บทตั้งของเกาส์สำหรับฟิลด์ฟังก์ชัน

นายบวร คูหิรัญ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2551

GAUSS' LEMMA FOR FUNCTION FIELDS

Mr. Borworn Khuhirun

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Mathematics

Department of Mathematics

Faculty of Science

Chulalongkorn University

Academic Year 2008

Thesis Title	GAUSS' LEMMA FOR FUNCTION FIELDS
By	Mr. Borworn Khuhirun
Field of Study	Mathematics
Advisor	Associate Professor Ajchara Harnchoowong, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

S. Hannongbua ..... Dean of the Faculty of Science

(Professor Supot Hannongbua, Dr.rer.nat.)

THESIS COMMITTEE

P. Udomkavanich ..... Chairman

(Associate Professor Patanee Udomkavanich, Ph.D.)

Ajchara Harnchoowong ..... Advisor

(Associate Professor Ajchara Harnchoowong, Ph.D.)

Yotsanan Meemark ..... Examiner

(Yotsanan Meemark, Ph.D.)

U. Leerawat ..... External Examiner

(Associate Professor Utsanee Leerawat, Ph.D.)

บวร คูหิรัญ : บทตั้งของเกาส์สำหรับฟิลด์ฟังก์ชัน. (GAUSS' LEMMA FOR FUNCTION FIELDS). อ. ที่ปรึกษาวิทยานิพนธ์หลัก : รศ. ดร. อัจฉรา หาญชูวงศ์, 28 หน้า.

กำหนดให้ L เป็นฟิลด์จำนวนและให้ O_L เป็นริงของจำนวนเต็มพีชคณิตใน L สำหรับพหุนาม f ซึ่งมีสัมประสิทธิ์อยู่ใน O_L *คอนเทนต์* ของ f ใน L คือ ไอดีล ของ O_L ซึ่งก่อกำเนิดโดยสัมประสิทธิ์ของ f พหุนาม f จะถูกกล่าวว่า *พริมีทีฟ* ใน L เมื่อคอนเทนต์ของ f ใน L คือ O_L

ในปีคริสต์ศักราช 2005 อาทูโร่ แมกจิดิน และ เดวิด แมกคินนอน ได้พิสูจน์บทตั้งของเกาส์สำหรับฟิลด์จำนวน ซึ่งกล่าวว่า ผลคูณของพหุนามพริมีทีฟสองพหุนามยังคงเป็นพหุนามพริมีทีฟ และบทประยุกต์ซึ่งเป็นผลที่ตามมาจากบทตั้งของเกาส์สำหรับฟิลด์จำนวน

ในงานวิจัยนี้ เราจะศึกษาผลงานของ อาทูโร่ และ เดวิด สำหรับฟิลด์ฟังก์ชัน

ภาควิชา.....คณิตศาสตร์..... ลายมือชื่อนิสิต.....บวร คูหิรัญ.....

สาขาวิชา.....คณิตศาสตร์..... ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก.....อัจฉรา หาญชูวงศ์.....

ปีการศึกษา.....2551.....

4972346023 : MAJOR MATHEMATICS

KEYWORDS : GAUSS' LEMMA / FUNCTION FIELDS

BORWORN KHUHIRUN : GAUSS' LEMMA FOR FUNCTION FIELDS.

ADVISOR : ASSOC. PROF. AJCHARA HARNCHOOWONG, Ph.D., 28 pp.

Let L be a number field and O_L the ring of algebraic integers in L. For a polynomial f with coefficients in O_L, the *content* of f in L is the ideal of O_L generated by coefficients of f. The polynomial f is *primitive* in L if the content of f in L is O_L.

In 2005, Arturo Magidin and David McKinnon proved the Gauss' lemma for number fields, the product of two primitive polynomials is also primitive, and some applications following from Gauss' lemma for number fields.

A *function field* K over a finite field k is a finite separable field extension over $k(x)$ where x is a transcendantal element.

In this research, we study Magidin and McKinnon's work on the function fields.

Department : ....Mathematics.... Student's Signature : Borworn Khuhirun

Field of Study : ....Mathematics.... Advisor's Signature : Ajchara Harnchoowan

Academic Year : .....2008.....

ACKNOWLEDGEMENTS

I am very grateful to Associate Professor Dr. Ajchara Harnchoowong, my thesis supervisor, for her kind and helpful suggestions and guidance. Her assistance and careful reading are of great value to me in the preparation and completion of this thesis. I would like to express my gratitude to my thesis committee for their valuable comments and to all the lecturers during my study.

Also, I would like to acknowledge the Development and Promotion of Science and Technology Talents Project for the financial support during the period of my study.

In particular, I feel very grateful to my parents for their kind and untired encouragement throughout my study.

CONTENTS

CHAPTER I

INTRODUCTION

The content of a polynomial with coefficients in $\mathbb{Z}$ is defined to be the greatest common divisor of its coefficients and a polynomial is said to be primitive if and only if its content is 1. Gauss' lemma is stated that the product of two primitive polynomials is again primitive. In [1], Arturo Magidin and David McKinnon studied this for polynomials with coefficients in the ring of integers O_L of a number field L. Unlike, the ring of integers $\mathbb{Z}$, for any number field L, O_L may not be a unique factorization domain. Fortunately, in O_L, the factorization of ideals as a product of prime ideals is unique. The content of a polynomial with coefficients in O_L is defined to be the ideal generated by its coefficients and a polynomial is said to be primitive if and only if its content is O_L. Gauss' lemma is also true in O_L, i.e. the product of two primitive polynomials is primitive.

A function field K over a finite field k is a finite separable field extension over $k(x)$ where x is a transcendental element. In this research, we study whether these properties still hold in function fields.

CHAPTER II

PROPERTIES OF FUNCTION FIELDS

2.1 Function Fields and Integrallity

In this section, we will give the definition of function fields and their properties. Let k be a finite field of q elements for some prime power q. We introduce function fields by the following definition.

Definition 2.1.1. Let k be a finite field and x a transcendental element.
A *function field* K over k is a finite separable field extension over $k(x)$.

From now on, we use K as a function field over k together with x a transcendental element.

Definition 2.1.2. Let L be a field extension over $k(x)$. $\alpha \in L$ is said to be *integral* over $k[x]$ if there exist $a_0, a_1, \ldots, a_{n-1} \in k[x]$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Definition 2.1.3. Let L be a field extension over $k(x)$. The set of all elements in L that are integral over $k[x]$ forms a subring of L containing $k[x]$. It is called the *integral closure* of $k[x]$ in L, denoted by O_L.

For a function field K over k we have :

Theorem 2.1.4. *Let K be a function field over k. Then K is the field of fractions of O_K.*

Proof. Let $\alpha \in K$. Since K is a finite field extension over $k(x)$, K is a algebraic extension over $k(x)$. Consequently, α is algebraic over $k(x)$. Then there exist $a_0, a_1, \ldots, a_{n-1} \in k(x)$ such that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Moreover, there exists $0 \neq d \in k[x] \subseteq O_K$ such that $da_i \in k[x]$ for all i. By multiplying d^n to both sides of the previous equation, we have

$$(d\alpha)^n + da_{n-1}(d\alpha)^{n-1} + \cdots + d^{n-1}a_1(d\alpha) + d^n a_0 = 0$$

Since $da_i \in k[x]$ for all i, $d\alpha$ is integral over $k[x]$. Thus $d\alpha := \beta \in O_K$, so $\alpha = \frac{\beta}{d}$. Hence K is the field of quotients of O_K as desired. □

Definition 2.1.5. Let R be an integral domain and F its field of fractions. R is said to be an *integrally closed domain* if for every $\alpha \in F$, if α is integral over R, then $\alpha \in R$.

In order to show that $k[x]$ is an integrally closed domain, we need the following theorem.

Theorem 2.1.6. *If R is a unique factorization domain, then R is an integrally closed domain.*

Proof. See [7]. □

Since k is a field, $k[x]$ is a Euclidean domain and so a unique factorization domain. By applying the previous theorem, we have

Corollary 2.1.7. *$k[x]$ is an integrally closed domain.*

2.2 Dedekind Domains

Definition 2.2.1. An integral domain D is called a *Dedekind domain* if and only if

(i) D is integrally closed,

(ii) D is Noetherian,

(iii) Every nonzero prime ideal of D is a maximal ideal.

The concept of Dedekind domain takes an important role in this thesis because we can uniquely write a nonzero proper ideal as a product of prime ideals (maximal ideals) as stated in the next theorem.

Theorem 2.2.2. ***(Unique Factorization of Ideal)***

Every nonzero proper ideal in a Dedekind domain D can be written uniquely as a product of prime ideals (maximal ideals).

Proof. See [2]. □

Next, we will show that $k[x]$ and O_K are Dedekind domains. We have already known that $k[x]$ is integrally closed, so we have to show that $k[x]$ is Noetherian and every nonzero prime ideal of $k[x]$ is a maximal ideal.

Theorem 2.2.3. *Every principal ideal domain is Noetherian.*

Proof. See [5]. □

Theorem 2.2.4. *A nonzero ideal in a principal ideal domain is maximal if and only if it is prime.*

Proof. See [5]. □

Since $k[x]$ is a principal ideal domain, by Theorem 2.2.3 and Theorem 2.2.4, $k[x]$ is a Dedekind domain as we desire. Finally, we have the following corollary.

Corollary 2.2.5. *$k[x]$ is a Dedekind domain.*

Similar to the number field case, O_K is also a Dedekind domain by the following theorem.

Theorem 2.2.6. *Let D be a Dedekind domain with the field of fractions F, and let L be a finite field extension of F. Then the integral closure of D in L is a Dedekind domain.*

Proof. See [3]. □

By Corollary 2.2.5, $k[x]$ is a Dedekind domain with the field of fractions $k(x)$ and K is a finite separable extension of $k(x)$, so we apply Theorem 2.2.6 to this fact. Hence O_K is a Dedekind domain as stated in the following corollary.

Corollary 2.2.7. *Let K be a function field over k. Then O_K is a Dedekind domain.*

Since the ideals of a Dedekind domain can be uniquely factorized as the product of its prime ideals, we can define the divisibility of ideals in a Dedekind domain as follows:

Definition 2.2.8. Let A and B be ideals in a Dedekind domain D. We say that *A divides B*, denoted by $A|B$, if there exists an ideal C such that $B = AC$.

Moreover, we have an easier method to determine the divisibility of ideals in the following proposition.

Proposition 2.2.9. *Let A and B be ideals in a Dedekind domain D. Then $A|B$ if and only if $B \subseteq A$.*

Proof. See [2]. □

Next, we will define the definition of lying over prime ideal and some of its property which we will use in Lemma 3.2.2.

Definition 2.2.10. Let R and A be rings such that $R \subseteq A$. If Q is a prime ideal of A, then $Q \cap R$ is a prime ideal of R. A prime ideal Q of A is said to *lie over* a prime ideal P of R in case $Q \cap R = P$.

Proposition 2.2.11. *If A is integral over R, then for each prime ideal P of R, there exists a prime ideal Q of A which lies over P.*

Proof. See [5]. □

2.3 Ideal Class Groups

Definition 2.3.1. Let D be a Dedekind domain and F its field of fractions. A *fractional ideal* of D is the set of the form αI, for some $\alpha \in F - \{0\}$ and some ideal I of D.

Note that every ordinary ideal of a Dedekind domain D is a fractional ideal of D. From now on, we use D_0 as the group of all nonzero principal fractional ideals of O_K and D_1 as the group of nonzero fractional ideals of O_K.

Definition 2.3.2. The quotient group $Cl(K) = D_1/D_0$ is called the *class group* of K. The order of $Cl(K)$ is denoted by h_K and is called the *class number* of K.

Next, we will provide the definition of valuations, places, product formula and global fields.

Definition 2.3.3. Let F be a field. A *valuation* on F is a real-valued function on F $|\cdot|$ satisfying

(i) $|x| \geq 0$, with equality if and only if $x = 0$,

(ii) $|x + y| \leq |x| + |y|$,

(iii) $|xy| = |x||y|$.

Definition 2.3.4. Two valuations $|\cdot|_1$ and $|\cdot|_2$ on a field F are said to be *equivalent* if and only if they give the same topology on F. An equivalence class of valuations on F is called a *place* on F.

Theorem 2.3.5. *Let F be a field. Let $|\cdot|_1$ and $|\cdot|_2$ be valuations on F. Then the following conditions are equivalent:*

(i) *$|\cdot|_1$ is equivalent to $|\cdot|_2$,*

(ii) *if $|a|_1 < 1$, then $|a|_2 < 1$ for all $a \in F$,*

(iii) *if $|a|_1 > 1$, then $|a|_2 > 1$ for all $a \in F$,*

(iv) *$|a|_1 = |a|_2^{\gamma}$ for some positive real γ and all $a \in F$.*

Proof. See [6]. □

Definition 2.3.6. A set S of places on F is said to satisfy a *product formula* if for any $a \in F^{\times}$, $|a|_P = 1$ for almost all $P \in S$ and $\prod_{P \in S} |a|_P = 1$.
(Here $|\cdot|_P$ is a valuation in a place P.)

Definition 2.3.7. A *global field* is a field with a set of places satisfying a product formula.

Let $p' \in k[x]$ be an irreducible polynomial, $\delta_{p'}$ the degree of p' and $a \in k(x) - \{0\}$. Then we can write $a = \prod_p p^{\upsilon_p(a)}$ where $\upsilon_p(a) \in \mathbb{Z}$. There are finitely many irreducible polynomials $p'' \in k[x]$ such that $\upsilon_{p''}(a) \neq 0$. We define the p'-adic valuation $|\cdot|_{p'}$ on $k(x)$ by

$$|a|_{p'} = q^{-\delta_{p'}\upsilon_{p'}(a)} \quad \text{and} \quad |0|_{p'} = 0.$$

Moreover, the equivalence class of $|\cdot|_{p'}$ is denoted by $P_{p'}$. In addition, we define a valuation $|\cdot|_\infty$ on $k(x)$ by

$$|a|_\infty = q^{\sum_p \delta_p \upsilon_p(a)} \qquad \text{and} \qquad |0|_\infty = 0.$$

Similarly, the equivalence class of $|\cdot|_\infty$ is denoted by ∞.

Theorem 2.3.8. *The set $S := \{P_p | p \in k[x]$ is a monic irreducible polynomial$\} \cup \{\infty\}$ is a set of places on $k(x)$.*

Proof. We have to prove that if p', p'' are distinct monic irreducible polynomials, then $|\cdot|_{p'}$ and $|\cdot|_{p''}$ are inequivalent. First, we consider

$$|p'|_{p'} = q^{-\delta_{p'}} < 1 \quad \text{and} \quad |p'|_{p''} = q^{-\delta_{p''}0} = q^0 = 1.$$

By Theorem 2.3.5, $|\cdot|_{p'}$ is not equivalent to $|\cdot|_{p''}$. On the other hand, we have

$$|p'|_{p'} = q^{-\delta_{p'}} < 1 \quad \text{and} \quad |p'|_\infty = q^{\delta_{p'}} > 1.$$

By Theorem 2.3.5, $|\cdot|_{p'}$ is not equivalent to $|\cdot|_\infty$. Hence the set

$$S := \{P_p | p \in k[x] \text{ is a monic irreducible polynomial}\} \cup \{\infty\}$$

is a set of places on $k(x)$ as desired. □

Theorem 2.3.9. *$k(x)$ is a global field.*

Proof. We claim that $k(x)$ together with the set of places

$$S := \{P_p | p \in k[x] \text{ is a monic irreducible polynomial}\} \cup \{\infty\}$$

satisfy a product formula. Let $a \in k(x) - \{0\}$. Then there are finitely many monic irreducible polynomials $p' \in k[x]$ such that $\upsilon_{p'}(a) \neq 0$. Hence $\upsilon_{p''}(a) = 0$ and so

$|a|_{p''} = q^{\upsilon_{p''}(a)} = q^0 = 1$ for almost all monic irreducible polynomials $p'' \in k[x]$. Consequently, $|a|_P = 1$ for almost all $P \in S$. Moreover

$$\begin{aligned}\prod_{P\in S} |a|_P &= (\prod_p |a|_p) \cdot |a|_\infty \\ &= q^{-\sum_p \delta_p \upsilon_p(a)} \cdot q^{\sum_p \delta_p \upsilon_p(a)} \\ &= q^{-\sum_p \delta_p \upsilon_p(a) + \sum_p \delta_p \upsilon_p(a)} \\ &= q^0 \\ &= 1.\end{aligned}$$

Hence $k(x)$ is a global field. □

Additionally, K is a global field due to the following theorem.

Theorem 2.3.10. *Any separable extension of a global field is again a global field.*

Proof. See [6]. □

Corollary 2.3.11. *K is a global field.*

Finally, the class number of K is finite as the consequence of the following theorem.

Theorem 2.3.12. *The ideal class group of any global field is finite.*

Proof. See [6]. □

CHAPTER III

GAUSS' LEMMA FOR FUNCTION FIELDS

3.1 Differences between $\mathbb{Z}$ and O_K

In this section, we would like to find out the difference between $\mathbb{Z}$ and O_K. By the fundamental theorem of arithmetic $\mathbb{Z}$ is a unique factorization domain. Unfortunately O_K may not be a unique factorization domain. First, we need to show five theorems in order to give an example that O_K may not be a UFD.

Theorem 3.1.1. *Let $f(y)$ be a monic polynomial in $k[x][y]$. Suppose that $f(y) = g(y)h(y)$ where $g(y)$ and $h(y)$ are monic polynomials in $k(x)[y]$. Then $g(y), h(y) \in k[x][y]$.*

Proof. Let $f(y)$ be a monic polynomial in $k[x][y]$. Suppose that $f(y) = g(y)h(y)$ where $g(y)$ and $h(y)$ are monic polynomials in $k(x)[y]$. Let m, n be monic polynomials in $k[x]$ of smallest degree such that $mg(y), nh(y) \in k[x][y]$. Thus the greatest common divisor of coefficients of $mg(y)$ and $nh(y)$ are in $k[x]$. Next, we claim that $mn \in k - \{0\}$. Assume that $mn \notin k - \{0\}$. Then $mn = 0$ or $deg(mn) \geq 1$. Since $k[x]$ is an integral domain and $m, n \neq 0$, $mn \neq 0$ and so $deg(mn) \geq 1$. Let r be an irreducible polynomial in $k[x]$ such that $r|mn$. Since r is irreducible, $k[x]/(r(x))$ is an integral domain, and so is $(k[x]/(r(x)))[y]$. By considering the equation

$$(mg(y))(nh(y)) = mnf(y)$$

in $(k[x]/(r(x)))[y]$, we have

$$(\overline{mg(y)})(\overline{nh(y)}) = \overline{mnf(y)} = \overline{0}.$$

Because $(k[x]/(r(x)))[y]$ is an integral domain, $\overline{mg(y)} = \overline{0}$ or $\overline{nh(y)} = \overline{0}$. Without loss of generality, suppose that $\overline{mg(y)} = \overline{0}$. Then r divides the greatest common divisor of coefficients of $mg(y)$, a contradiction. Consequently, $mn \in k - \{0\}$ as we claim. Hence $m, n \in k - \{0\}$, so $g(y), h(y) \in k[x][y]$ as desired. □

Theorem 3.1.2. *Let $\alpha \in k(x)$ be integral over $k[x]$ and $f(y)$ the monic polynomial in $k[x][y]$ of least degree having α as a root. Then $f(y)$ is irreducible over $k(x)$.*

Proof. Let $\alpha \in k(x)$ be integral over $k[x]$ and $f(y)$ the monic polynomial in $k[x][y]$ of least degree having α as a root. Assume that $f(y) = g(y)h(y)$ where $g(y)$ and $h(y)$ are monic nonconstant polynomials in $k(x)[y]$. By Theorem 3.1.1, $g(y), h(y) \in k[x][y]$. Since $0 = f(\alpha) = g(\alpha)h(\alpha)$, $g(\alpha) = 0$ or $h(\alpha) = 0$. Furthermore, $deg(g(y)), deg(h(y)) < deg(f(y))$, this contradicts to the minimality of $deg(f(y))$. Hence $f(y)$ is irreducible over $k(x)$. □

Theorem 3.1.3. *Let k be a finite field of characteristic $p \neq 2$ and x a transcendental element. Let $f(x) \in k[x]$ be squarefree. Then $K = k(x, \sqrt{f(x)})$ is a function field over k. Moreover $O_K = k[x, \sqrt{f(x)}]$.*

Proof. Let k be a finite field of characteristic $p \neq 2$ and x a transcendental element. Let $f(x) \in k[x]$ be squarefree and $K = k(x, \sqrt{f(x)})$. Initially, we will show that K is a function field over k. It is obvious that K is a finite extension of $k(x)$, and so an algebraic extension of $k(x)$. Since $char(k) = p \neq 2$, $\sqrt{f(x)} \neq -\sqrt{f(x)}$. So the minimal polynomial of $\sqrt{f(x)}$ over $k(x)$ is $y^2 - f(x)$ and has two distinct roots. Hence K is a separable extension of $k(x)$. Eventually, K is a function field over k.

In addition, we claim that $O_K = k[x, \sqrt{f(x)}]$. First, we will show that $O_K \supseteq k[x, \sqrt{f(x)}]$. Let $\alpha \in k[x, \sqrt{f(x)}]$. Thus $\alpha = a(x)+b(x)\sqrt{f(x)}$ where $a(x), b(x) \in k[x]$. If $b(x) = 0$, then $\alpha = a(x) \in k[x] \subseteq O_K$. Assume that $b(x) \neq 0$. Then

$$\begin{aligned} g(y) &:= [y - (a(x) + b(x)\sqrt{f(x)})][y - (a(x) - b(x)\sqrt{f(x)})] \\ &= [(y - a(x)) - b(x)\sqrt{f(x)})][(y - a(x)) + b(x)\sqrt{f(x)})] \\ &= (y - a(x))^2 - b^2(x)f(x) \\ &= y^2 - 2a(x)y + [a^2(x) - b^2(x)f(x)]. \end{aligned}$$

Therefore $g(y) \in k[x][y]$ is a monic polynomial having α as a root. Hence $\alpha \in O_K$.

Next, we will show that $O_K \subseteq k[x, \sqrt{f(x)}]$. Let $\beta \in O_K \subseteq K$. Then $\beta = c(x) + d(x)\sqrt{f(x)}$ where $c(x), d(x) \in k(x)$. If $d(x) = 0$, then $\beta = c(x) \in k(x)$ and $\beta \in O_K$. Since $k[x]$ is an integrally closed domain, $\beta \in k[x] \subseteq k[x, \sqrt{f(x)}]$.
For $d(x) \neq 0$, we have

$$\begin{aligned} h(y) &:= [y - (c(x) + d(x)\sqrt{f(x)})][y - (c(x) - d(x)\sqrt{f(x)})] \\ &= [(y - c(x)) - d(x)\sqrt{f(x)})][(y - c(x)) + d(x)\sqrt{f(x)})] \\ &= (y - c(x))^2 - d^2(x)f(x) \\ &= y^2 - 2c(x)y + [c^2(x) - d^2(x)f(x)] \\ &\in k(x)[y] \end{aligned}$$

Therefore $h(y)$ is the minimal polynomial of β over $k(x)$. Consequently, the conjugates $\bar{\beta}$ of $\beta = c(x) + d(x)\sqrt{f(x)}$ are β itself and $\bar{\beta} = c(x) - d(x)\sqrt{f(x)}$. Thus

$$Tr(\beta) = \beta + \bar{\beta} = (c(x) + d(x)\sqrt{f(x)}) + (c(x) - d(x)\sqrt{f(x)}) = 2c(x) \in k[x].$$

Since the characteristic $p \neq 2$, $c(x) \in k[x]$. Moreover,

$$N(\beta) = \beta\bar{\beta} = (c(x) + d(x)\sqrt{f(x)})(c(x) - d(x)\sqrt{f(x)}) = c^2(x) - d^2(x)f(x) \in k[x].$$

Since $c(x) \in k[x]$, $c^2(x) \in k[x]$. Therefore $l(x) := d^2(x)f(x) \in k[x]$. We claim that $d(x) \in k[x]$. Since $d(x) \in k(x)$, we can write

$$d(x) = \frac{r(x)}{s(x)} \quad \text{where} \quad r(x), s(x) \in k[x], s(x) \neq 0 \ \text{ and } \ \gcd(r(x), s(x)) = 1.$$

Then

$$\begin{aligned} d^2(x)f(x) = \frac{r^2(x)}{s^2(x)}f(x) &= l(x), \text{so} \\ r^2(x)f(x) &= s^2(x)l(x). \end{aligned}$$

Thus $s^2(x)|r^2(x)f(x)$, Because $\gcd(r(x), s(x)) = 1$, $s^2(x)|f(x)$. Since $f(x)$ is squarefree, $s(x)$ must be a unit of $k[x]$, so $s(x) \in k - \{0\}$. Consequently, $d(x) = \frac{r(x)}{s(x)} \in k[x]$. Therefore $\beta = c(x) + d(x)\sqrt{f(x)} \in k[x, \sqrt{f(x)}]$. Hence $O_K = k[x, \sqrt{f(x)}]$ as desired. □

Theorem 3.1.4. *Let K be a function field over k. Then $u \in O_K$ is a unit if and only if $N(u) \in k - \{0\}$.*

Proof. Let K be a function field over k. Initially, we will prove the sufficient condition. Let $u \in O_K$ be a unit. Then there exists $v \in O_K$ such that $uv = 1$, so $N(u)N(v) = N(uv) = 1$. Since $u, v \in O_K$, $N(u), N(v) \in k[x]$, so are units in $k[x]$. Therefore $N(u), N(v) \in k - \{0\}$. To prove the necessary condition, let $u \in O_K$ be such that $N(u) \in k - \{0\}$. Then $(N(u))^{-1} \in k - \{0\}$ is integral over $k[x]$ Because $u \in O_K \subseteq K$, $u^{-1} \in K$. Let $u = u_1, u_2, \ldots, u_n$ be all conjugates of u for some $n \in \mathbb{N}$. Since $u \in O_K$, $u_2, \ldots, u_n$ are also integral over $k[x]$. Thus $u^{-1} = u_2 \ldots u_n (N(u))^{-1}$ is integral over $k[x]$. Therefore $u^{-1} \in O_K$. Hence u is a unit in O_K. □

Theorem 3.1.5. *Let K be a function field over k and $a, b \in O_K - \{0\}$. Then*

(i) if $a|b$ in O_K, then $N(a)|N(b)$ in $k[x]$,

(ii) if $N(a)$ is irreducible in $k[x]$, then a is irreducible in O_K,

(iii) if a and b are associate, then $N(a) = cN(b)$ where $c \in k - \{0\}$.

Proof. Let K be a function field over k and $a, b \in O_K - \{0\}$. To prove (i), suppose that $a|b$ in O_K. Then there exists $c \in O_K$ such that $b = ac$, so $N(b) = N(a)N(c)$. Since $a, b, c \in O_K$, $N(a), N(b), N(c) \in k[x]$ Thus $N(a)|N(b)$ in $k[x]$. In order to prove (ii), assume that $N(a)$ is irreducible in $k[x]$. Suppose that $a = bc$ for some $b, c \in O_K$. Then $N(a) = N(b)N(c)$ and $N(a), N(b), N(c) \in k[x]$ because $a, b, c \in O_K$. Since $N(a)$ is irreducible in $k[x]$, $N(b)$ or $N(c)$ is a unit in $k[x]$. Without loss of generality, suppose that $N(b)$ is a unit in $k[x]$, so $N(b) \in k - \{0\}$. By Theorem 3.1.4, b is a unit in O_K. Hence a is irreducible in O_K. Finally, to prove (iii), assume that a and b are associate. Then there exists a unit $u \in O_K$ such that $a = bu$, so $N(a) = N(b)N(u)$. By Theorem 3.1.4, $c := N(u) \in k - \{0\}$. Therefore $N(a) = cN(b)$ where $c \in k - \{0\}$. □

In the next example, we will illustrate that O_K may not be a unique factorization domain.

Example 3.1.6. Let $K = \mathbb{F}_3(x, \sqrt{2x^3 + x + 1})$ and $f(x) = 2x^3 + x + 1$. Then $f(0) = f(1) = f(2) = 1$, so $f(x)$ is irreducible and squarefree. By Theorem 3.1.3, K is a function field and $O_K = \mathbb{F}_3[x, \sqrt{2x^3 + x + 1}]$. Let $\alpha \in O_K = \mathbb{F}_3[x, \sqrt{2x^3 + x + 1}]$. Thus $\alpha = a(x) + b(x)\sqrt{2x^3 + x + 1}$ where $a(x), b(x) \in \mathbb{F}_3[x]$. Therefore the conjugates of $\alpha = a(x) + b(x)\sqrt{2x^3 + x + 1}$ is α itself and $\bar{\alpha} = a(x) - b(x)\sqrt{2x^3 + x + 1}$. Let $A := \mathbb{F}_3[x, \sqrt{2x^3 + x + 1}] - \mathbb{F}_3[x]$ and $\beta \in A$. Then

$\beta = c(x) + d(x)\sqrt{2x^3 + x + 1}$ where $c(x), d(x) \in \mathbb{F}_3[x]$ and $d(x) \neq 0$. Therefore

$$\begin{aligned} N(\beta) = \beta\bar{\beta} =& (c(x) + d(x)\sqrt{2x^3 + x + 1})(c(x) - d(x)\sqrt{2x^3 + x + 1}) \\ =& c^2(x) - d^2(x)(2x^3 + x + 1) \\ =& c^2(x) + 2d^2(x)(2x^3 + x + 1) \\ =& c^2(x) + d^2(x)(x^3 + 2x + 2) \end{aligned}$$

Thus $c^2(x) = 0$ or $\deg(c^2(x)) = 2\deg(c(x))$ is even. On the other hand, $\deg(d^2(x)(x^3 + 2x + 2)) = 2\deg(d(x)) + 3 \geq 3$ is odd. Thus $\deg(c^2(x)) \neq \deg(d^2(x)(x^3 + 2x + 2))$. Consequently, $\deg(N(\beta)) = \deg(c^2(x) + d^2(x)(x^3 + 2x + 2))$ cannot be reduced by the characteristic 3 of $\mathbb{F}_3$ and $\deg(N(\beta)) \geq 3$. Additionally, if we let $\delta \in \mathbb{F}_3[x]$, then $\delta = h(x) \in \mathbb{F}_3[x]$ and $N(\delta) = h^2(x)$.

To show that O_K is not a unique factorization domain, we choose $\gamma = (x + 2) + \sqrt{2x^3 + x + 1}$. Then

$$\begin{aligned} \gamma\bar{\gamma} = N(\gamma) &= [(x + 2) + \sqrt{2x^3 + x + 1}][(x + 2) - \sqrt{2x^3 + x + 1}] \\ &= (x + 2)^2 + 2(2x^3 + x + 1) \\ &= (x^2 + 4x + 4) + (x^3 + 2x + 2) \\ &= x^3 + x^2 \\ &= x \cdot x \cdot (x + 1) \end{aligned}$$

Thus $N(\gamma) = N(\bar{\gamma}) = x^3 + x^2$, $N(x) = x^2$ and $N(x + 1) = (x + 1)^2$. By Theorem 3.1.5 (iii), γ is not associate to either x or $x + 1$. Similarly, $\bar{\gamma}$ is not associate to either x or $x + 1$.

Next, we will illustrate that $x, x+1, \gamma$ and $\bar{\gamma}$ are irreducible in O_K. First, it is obvious that there is no element in $\mathbb{F}_3[x]$ has norm either x or $x+1$. Moreover, there is no element in A has norm either x or $x + 1$ since $\deg(x) = \deg(x + 1) = 1 < 3$. By Theorem 3.1.4 and Theorem 3.1.5 (i), x and $x+1$ are irreducible in O_K. For γ

and $\bar{\gamma}$, similar to the previous case, there is no element in O_K has norm $x(x+1)$. In addition, there is no element in A has norm x^2 since $\deg(x^2) = 2 < 3$. It is easy to see that the elements in O_K of norm x^2 must be x and $2x$. With out loss of generality, suppose that x divides γ. Then there exists $\lambda \in O_K$ such that $\gamma = x\lambda$. Since $\lambda \in O_K = \mathbb{F}_3[x]$,we can write λ as $r(x) + s(x)\sqrt{2x^3 + x + 1}$ where $r(x), s(x) \in \mathbb{F}_3[x]$. Furthermore,

$$\begin{aligned}(x+2) + \sqrt{2x^3 + x + 1} &= \gamma \\ &= x\lambda \\ &= x(r(x) + s(x)\sqrt{2x^3 + x + 1}) \\ &= xr(x) + xs(x)\sqrt{2x^3 + x + 1}.\end{aligned}$$

Therefore $xs(x) = 1$, but $\deg(xs(x)) = \deg(x) + \deg(s(x)) \geq 1$ and $\deg(1) = 0$, a contradiction. Consequently, x does not divide γ and so x does not divide $\bar{\gamma}$. Hence there is no element in O_K of norm $x, x+1, x(x+1)$. Moreover, x and $2x$ which are the elements in O_K of norm x^2 do not divide either γ or $\bar{\gamma}$. By Theorem 3.1.4 and Theorem 3.1.5 (i), γ and $\bar{\gamma}$ are irreducible in O_K. Finally, O_K is not a unique factorization domain.

3.2 Gauss' Lemma

We have already known that the content of a polynomial in $\mathbb{Z}[y]$ is the great common divisor of its coefficients. Initially, we would like to define the content of a polynomial in $O_K[y]$, but O_K may not be a unique factorization domain as we illustrate in the previous section. Therefore the great common divisor of elements in O_K may not exist. Eventually, we will give the definition of content as follows:

Definition 3.2.1. For a polynomial $f(y) \in O_K[y]$, the *content* of $f(y)$ in K, denoted by $cont_K(f)$, is the ideal of O_K generated by the coefficients of $f(y)$. The

polynomial $f(y)$ is *primitive* in K if $cont_K(f) = O_K$.

As we see in the previous definition, if we replace O_K by $\mathbb{Z}$ and K by $\mathbb{Q}$, the content of a polynomial in $\mathbb{Z}[y]$ is the ideal of $\mathbb{Z}$ generated by its coefficients. In the different point of view, it is the ideal of $\mathbb{Z}$ generated by the great common divisor of its coefficients because $\mathbb{Z}$ is a principal ideal domain. On the other hand, a polynomial in $\mathbb{Z}[y]$ is primitive if its content is $\mathbb{Z}$,which is the ideal of $\mathbb{Z}$ generated by 1. Hence the Definition 3.2.1 is a generalization of the definition of content.

The content of a polynomial clearly depends on K because it is an ideal of O_K. By applying Theorem 2.2.2 to O_K which is a Dedekind domain, it is shown that the property of being primitive does not depend on specific K.

Lemma 3.2.2. ***(Independence of Primitivity)***

Let K and K' be function fields over the same finite field k. Let $f(y) \in O_K[y], O_{K'}[y]$. Then $f(y)$ is primitive in K if and only if it is primitive in K'.

Proof. Let K and K' be function fields over k. Let L be the smallest field containing both K and K'. Then $f(y) \in O_L[y]$. Without loss of generality, we consider the field $K \subseteq L$. Claim that $f(y)$ is primitive in K if and only if it is primitive in L. In order to prove the necessary condition, suppose that $f(y) := a_n y^n + \cdots + a_1 y + a_0$ is not primitive in K. Then $cont_K(f) \neq O_K$. By Theorem 2.2.2, $cont_K(f) = P_1 P_2 \dots P_m$ where $m \in \mathbb{N}$ and P_j are prime ideals of O_K for all j. Thus $a_i \in cont_K(f) = P_1 P_2 \dots P_m \subseteq P_1$ for all i. Let Q_1 be a prime ideal in O_L lying over P_1. Hence $Q_1 \cap O_K = P_1$, so $a_i \in Q_1$ for all i. Therefore $cont_L(f) \subseteq Q_1 \subset O_L$. Finally, $f(y)$ is not primitive in L.

On the other hand, suppose that $f(y) := a_n y^n + \cdots + a_1 y + a_0$ is not primitive in L. Then $cont_L(f) \neq O_L$. Similar to the necessary condition, there exists a prime ideal Q_2 of O_L such that $a_i \in Q_2$ for all i. Let $P_2 := Q_2 \cap O_K$. Therefore

P_2 is a prime ideal of O_K Since $f(y) \in O_K[y]$, $a_i \in O_K$ for all i, so $a_i \in P_2$ for all i. Thus $cont_K(f) \subseteq P_2 \subset O_K$. Hence $f(y)$ is not primitive in K.

Therefore $f(y)$ is primitive in K if and only if it is primitive in L. Similarly, we have $f(y)$ is primitive in K' if and only if it is primitive in L. Hence $f(y)$ is primitive in K if and only if it is primitive in K' as desired. □

Gauss' lemma is stated that the product of two primitive polynomials is also primitive. This lemma remains true by the definition of content in Definition 3.2.1. Hence we acquire the next important theorem, Gauss' lemma for function fields.

Theorem 3.2.3. ***(Gauss' Lemma for Function Fields)***

The product of two primitive polynomials is primitive.

Proof. Let K be a function field over k, $f(y), g(y) \in O_K[y]$ be primitive polynomials. Write

$$f(y) := \sum_{i=0}^{n} a_i y^i, \quad g(y) := \sum_{j=0}^{m} b_j y^j \quad \text{and} \quad f(y)g(y) := h(y) := \sum_{l=0}^{r} c_l y^l$$

Let P be a prime ideal in O_K. If $a_i \in P$ for all i, then $cont_K(f) \subseteq P \subset O_K$, so $f(y)$ is not primitive, a contradiction. Then there exists the smallest $i_0 \in \{0, 1, \ldots, n\}$ such that $a_{i_0} \notin P$ and the smallest $j_0 \in \{0, 1, \ldots, m\}$ such that $b_{j_0} \notin P$. Consider

$$\begin{aligned} c_{i_0+j_0} = a_0 b_{i_0+j_0} + \cdots + a_{i_0-1} b_{j_0+1} \\ + a_{i_0} b_{j_0} \\ + a_{i_0+1} b_{j_0-1} + \cdots + a_{i_0+j_0} b_0. \end{aligned}$$

Since $a_0, \ldots, a_{i_0-1} \in P$, $a_0 b_{i_0+j_0} + \cdots + a_{i_0-1} b_{j_0+1} \in P$. And because $b_0, \ldots, b_{j_0-1} \in P$, $a_{i_0+1} b_{j_0-1} + \cdots + a_{i_0+j_0} b_0 \in P$. Assume that $a_{i_0} b_{i_0} \in P$. Since P is a prime ideal, $a_{i_0} \in P$ or $b_{i_0} \in P$, a contradiction. Thus $a_{i_0} b_{i_0} \notin P$, so $c_{i_0+j_0} \notin P$. Therefore we

have for every prime ideal P of O_K, there exists a coefficient c_P of $h(y)$ such that $c_P \notin P$. Because P is arbitrary, $cont_K(h) = O_K$. Hence $h(y)$ is primitive. □

3.3 Complete Factorization

In section 3.1, we have already shown that O_K may not be a unique factorization domain. Therefore O_K may not be a principal ideal domain since every principal ideal domain is a unique factorization domain. Let A be an ideal in O_K. Although A may not be principal, there exists a finite extension L of K such that AO_L is principal by using Theorem 2.3.12 to obtain the following lemma.

Lemma 3.3.1. ***(Extending to a Principal Ideal)***

Let K be a function field over k, and A be an ideal of O_K. Then there exists $r \in \mathbb{N}$ such that A^r is principal. In particular, there exists a finite extension L of K such that AO_L is principal.

Proof. By Theorem 2.3.12, the ideal class number of K is finite, says $r \in \mathbb{N}$. Then $A^r \in D_0$, so $A^r = (a)$ for some $a \in K$. Take $L = K(a^{1/r})$ where $a^{1/r}$ is a fixed r^{th} root of a. Therefore

$$(a^{1/r})^r = (a) = A^r O_L = (AO_L)^r.$$

Moreover, it is clear that L is a finite extension of K. Since K is a finite extension of $k(x)$, L is also a finite extension of $k(x)$. By Corollary 2.2.6, O_L is a Dedekind domain. Hence, by Theorem 2.2.2, $AO_L = (a^{1/r})$. □

There is a theorem stated that every nonzero polynomial $f(y) \in \mathbb{Q}[y]$ can be written in the form $f(y) = c_f f^*(y)$ where $c_f \in \mathbb{Q}$ and $f^*(y) \in \mathbb{Z}[y]$ is primitive. Furthermore c_f and $f^*(y)$ are unique up to multiplication by units in $\mathbb{Z}$. We would like to apply this theorem to K. Unfortunately it does not work in the function

field case because O_K may not be a principal ideal domain. Hence we have to apply Lemma 3.3.1 in order to obtain the next theorem.

Theorem 3.3.2. ***(Factoring Out the Content in Function Fields)***

Let K be a function field over k, and $f(y) \in K[y]$. Then there exists a finite extension L of K such that

$$f(y) = c_f f^*(y)$$

where $c_f \in L$ and $f^*(y) \in O_L[y]$ is a primitive polynomial. Moreover c_f and $f^*(y)$ are unique up to multiplication by units in O_L.

Proof. Let K be a function field over k, and $f(y) \in K[y]$. Then $f(y) := a_n y^n + \cdots + a_1 y + a_0$ for some $n \in \mathbb{N}$ and $a_i \in K$ for all i. By Theorem 2.1.4, for each i, $a_i = \frac{b_i}{c_i}$ where $b_i, c_i \in O_K$. Thus $f(y) := \frac{b_n}{c_n} y^n + \cdots + \frac{b_1}{c_1} y + \frac{b_0}{c_0}$.
By multiplying $c_n \dots c_1 c_0$ to both sides of the previous equation, we have

$$g(y) := (c_n \dots c_1 c_0) f(y) = (c_{n-1} \dots c_1 c_0) b_n y^n + \dots (c_n \dots c_2 c_0) b_1 y + (c_n \dots c_2 c_1) b_0.$$

It is easy to see that $g(y) \in O_K[y]$. Therefore $cont_K(g)$ is an ideal of O_K. By Theorem 3.3.1, there exists a finite extension L of K such that $cont_K(g) O_L = cont_L(g)$ is principal. Thus $cont_L(g) = (d)$ for some $d \in O_L$. By considering $g(y) \in O_K[y] \subseteq O_L[y]$, $g(y) = d \cdot g^*(y)$ where $g^*(y) \in O_L[y]$ is a primitive polynomial, so we have

$$\begin{aligned}(c_n \dots c_1 c_0) f(y) =& g(y) = d \cdot g^*(y).\\ f(y) =& \frac{d}{c_n \dots c_1 c_0} \cdot g^*(y).\end{aligned}$$

Since $d \in O_L \subseteq L$ and $c_n, \dots, c_1, c_0 \in O_K \subseteq K \subseteq L$, $\frac{d}{c_n \dots c_1 c_0} \in L$. Let $c_f = \frac{d}{c_n \dots c_1 c_0}$ and $f^*(y) = g^*(y)$. Hence $f(y) = \frac{d}{c_n \dots c_1 c_0} \cdot g^*(y) = c_f f^*(y)$ as desired. In order to prove the uniqueness up to multiplication by units in O_L, assume that $f(y) = c_f f^*(y) = c_g g^*(y)$ where $c_f, c_g \in L$ and $f^*(y), g^*(y) \in O_L[y]$ are primitive

polynomials. Then $f^*(y) = \frac{c_g}{c_f} \cdot g^*(y) =: c \cdot g^*(y)$ where $c = \frac{c_g}{c_f} \in L$. By Theorem 2.1.4, $c = \frac{u}{v}$ where $u, v \in O_L$ are relatively prime. Hence $v \cdot f^*(y) = u \cdot g^*(y)$. Since $f^*(y), g^*(y)$ are primitive, $(v) = (v)O_L = (v)cont_L(f^*) = (u)cont_L(g^*) = (u)O_L = (u)$. Therefore u and v are associate, so there exists a unit $c' \in O_L$ such that $u = c'v$. Consequently, $c = \frac{u}{v} = c'$ is a unit in O_L. Eventually, $c_f = c^{-1}c_g$ and $f^*(y) = c \cdot g^*(y)$, that is c_f and $f^*(y)$ are unique up to multiplication by units in O_L. □

For a polynomial $f(y) \in \mathbb{Z}[y]$, if $f(y) = g(y)h(y)$ for polynomials $g(y), h(y) \in \mathbb{Q}[y]$, then $f(y) = G(y)H(y)$ where $G(y), H(y) \in \mathbb{Z}[y]$. We also have this theorem in the function fields version by relying on Theorem 3.2.3 together with Theorem 3.3.2, so we acquire the following theorem as a consequence.

Theorem 3.3.3. ***(Lifting a Factorization)***

Let K be a function field over k and $f(y) \in O_K[y]$. If

$$f(y) = g(y)h(y)$$

for polynomials $g(y), h(y) \in K[y]$, then there exists a finite extension L of K such that

$$f(y) = G(y)H(y)$$

where $G(y), H(y) \in O_L[y]$, $G(y)$ and $H(y)$ are L-multiples of $g(y)$ and $h(y)$, respectively.

Proof. Let K be a function field over k and $f(y) \in O_K[y]$. Suppose that $f(y) = g(y)h(y)$ for polynomials $g(y), h(y) \in K[y]$. By Theorem 3.3.2, there exist finite extensions L_g and L_h of K such that

$$g(y) = c_g g^*(y) \quad \text{and} \quad h(y) = c_h h^*(y)$$

where $c_g \in L_g$, $c_h \in L_h$, $g^*(y) \in O_{L_g}[y]$ and $h^*(y) \in O_{L_h}[y]$ are primitive polynomials. Since $f(y) \in O_K[y]$, $cont_K(f)$ is an ideal of O_K. By Theorem 3.3.1, there exists a finite extension L_f of K such that $cont_K(f)O_{L_f} = cont_{L_f}(f)$ is principal. Then there exists $c_f \in O_{L_f}$ such that $cont_{L_f}(f) = (c_f)$. By considering $f(y) \in O_K[y] \subseteq O_{L_f}[y], f(y) = c_f f^*(y)$ where $f^*(y) \in O_{L_f}[y]$ is a primitive polynomial. Let L be smallest field containing L_f, L_g and L_h. Since L_f, L_g and L_h are finite extensions of K, L is also a finite extension of K. Hence we have a finite extension L of K such that

$$f(y) = c_f f^*(y), \quad g(y) = c_g g^*(y) \quad \text{and} \quad h(y) = c_h h^*(y)$$

where $c_f \in O_L$, $c_g, c_h \in L$ and $f^*(y), g^*(y), h^*(y) \in O_L[y]$ are primitive polynomials. Thus

$$c_f f^*(y) = f(y) = g(y)h(y) = (c_g c_h)g^*(y)h^*(y)$$

By Theorem 3.2.3, $g^*(y)h^*(y)$ is a primitive polynomial. By the uniqueness part of Theorem 3.3.2, $c_f = uc_g c_h$ for some unit $u \in O_L$. Because $u, c_f \in O_L$, $c_g c_h = u^{-1}c_f \in O_L$. Let $G(y) = c_g c_h g^*(y)$ and $H(y) = h^*(y)$. Since $c_g c_h \in O_L$ and $g^*(y), h^*(y) \in O_L[y]$, $G(y), H(y) \in O_L[y]$. In addition,

$$G(y) = c_h g(y), \quad H(y) = {c_h}^{-1}h(y) \quad \text{and} \quad f(y) = G(y)H(y),$$

that is $G(y)$ is an L-multiple of $g(y)$, and $H(y)$ is an L-multiple of $h(y)$. □

Additionally, we have the Complete Factorization resulting from Theorem 3.3.3 as the next corollary.

Corollary 3.3.4. ***(Complete Factorization)***

Let K be a function field over k and $f(y) \in O_K[y]$. Then there exists a finite extension L of K such that $f(y)$ can be factored into a product of (not necessarily monic) linear factors in $O_L[y]$.

Proof. Let K be a function field over k and $f(y) \in O_K[y] \subseteq K[y]$. Let K' be a splitting field over K of $f(y)$. Then it is obvious that K' is a finite extension over K. Thus $f(y) \in O_K[y] \subseteq O_{K'}[y]$ and $f(y)$ splits over K'. By Theorem 3.3.3, there exists a finite extension L of K' such that $f(y)$ can be factored into a product of (not necessarily monic) linear factors in $O_L[y]$. Since K' is a finite extension over K, L is also a finite extension over K. Consequently, there exists a finite extension L of K such that $f(y)$ can be factored into a product of (not necessarily monic) linear factors in $O_L[y]$ as desired. □

Furthermore, we have another corollary by specializing to polynomials which have coefficients in k.

Corollary 3.3.5. *Let $f(y) \in k[x][y]$. Then there exists a finite extension L of $k(x)$ such that $f(y)$ can be factored into a product of (not necessarily monic) linear factors in $O_L[y]$.*

Proof. Let $f(y) \in k[x][y]$. Then we have a function field $L = k(x)$, $O_L = k[x]$ and $f(y) \in k[x][y] \subseteq O_L[y]$. By Corollary 3.3.4, there exists a finite extension K of L such that $f(y)$ can be factored into a product of (not necessarily monic) linear factors in $O_K[y]$. □

Finally, we will illustrate an example of Corollary 3.3.5 as follows:

Example 3.3.6. Let x be a transcendental element and $f(y) = 3xy^2 + xy + (x^2 + 1) \in \mathbb{F}_5[x][y]$. Then the roots of f are

$$\begin{aligned} y =& \frac{-x \pm \sqrt{x^2 - 4(3x)(x^2+1)}}{2(3x)} \\ =& \frac{4x \pm \sqrt{x^2 + (3x)(x^2+1)}}{x} \\ =& \frac{4x \pm \sqrt{3x^3 + x^2 + 3x}}{x} \end{aligned}$$

$$=\frac{4x \pm \sqrt{(x+1)^2(3x)}}{x}$$
$$=\frac{4x \pm (x+1)\sqrt{3x}}{x}$$

Therefore we have $y = \frac{4x+(x+1)\sqrt{3x}}{x}, \frac{4x-(x+1)\sqrt{3x}}{x} = \frac{4x+4(x+1)\sqrt{3x}}{x}$. Consequently,

$$\begin{aligned} f(y) =& 3xy^2 + xy + (x^2+1) \\ =& 3x(y - \frac{4x+(x+1)\sqrt{3x}}{x})(y - \frac{4x+4(x+1)\sqrt{3x}}{x}) \\ =& 3x(y + 4\frac{4x+(x+1)\sqrt{3x}}{x})(y + 4\frac{4x+4(x+1)\sqrt{3x}}{x}) \\ =& 3x(y + \frac{x+4(x+1)\sqrt{3x}}{x})(y + \frac{x+(x+1)\sqrt{3x}}{x}) \end{aligned}$$

Let $g(y) := y + \frac{x+4(x+1)\sqrt{3x}}{x}$ and $h(y) := y + \frac{x+(x+1)\sqrt{3x}}{x}$. Thus $f(y) = 3xg(y)h(y)$ and f splits over $K = \mathbb{F}_5(x, \sqrt{3x})$. Since $3x$ is squarefree, by Theorem 3.1.3, K is a function field and $O_K = \mathbb{F}_5[x, \sqrt{3x}]$. Furthermore, we let

$$g'(y) := xg(y) = xy + x + 4(x+1)\sqrt{3x} \quad \text{and} \quad h'(y) := xh(y) = xy + x + (x+1)\sqrt{3x}.$$

Thus $g'(y), h'(y) \in \mathbb{F}_5[x, \sqrt{3x}][y] = O_K[y]$. Next, we consider

$$cont_K(g') = (x, x + 4(x+1)\sqrt{3x}) \quad \text{and} \quad cont_K(h') = (x, x + (x+1)\sqrt{3x}).$$

Initially, we have

$$\begin{aligned} cont_K^2(g') =& (x, x + 4(x+1)\sqrt{3x})^2 \\ =& (x^2, x^2 + (4x^2+4x)\sqrt{3x}, (3x^3+2x^2+3x) + (3x^2+3x)\sqrt{3x}) \\ =& (x^2, x(x + (4x+4)\sqrt{3x}), x((3x^2+2x+3) + (3x+3)\sqrt{3x})) \end{aligned}$$

Then $cont_K^2(g') \subseteq (x)$. Moreover,

$$(x^2+x)\sqrt{3x} = 4[(x^2 + (4x^2+4x)\sqrt{3x}) - x^2] \in cont_K^2(g'),$$

also

$$x + (x^2+x)\sqrt{3x} = 2[((3x^3+2x^2+3x) + (3x^2+3x)\sqrt{3x}) - 3x(x^2) - 2(x^2)] \in cont_K^2(g').$$

Finally,

$$x = (x + (x^2 + x)\sqrt{3x}) - ((x^2 + x)\sqrt{3x}) \in cont_K^2(g').$$

Hence $cont_K^2(g') = (x)$. Next, we have

$$\begin{aligned} cont_K^2(h') =& (x, x + (x+1)\sqrt{3x})^2 \\ =& (x^2, x^2 + (x^2 + x)\sqrt{3x}, (3x^3 + 2x^2 + 3x) + (2x^2 + 2x)\sqrt{3x}) \\ =& (x^2, x(x + (x+1)\sqrt{3x}), x((3x^2 + 2x + 3) + (2x + 2)\sqrt{3x})) \end{aligned}$$

Thus $cont_K^2(h') \subseteq (x)$. Furthermore,

$$(x^2 + x)\sqrt{3x} = (x^2 + (x^2 + x)\sqrt{3x}) - x^2 \in cont_K^2(h'),$$

and

$$4x + (x^2 + x)\sqrt{3x} = 3[((3x^3 + 2x^2 + 3x) + (2x^2 + 2x)\sqrt{3x}) - 3x(x^2) - 2(x^2)] \in cont_K^2(h').$$

Therefore

$$4x = (4x + (x^2 + x)\sqrt{3x}) - ((x^2 + x)\sqrt{3x}) \in cont_K^2(h'),$$

so $x = 4 \cdot 4x \in cont_K^2(h')$. Eventually, $cont_K^2(h') = (x)$.

By the proof of Theorem 3.3.2, the content factored out from $g(y)$ and $h(y)$ is $\frac{\sqrt{x}}{x} = \frac{1}{\sqrt{x}}$ and we get $L = \mathbb{F}_5(x, \sqrt{3x}, \sqrt{x}) = \mathbb{F}_5(x, \sqrt{x}, \sqrt{3}) = \mathbb{F}_5(\sqrt{x}, \sqrt{3})$ a finite extension of $\mathbb{F}_5(x)$. Moreover,

$$\begin{aligned} g(y) =& y + \frac{x + 4(x+1)\sqrt{3x}}{x} \\ =& \frac{1}{\sqrt{x}}(\sqrt{x}y + \frac{x + 4(x+1)\sqrt{3x}}{\sqrt{x}}) \\ =& \frac{1}{\sqrt{x}}(\sqrt{x}y + \sqrt{x} + 4\sqrt{3}(x+1)), \end{aligned}$$

and

$$\begin{aligned} h(y) =& y + \frac{x + (x+1)\sqrt{3x}}{x} \\ =& \frac{1}{\sqrt{x}}(\sqrt{x}y + \frac{x + (x+1)\sqrt{3x}}{\sqrt{x}}) \\ =& \frac{1}{\sqrt{x}}(\sqrt{x}y + \sqrt{x} + \sqrt{3}(x+1)). \end{aligned}$$

Finally,

$$\begin{aligned} f(y) =& 3xg(y)h(y) \\ =& 3x(\frac{1}{\sqrt{x}}(\sqrt{x}y + \sqrt{x} + 4\sqrt{3}(x+1)))(\frac{1}{\sqrt{x}}(\sqrt{x}y + \sqrt{x} + \sqrt{3}(x+1))) \\ =& 3(\sqrt{x}y + \sqrt{x} + 4\sqrt{3}(x+1))(\sqrt{x}y + \sqrt{x} + \sqrt{3}(x+1)). \end{aligned}$$

Additionally, $\sqrt{x}$ is a root of $r(y) = y^2 + 4x \in \mathbb{F}_5[x][y]$ and $\sqrt{3}$ is a root of $s(y) = y^2 + 2 \in \mathbb{F}_5[x][y]$, so $\sqrt{x}, \sqrt{3} \in O_L$. Hence $f(y)$ can be factored into a product of linear factors in $O_L[y]$.

REFERENCES

[1] A. Magidin, D. McKinnon.(2005). Gauss's Lemma for Number Fields. *Amer. Math. Monthly, 112*, 385-416.

[2] D.A. Marcus.(1977). *Number Fields.* New York: Springer-Verlag.

[3] G.J. Janusz.(1996). *Algebraic Number Fields* (Second Edition). American Mathematical Society.

[4] H. Koch.(2000). *Number Theory: Algebraic Numbers and Functions.* American Mathematical Society.

[5] P.A. Grillet.(1999). *Algebra.* A Wiley-Interscience Publication.

[6] P.M. Cohn.(1991). *Algebraic Numbers and Algebraic Functions.* Padstow: T.J.Press.

[7] T.W. Hungerford.(1974). *Algebra.* Holt, Rinehart and Winston.

VITA

Name	Mr. Borworn Khuhirun
Date of Birth	21 September 1984
Place of Birth	Lopburi, Thailand
Education	B.Sc. (Mathematics) (First Class Honours), Chulalongkorn University, 2006
Scholarship	The Development and Promotion of Science and Technology Talents Project (DPST)