \alpha^2t^2 + \alpha^2t + \alpha^2, \tag{5.34}$$
$$t^4 + t^3 + \alpha^2t^2 + \alpha^2t + \alpha, \tag{5.35}$$
$$t^4 + t^3 + \alpha t^2 + \alpha t + \alpha^2, \tag{5.36}$$

$$t^4+t^3+\alpha t^2+\alpha t+\alpha, \tag{5.37}$$
$$t^4+t^3+t^2+\alpha^2, \tag{5.38}$$
$$t^4+t^3+t^2+\alpha, \tag{5.39}$$
$$t^4+t^3+t+\alpha^2, \tag{5.40}$$
$$t^4+t^3+t+\alpha, \tag{5.41}$$
$$t^3+\alpha^2t^2+\alpha t+\alpha^2, \tag{5.42}$$
$$t^3+\alpha^2t^2+\alpha t+\alpha, \tag{5.43}$$
$$t^3+\alpha t^2+\alpha^2t+\alpha^2, \tag{5.44}$$
$$t^3+\alpha t^2+\alpha^2t+\alpha, \tag{5.45}$$
$$t^3+t^2+t+\alpha^2, \tag{5.46}$$
$$t^3+t^2+t+\alpha, \tag{5.47}$$
$$t^3+\alpha^2, \tag{5.48}$$
$$t^3+\alpha. \tag{5.49}$$

(5.18)–(5.49) are irreducible over $\mathbb{F}_4$. Here, we give another proof of Theorem 5.2:

Proof of Theorem 5.2. By the claim in Example 1.3, for any $A \in \mathbb{F}_3[t]$ with $\deg A < 1$, the polynomial $A^2 - t^3 + t + 1 \in \mathbb{F}_3[t]$ is irreducible. This satisfies the condition (iii) of Theorem 1.2. Hence, it follows from Theorem 1.2 that $\mathbb{F}_3[t, \sqrt{t^3-t-1}]$ has class number 1. Similarly, we prove that $\mathbb{F}_4[t, \omega_{t^3+\alpha}]$ has class number 1 by Theorem 4.3.1. □

6 Conclusion and future work

In this paper, we described that there is a deep analogy between the ring of rational integers and a univariate polynomial ring over a field. We gave an analogue of Euler primes for polynomials and a polynomial version of Theorem 1.2. Euler primes have the following property:

> "For $\alpha = (1/2) + (1/2)\sqrt{-163}$ and $\alpha^* = (1/2) - (1/2)\sqrt{-163}$, the *integer* $x^2+x+41 = (x+\alpha)(x+\alpha^*)$ is *prime* for $x \in \mathbb{Z}$ with $0 \leq x < \alpha\alpha^* - 1 (= 40)$".

As we showed in this paper, an analogue of Euler primes for polynomials in $\mathbb{F}_3[t]$ is given by

> "For $\alpha := \sqrt{t^3-t-1}$, $\alpha^* := -\sqrt{t^3-t-1} \in \mathbb{F}_3[t, \sqrt{t^3-t-1}]$, the polynomial $X^2 - t^3 + t + 1 = (X+\alpha)(X+\alpha^*)$ is *irreducible* for $X \in \mathbb{F}_3[t]$ with $\deg X < \deg(t^3-t-1)$".

Euler primes (resp. its analogue for polynomials) correspond to an extension ring of the ring of rational integers (resp. a polynomial ring) with class number 1. In rational integers, there are other special prime numbers which are related to an integer ring of a quadratic field. For example, a rational integer of the form $2x^2 + 29$ is a prime for each $x = 0, 1, \ldots, 28$. Their property is related to the fact that the integer ring

$$\mathbb{Z}\left[\sqrt{-58}\right] = \left\{ a + b\sqrt{-58} \;\middle|\; a, b \ \in \mathbb{Z} \right\}$$

has class number 2, see [1] and [6]. Similarly to Euler primes, we expect that we can construct irreducible polynomials which are viewed as primes of the type $2x^2 + 29$. Our future work is to find such irreducible polynomials.

Acknowledements

I am grateful to my advisor Professor Yuichiro Takeda who gave me beneficial advices about this study and a polite guidance of writing a paper. When I got bogged down in my study, he always treated me patiently and politely. In addition, I thank him for researching fields related to this study and giving me invaluable advices.

I would like to thank Professor Yuichiro Taguchi (Tokyo Institute of Technology) who were my former supervisor for earnest guidance of my seminar. He was the first person who suggested me the research theme as Euler primes for a polynomial ring. Because of his offer, I could get my own results.

I would like to thank Professor Minoru Itoh (Kagoshima University). When I enrolled in Kagoshima University, he led me to study the relationship between Euler primes and class numbers. Since I learned about Euler primes on his lecture of ring theory for the first time, I could start to study on this field.

I also would like to thank Momonari Kudo for teaching me how to write a paper in English. Even though I often made grammatical mistakes and typos in writing this paper, he kept on supervising me tirelessly. I appreciate his such guidance. In addition, I thank him for enlightening me on the possibilities for the development of this study.

Finally, I would like to thank my family for their financial supports and kind hearted words encouraging me so far.

References

[1] F. G. Frobenius, *Über quadratische Formen die viele Primzahlen darstellen*, Sitzungsberichte der Königliche Akademie der Wissenschaften zu Berlin, pp. 966–980, 1912.

[2] G. Rabinovitch, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern*, Journal fur die reine und angewandte Mathematik, Volume **142**, pp. 153–164, 1913.

[3] N. Aoki, *Number theory of prime numbers and quadratic fields* (in Japanese), Kyouritsu Press, 2012.

[4] T. Yamazaki, *Elementary number theory —first steps towards arithmetic geometry* (in Japanese), Kyouritsu Press, 2015.

[5] Pietro Mercuri, Claudio Stirpe, *Classification of Algebraic Function Fields with Class Number One*, Journal of Number Theory, Volume **154**, pp. 365–374, 2015.

[6] M. D. Hendy, *Prime Quadratics associated with complex quadratic fields of class number two*, Proceedings of the American Mathematical Society, Volume **43**, No. 2, pp. 253–260, 1974.