creative commons

COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

조선대학교
CHOSUN UNIVERSITY

[UCI]I804:24011-200000265880

2017년 2월
교육학석사(수학)학위논문

Hurwitz 다항식 환의 대수적 성질 연구

조선대학교 교육대학원

수학교육전공

정 학 진

조선대학교
CHOSUN UNIVERSITY

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

Hurwitz 다항식 환의 대수적 성질 연구

On the algebraic properties of Hurwitz's polynomial rings

2017년 2월

조선대학교 교육대학원

수학교육전공

정 학 진

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

Hurwitz 다항식 환의 대수적 성질 연구

지도교수 오 동 렬

이 논문을 교육학석사(수학교육)학위 청구논문으로 제출함.

2016년 10월

조선대학교 교육대학원

수학교육전공

정 학 진

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

정학진의 교육학 석사학위 논문을 인준함.

심사위원장 조선대학교 교수 안 영 준 인

심사위원 조선대학교 교수 김 진 홍 인

심사위원 조선대학교 교수 오 동 렬 인

2016년 12월

조선대학교 교육대학원

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

CONTENTS

ABSTRACT

1. 소 개 ····· 2

2. 다항식환 ····· 3

3. Hurwitz 다항식환 ····· 10

4. Hurwitz 다항식 기약판별법 ····· 16

참고문헌 ····· 20

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

ABSTRACT

On the algebraic properties of Hurwitz's polynomial rings

Jeong, Hak Jin
Advisor : Prof. Dong Yeol Oh Ph.D.
Major in Mathematics Education
Graduate School of Education, Chosun University

The formal power series rings and polynomial rings have been of interest and have had important applications in many areas including algebra and commutative ring theory. Keigher introduced a variant of the rings of formal power series rings and polynomial rings, and then called them Hurwitz power series rings and Hurwitz polynomial rings, respectively. Since then, many works on the ring of Hurwitz power series and polynomial rings have been done. In this thesis, we introduce a Hurwitz polynomial ring and study its basic algebraic properties. Moreover, we investigate the irreduciblilty of Hurwitz polynomials over the ring of integers and compare those with usual polynomials with integer coefficients.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

제 1 장

소 개

곱셈항등원을 갖는 가환환(commutative ring with unity) 상에서 계수를 갖는 형식적 멱급수환(formal power series ring)과 다항식환(polynomial ring)은 대수학 및 가환환 이론의 중요한 연구 대상 중 하나이며 많은 응용성을 갖고 있다. 형식적 멱급수환 및 다항식환에 대한 연구는 1950년대부터 많은 수학자들에 의하여 활발히 이루어졌으며, 특히 다항식환을 일반화한 반군환(semigroup ring)에 대한 연구도 1970년대 후반부터 활발히 이루어지고 있다. 반군환의 경우 다항식환의 차수에 대한 일반화이다. 반면 1976년 Keigher[4]에 의하여 변형된 멱급수환과 다항식환이 소개되었으며, 이후 [5] 이 변형된 멱급수환 및 다항식환을 Hurwitz 멱급수환 및 다항식환(Hurwitz power series ring, Hurwitz polynomial ring)이라 명명하였다. 1997년 이후 Hurwitz 멱급수환 및 다항식환에 대하여 기존의 형식적 멱급수환 및 다항식환의 성질과 비교 분석한 많은 연구들이 이루어졌다 [1],[2],[6]. Hurwitz 멱급수환과 다항식환은 두 멱급수 또는 두 다항식의 곱셈에서 계수에 특별한 무게(weight)를 주는 것으로 반군환과는 다른 관점으로 기존의 멱급수환과 다항식환을 일반화한 것이다.

이 논문에서는 Hurwitz 다항식환을 소개하고 기존의 다항식환에서의 성질이 Hurwitz 다항식환에서는 어떻게 나타나는지를 확인해 봄으로써 Hurwitz 다항식환의 성질을 분석하였다. 2장에서는 다항식환에 대한 잘 알려진 내용들을 복습하였다. 3장에서는 Hurwitz 다항식환을 소개하고 간단한 내용을 다룬다. 특히 정역, 유클리드정역에 대한 내용을 다루고 이항정리에 대해서도 언급하였다. 마지막으로 4장에서는 Hurwitz 다항식환과 기존의 다항식환에서의 기약 다항식에 대한 성질을 비교분석하였다. 구체적으로 정수 계수를 갖는 2차 및 3차 다항식이 기존의 다항식환에서 기약인지를 판별하는 잘 알려진 유용한 방법들이 있다. 이 들 방법들을 이용하여 정수 계수를 갖는 Hurwitz 다항식이 기약인지를 판별할 수 있는지 확인하였다. 또한 고차다항식의 경우 정수 계수를 갖는 Hurwitz 다항식이 기약임을 판별할 수 방법을 조사해보았다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

제 2 장

다항식환

이 장에서는 다항식환의 정의와 성질을 소개한다.
이 장의 내용은 [3], [7] 을 참고로 하여 요약정리 하였다. 다항식환의 대부분의 성질에 대한 증명은 잘 알려진 것으로 생략하기로 하며 3장과 4장에서 필요한 정리의 경우 그 증명을 간단하게 하도록 하겠다.

정의 2.1 집합 R $(\neq \phi)$에 덧셈과 곱셈으로 불리는 두 개의 이항연산 $+, \cdot$ 이 다음 공리를 만족하면 $< R, +, \cdot >$을 환$(ring)$ 이라고 부른다.

1. $< R, + >$는 아벨군*(abelian group)*
2. 임의의 $a, b, c \in R$에 대하여, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ 결합법칙*(associative law)*
3. 임의의 $a, b, c \in R$에 대하여 $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ 왼쪽분배법칙*(left distributive law)*, $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ 오른쪽분배법칙*(right distributive law)*

환 R의 임의의 원소 a, b에 대하여 $a \cdot b = b \cdot a$ 이면 R을 가환환*(commutative ring)*이라 한다.

참고 집합 $G(\neq \phi)$의 정의된 이항연산 $*$에 대하여 다음 성질을 만족하면 G는 아벨군(abelian group)이다.

1. 모든 $a, b, c \in G$에 대하여 $(a * b) * c = a * (b * c)$
2. 모든 $x \in G$에 대해서 $e * x = x * e = x$ 인 $e \in G$ 존재
3. G내의 원소 a에 대응하는 $a' * a = a * a' = e$ 인 $a' \in G$ 존재

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

4. 모든 $a, b \in G$ 에 대하여 $a * b = b * a$ 이다.

정의 2.2 환 R의 임의의 원소 a에 대하여 $a \cdot e = e \cdot a = a$ 을 만족하는 R의 원소 e가 이 존재하면 e를 R의 곱셈항등원 또는 단위원*(unity)*이라 하고 이때 R을 곱셈항등원을 갖는 환*(ring with identity)*라 한다.

환에서 덧셈항등원을 0으로 나타내고 곱셈항등원을 갖는 환의 경우 곱셈항등원을 1로 나타내도록 한다.

정의 2.3 곱셈항등원을 갖는 환 R의 원소 $u \in R$에 대하여 $u \cdot v = v \cdot u = 1$을 만족하는 R의 원소 v가 존재하면 u를 R의 단원 *(unit)* 또는 가역원*(invertible element)* 이라 하고 이 때 v를 u^{-1}로 나타낸다. 환 R 의 영이 아닌 모든 원소가 단원이면 R은 나눗셈환*(division ring)* 이라 한다. 또한 가환인 나눗셈환을 체*(field)*라 한다.

환 R의 원소 a, b 에 대하여 $b = a \cdot c$ 를 만족하는 원소 c가 존재하면 a를 b의 약수라고 하고 기호로 $a \mid b$로 나타낸다.

정의 2.4 곱셈항등원을 갖는 가환환에서 0의 약수가 0 밖에 없으면 이 환을 정역이라 한다.

참고 곱셈항등원을 갖는 가환환 R에 대하여 다음은 동치이다.

1. R은 정역이다.

2. 임의의 $a, b \in R$ 에 대하여, $ab = 0$ 이면 $a = 0$ 또는 $b = 0$이다.

정의 2.5 환 R의 임의의 원소 a에 대하여 $n \cdot a = 0$인 양의정수 n이 존재하면 그 성질을 만족하는 가장 작은 양의정수를 환 R의 표수*(charcateristic of R)*라 하고, 기호로 $ch(R)$로 나타낸다. 그런 양의정수가 존재하지 않으면 R의 표수는 0이라고 한다.

환 R이 곱셈항등원을 갖는 가환환이고 $n \cdot 1 = 0$을 만족하는 양의정수 n이 존재한다고 하자. 이 때 m을 $m \cdot 1 = 0$ 을 만족하는 가장 작은 양의정수라 하면 환 R의 임의의 원소 $a(a \neq 0)$에 대하여 $m \cdot a = m \cdot (1 \cdot a) = (m \cdot 1) \cdot a = 0 \cdot a = 0$ 이다. 따라서 환 R의 표수는 m이 된다. 즉 곱셈항등원을 갖는 가환환 R에서 $n \cdot 1 = 0$을 만족하는 양의정수 n이 존재하면 환 R의 표수는 이를 만족하는 가장 작은 양의정수이고, 이런 양의정수가 존재하지 않으면 환 R의 표수는 0이다.

정리 2.6 정역 R 의 표수는 0 또는 소수 p이다.

증명 정역 R의 표수가 0이 아닐 때 R의 표수를 합성수 mn (m, n은 양의 정수)이라 하자. 정역은 곱셈항등원 1을 갖는 가환환이므로, $mn \cdot 1 = 0$이다. 따라서

$$mn \cdot 1 = (m \cdot 1) \cdot (n \cdot 1) = 0$$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

R이 정역이므로 $m \cdot 1 = 0$ 또는 $n \cdot 1 = 0$ 이다. 이는 R의 표수가 mn이라는 사실에 모순이다. 따라서 정역 R의 표수는 0 또는 소수 p이다.

이제 다항식환에 대해 알아보자. 다항식환의 정의와 성질은 다음과 같다.

정의 2.7 환 R과 부정원 x에 대하여 다음과 같은 꼴의 형식적인 무한합*(formal infinite sum)*을 R 위의 다항식*(polynomial)*이라고 한다.

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n + \cdots (a_i \in R)$$

(유한 개를 제외한 모든 i 에 대하여 $a_i = 0$)
그리고, R 위의 x에 관한 다항식 전체의 집합을 $R[x]$라 한다.

위의 정의에서 $a_0, a_1 x, \cdots, a_n x^n, \cdots$ 을 각각 $f(x)$의 항(term)이라 하고 그 중 a_0를 상수항이라고 하며 $a_0, a_1, \cdots, a_n, \cdots$을 $f(x)$의 계수(coefficient)라 한다. 또한 $i > n$인 모든 i 에 대하여 $a_i = 0$ 일 때, $f(x)$를

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n (a_i \in R) \qquad (*)$$

로 나타낸다. 다항식 중에서 상수항을 제외한 모든 계수가 0인 다항식 $f(x) = a_0$를 상수다항식(constant polynomial) 이라 하고, 모든 계수가 0인 다항식을 영다항식(zero polynomial) 이라고 한다. 식$(*)$에서 a_n이 0이 아니면 $f(x)$의 차수(degree)를 n이라 하고 기호로 $\deg f = n$이라 나타낸다.

환 R에서 정의된 모든 다항식들의 집합 $R[x]$에 대하여 다항식의 덧셈과 곱셈을 다음과 같이 정의하자.
임의의 원소 $f(x) = \sum_{i=0}^{n} a_i x^i,\ g(x) = \sum_{j=0}^{m} b_j x^j \in R[x]$에 대하여

$$f + g := \sum_{i=0}^{k} c_i x^i, \quad c_i = a_i + b_i, \quad k = \max(m, n)$$

$$fg := \sum_{i=0}^{m+n} d_k x_k, \quad d_k = \sum_{i=0}^{k} a_i b_{k-i}$$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

정리 2.8 환 R에서 정의된 모든 다항식들의 집합 $R[x]$은 앞에서 정의한 덧셈과 곱셈에 의하여 환이 된다.

증명 [3], [7] 참조

보조정리 2.9 환 R을 곱셈항등원을 갖는 가환환이라 하자. 임의의 $f(x),\ g(x) \in R[x]$에 대하여 다음이 성립한다.

1. $\deg(f+g) \leq \max\{\ \deg(f), \deg(g)\ \}$
2. $\deg(fg) \leq \deg(f) + \deg(g)$
3. R이 정역이면, $\deg(fg) = \deg(f) + \deg(g)$

증명 $f(x) = \sum_{i=0}^{n} a_i x^i,\ \ g(x) = \sum_{j=0}^{m} b_j x^j \in R[x]\ \ (n \leq m)$이라 하자.

1. i) $n = m$ 이고 $a_n = -b_m$ 이면 $f(x)+g(x) = (a_0+b_0)+\cdots\ +(a_{n-1}+b_{m-1})x^{m-1}$ 이므로 $\deg(f+g) < m = \max\{\ \deg(f), \deg(g)\ \}$
ii) $n = m$ 이고 $a_n \neq -b_m$이면 $f(x)+g(x) = (a_0+b_0)+\cdots+(a_n+b_m)x^m\ \ (a_n+b_m \neq 0)$이므로 $\deg(f+g) = m = \max\{\ \deg(f), \deg(g)\ \}$
iii)$n \neq m$ 이면 $f(x)+g(x) = (a_0+b_0)+\cdots+b_m x^m\ \ (b_m \neq 0)$이므로 $\deg(f+g) = m = \max\{\ \deg(f), \deg(g)\ \}$
따라서 i), ii), iii)에 의해 $\deg(f+g) \leq \max\{\ \deg(f), \deg(g)\ \}$ 이다.
2. $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{n+m}$ 이다.
$a_nb_m = 0$이면 $\deg(fg) < n+m = \deg(f)+\deg(g)$
$a_nb_m \neq 0$이면 $\deg(fg) = n+m = \deg(f)+\deg(g)$
따라서 $\deg(fg) \leq \deg(f)+\deg(g)$ 이다.
3. R이 정역이면 $a_n \neq 0, b_m \neq 0$ 일 때, $a_nb_m \neq 0$이므로 $\deg(fg) = \deg(f)+\deg(g)$ 이다.

다항식환의 정의와 보조정리 2.9에 의하여 다음을 간단히 얻을 수 있다.

따름정리 2.10 환 R에 대하여 x를 R위에서의 부정원이라 할 때, 다음이 성립한다.

1. R이 곱셈항등원 1을 갖는 환이면 $R[x]$도 곱셈항등원 1을 갖는다.
2. R이 가환환이면 $R[x]$도 가환환이다.
3. R이 정역이면 $R[x]$도 정역이다

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

증명 1,2번은 자명하므로 3번만 증명해보자. 3번은 정역의 정의를 사용하여 증명할 수도 있지만 여기서는 보조정리 2.9를 사용하여 증명해 보도록 하자. 임의의 영다항식이 아닌 $f(x), g(x) \in R[x]$ 에 대하여 $\deg f(x) \geq 0, \deg g(x) \geq 0$ 이다. 이때 보조정리 2.9에 의해 R이 정역이므로 $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$ 이다. 즉, $\deg(f(x)g(x)) \geq 0$ 이므로 $f(x)g(x)$ 영다항식이 아니다. 따라서 $R[x]$는 정역이다.

정의 2.11 영도 아니고 가역원도 아닌 정역 D의 원소 p가 D의 가역원이 아닌 두 원소의 곱으로 표현되지 않으면 p는 D의 기약*(irreducible)*이라 한다. 즉 $p = ab$ 일 때 a 또는 b가 가역원이면 p가 D의 기약이다.

이제 정역 R위의 다항식환 $R[x]$의 기약에 대해 알아보자.
영다항식이 아닌 다항식 $f(x) \in R[x]$가 가역원이라 하자. 적당한 $g(x) \in R[x]$가 존재해서 $g(x)f(x) = 1$이다. R이 정역이므로 보조정리 2.9에 의해 $0 = \deg 1 = \deg(f(x)g(x)) = \deg f(x) + \deg g(x)$이 성립한다. 이때 $\deg f(x) \geq 0, \deg g(x) \geq 0$ 이므로 $\deg f(x) = 0, \deg g(x) = 0$이다. 따라서 $R[x]$의 가역원은 상수다항식 즉, R에서의 가역원이다.
이제 정역 R위에서의 다항식환 $R[x]$에서의 기약임을 다음과 같이 설명할 수 있다. $f(x) \in R[x]$, $\deg(f(x)) \geq 1$이라고 하자. 다항식 $g(x), h(x) \in R[x]$에 대하여 $f(x) = g(x)h(x)$ 이면 $g(x) = a$ 또는 $h(x) = a$ (a는 R에서의 가역원) 일 때, $f(x)$를 $R[x]$의 기약다항식(irreducible polynomial)이라고 한다. 또한 기약이 아닌 다항식을 가약다항식이라고 한다.

체 F위의 다항식환 $F[x]$에 대하여 $f(x) \in F[x]$가 일차,이차 또는 삼차 다항식인 경우 F상에서의 해의 존재유무를 통해 기약임을 판별할 수 있다. 하지만 고차 다항식인 경우 다항식이 기약다항식인지 아닌지 판별하는것은 쉬운 일이 아니다. 하지만 특별히 정수환위의 다항식환 $\mathbb{Z}[x]$에서는 특별한 성질을 만족하는 고차다항식인의 경우 기약인지 판별하는 판정법이 있다.

정리 2.12 *(Eisenstein*의 기약판정법*)* 정수환 $\mathbb{Z}$위의 n차의 다항식 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $n \geq 1$ 에 대하여 다음이 성립한다. 적당한 소수p에 대하여 $p \nmid a_n$, $p | a_{n-1}, \cdots$, $p | a_1$, $p | a_0$, $p^2 \nmid a_0$이면, $f(x)$는 유리수체 $\mathbb{Q}$위에서 기약이다.

증명 [3], [7] 참조

정의 2.13 환 R에서의 부분집합 N $(\neq 0)$이 아래의 두 조건을 만족시키면 N을 환R의 아이디얼*(ideal)*이라고 한다.

1. $(N, +)$는 $(R, +)$의 부분군이다. 즉, $a, b \in N$ 이면 $a - b \in N$이다.
2. 임의의 원소 $a \in N, r \in R$에 대하여 $ra, ar \in N$ 이다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

환 R이 곱셈항등원을 가진 가환환이면 $N = \{ra \mid r \in R\}$는 임의의 원소 $r_1a, r_2a \in N$ 에대하여 $r_1a - r_2a = (r_1 - r_2)a \in N$이고, 임의의 $b \in R, ra \in N$ 에 대하여 $b(ra) = (br)a \in N$ 이고 $(ra)b = r(ab) = (rb)a \in N$ 이므로 R의 아이디얼이다.

정의 2.14 환 R이 곱셈항등원 1을 가진 가환환이고 $a \in R$이면, 아이디얼 $\{ ra \mid r \in R \}$을 a로 생성된 주아이디얼*(principal ideal)*이라 하고 기호로 $\langle a \rangle$ *or* (a)로 나타낸다. 즉, R의 주아이디얼 N은 R의 적당한 원소 a에 대하여 $N = \langle a \rangle$인 R의 아이디얼이다. 또한, 정역 D의 모든 아이디얼이 주아이디얼이면 D는 주아이디얼 정역*(principal ideal domain, PID)*이라 한다.

정의 2.15 유클리드 정역
정역의 유클리드 노름*(Euclidean norm)*은 다음 조건을 만족하는 D의 영이 아닌 원소들을 음수가 아닌 정수들의 집합으로 보내는 함수 v이다.
1. $a, b \in D$ 이고 $b \neq 0$ 이면, $a = bq + r$ 인 q와 r이 D에 존재하여 $r = 0$ 이거나 $v(r) < v(b)$ 이다.
2. $a, b \in D$ 이고 $a \neq 0, b \neq 0$ 이면 $v(a) \leq v(ab)$이다.
유클리드 정역*(Euclidean domain)* D는 유클리드 노름이 존재하는 정역이다.

정리 2.16 유클리드 정역은 주아이디얼 정역이다.

증명 유클리드 정역 D에 대하여 δ를 유클리드 노름이라 하고 N을 D의 아이디얼이라고 하자. 먼저 $N = 0$ 이면 $N = (0)$ 이다. 이제 $\{0\} \subsetneq N$ 이라고 하자. 이 때, 모든 $x \in N - \{0\}$에 대하여 $\delta(x) \geq 1$ 이므로 정수의 정렬성에 의하여 $N - \{0\}$에 속하는 원소중에서 δ의 값이 최소인 원소 $b \in N - \{0\}$가 존재한다. 즉, 모든 $x \in N - \{0\}$에 대하여 $0 < \delta(b) \leq \delta(x)$이고 $\{0\} \subsetneq (b) \subset N$ 이다. 그리고, 임의의 $a \in N$에 대하여 $a = bq + r, \delta(r) < \delta(b)$ 인 원소 $q, r \in D$가 존재하고 이때 $r = a - bq \in N$이고 $\delta(b)$의 최소성에 의해서 $r = 0$이므로 $a = bq \in (b)$이다. 그러므로 $N = (b)$ 이다. 따라서 유클리드 정역이면 주아이디얼 정역이다.

체 F위의 다항식환 $F[x]$가 주아이디얼 정역임은 잘 알려진 사실이며 이는 체상의 다항식환의 나눗셈 알고리즘을 이용하면 쉽게 증명 할 수 있다. 여기에서는 $F[x]$가 유클리드정역임을 보임으로써 정리 2.16를 통해 성립함 다시 한번 보이도록 한다. ([3], [7])
체F 위의 다항식환 $F[x]$의 나눗셈 알고리즘에 대한 내용은 다음과 같다.

보조정리 2.17 나눗셈 알고리즘 *(divison algorithm)*
체 F위의 다항식환 $F[x]$의 임의의 두 다항식 $f(x), g(x) \in F[x], g(x) \neq 0$에 대하여 $f(x) = q(x)g(x) + r(x),\ r(x) = 0$ 또는 $0 \leq \deg(r(x)) < \deg(g(x))$ 인 다항식 $q(x), r(x) \in F[x]$가 유일하게 존재한다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

이제 정의 2.15를 이용하여 F위에서의 다항식환 $F[x]$가 유클리드 정역임을 보일 수 있다. 사상 $\delta : F \to W$, $\delta(f(x)) = 2^{\deg(f(x))}$ (단, $2^{-\infty} = 0$) 라 하자.
$f(x) = 0 \Leftrightarrow \deg(f(x)) = -\infty \Leftrightarrow \delta(f(x)) = 2^{-\infty} = 0$ 이고, 또 두 다항식, $f(x), g(x) \in F[x], g(x) \neq 0$ 에 대하여 $\delta(f(x)) = 2^{\deg(f(x))} \leq 2^{\deg(f(x))+\deg(g(x))} \leq 2\deg(f(x)g(x)) \leq \delta(f(x)g(x))$ 이며 보조정리 2.17에 의해 $f(x) = q(x)g(x)+r(x)$, $r(x) = 0$ 또는 $0 \leq \deg(r(x)) < \deg(g(x))$ 인 다항식 $q(x), r(x) \in F[x]$가 존재하고 이때 $\deg(r(x)) < \deg(g(x))$ 이므로 $\delta(r(x)) < \delta(g(x))$이다. δ는 유클리드 노름이므로 $F[x]$는 유클리드 정역이다.

체F위에서의 다항식환$F[x]$가 유클리드 정역이므로 정리 2.16에 의해 $F[x]$는 주아이디얼 정역이다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

제 3 장

Hurwitz 다항식환

이 장에서는 앞에서 다루었던 다항식환 $R[x]$의 성질과 새로운 연산에 대한 다항식환의 성질을 비교해보고자 한다. 이 장의 대부분의 결과들은 [2], [5]에 나와있으며, 필요한 경우 증명을 다시 한 번 쓰도록 한다.

환 R에서 계수를 갖는 다항식 집합 $R[x]$에 두 연산 $+$, $*$ 을 다음과 같이 정의한다. 임의의 원소 $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{j=0}^{m} b_j x^j \in R[x]$에 대하여

$$f + g = \sum_{i=0}^{k} c_i x^i, \quad c_i = a_i + b_i, \quad k = \max(m, n)$$

$$f * g = \sum_{i=0}^{m+n} d_k x_k, \quad d_k = \sum_{i=0}^{k} \binom{k}{i} a_i b_{k-i}$$

다음 정리는 Keigher([5])에 의해 알려진 것으로 여기서는 증명을 다시한번 쓰도록 한다.

정리 3.1 R이 곱셈항등원 1을 가진 가환환 이면 $(R[x], +, *)$ 또한 곱셈항등원 1 을 갖는 가환환이다.

증명 임의의 $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ 에 대하여
$f(x) * 1 = f(x)$ 이므로 $(R[x], +, *)$은 곱셈항등원 1을 가진 환이 됨은 자명하다.

이제 $(R[x], +, *)$이 가환환임을 보이자.
임의의 $f(x), g(x) \in R$ 에 대하여

$$f(x) = \sum_{i=0}^{n} a_i x^i, \ g(x) = \sum_{j=0}^{m} b_j x^j, \ f(x) * g(x) = \sum_{k=0}^{m+n} d_k x^k, \ d_k = \sum_{i=0}^{k} \binom{k}{i} a_i b_{k-i}$$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

라하자.

$$\begin{aligned}
f(x)*g(x) &= d_0+d_1x+\cdots+d_{n+m}x^{n+m}\\
&= a_0b_0+(a_0b_1+a_1b_0)x+\cdots\\
&\quad+\left\{\binom{i}{0}a_0b_i+\binom{i}{1}a_1b_{i-1}+\cdots+\binom{i}{i}a_ib_0\right\}x^i+\cdots\\
&\quad+\left\{\binom{n+m}{0}a_0b_{n+m}+\cdots+\binom{n+m}{n+m}a_{n+m}b_0\right\}x^{n+m}\\
&= b_0a_0+(b_0a_1+b_1a_0)x+\cdots\\
&\quad+\left\{\binom{i}{i}b_0a_i+\binom{i}{i-1}b_1a_{i-1}+\cdots+\binom{i}{0}b_ia_0\right\}x^i+\cdots\\
&\quad+\left\{\binom{n+m}{n+m}b_0a_{n+m}+\cdots+\binom{n+m}{0}b_{n+m}a_0\right\}x^{n+m}\\
&= b_0a_0+(b_0a_1+b_1a_0)x+\cdots\\
&\quad+\left\{\binom{i}{0}b_0a_i+\binom{i}{1}b_1a_{i-1}+\cdots+\binom{i}{i}b_ia_0\right\}x^i+\cdots\\
&\quad+\left\{\binom{m+n}{0}b_0a_{m+n}+\cdots+\binom{m+n}{m+n}b_{m+n}a_0\right\}x^{m+n}\\
&= g(x)*f(x)
\end{aligned}$$

따라서 $(R[x],+,*)$은 가환환이다.

정리 3.1에서 보았듯이 곱셈항등원 1을 가진 가환환 R에 대하여 $(R[x],+,*)$도 곱셈항등원 1을 갖는 가환환이 된다. 이 환을 'Hurwitz 다항식환'이라 부르며 기호로 $h(R)$로 나타낸다.

$f(x)\in h(R)$에 대하여 $f(x)=a_0+a_1x+\cdots+a_nx^n$이라 하자. 이때 $a_n\neq 0$이면 $f(x)$의 차수(degree)를 n이라고 하고 기호로 $\deg f=n$이라 나타낸다.

R이 정역이면 다항식환 $R[x]$는 정역이다. 반면 R이 표수가 p인 정역인 경우 $x^{p-1}*x=\binom{p}{1}x^p=px^p=0$ 이므로 $h(R)$은 정역이 아니다. 따라서 $h(R)$이 언제 정역이 되는지 살펴보도록 하자. 다음 정리는 [2], [5]에 그 증명이 나와 있으나 다시 한 번 쓰도록 한다.

정리 3.2 곱셈항등원 1을 가진 가환환 R에 대하여 다음 두 조건은 동치이다.
(1) R이 표수가 0인 정역이다
(2) $h(R)$은 정역이다.

증명 (1) $\Rightarrow$ (2) 임의의 $f(x),g(x)\in h(R)$ 에 대하여 $f(x)=a_0+a_1x+\cdots+a_nx^n,\ g(x)=$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$b_0 + b_1x + \cdots + b_mx^m$
$\big(deg(f(x)) = n,\ deg(g(x)) = m, \quad n, m \neq 0\big)$ 라 하자.
$f(x) * g(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$ 이다.
이때 $c_{n+m} = \binom{n+m}{0}a_0b_{n+m} + \binom{n+m}{1}a_1b_{n+m-1} + \cdots + \binom{n+m}{n-1}a_{n-1}b_{m+1} + \binom{n+m}{n}a_nb_m + \binom{n+m}{n+1}a_{n+1}b_{m-1} + \cdots + \binom{n+m}{n+m}a_{n+m}b_0$ 이고
$a_{n+1} = a_{n+2} = \cdots = a_{n+m} = 0$, $b_{n+1} = b_{n+2} = \cdots = b_{n+m} = 0$ 이므로 $c_{n+m} = \binom{n+m}{n}a_nb_m$이다.
이때 $a_n \neq 0, b_m \neq 0$ 이고 R의 표수가 0이므로 $c_{n+m} \neq 0$ 이다. 따라서 $h(R)$은 정역이다.
(1) $\Leftarrow$ (2) 먼저 $R \subset h(R)$ 이므로 R은 정역이다. 또한 임의의 $a \in R(a \neq 0)$에 대하여 $a \in h(R)$ 이므로 $a \cdot n = 0 \Rightarrow a \cdot (n \cdot 1) = 0 \Rightarrow n \cdot 1 = 0$ 이므로 $n = 0$이다. 따라서 R의 표수는 0이다.

$F[x]$에서 다항식의 차수에 대한 보조정리 2.9의 내용이 $h(R)$에서도 성립하는지 확인해 보려 한다. $h(R)$은 표수의 영향을 받으므로 표수에 따라 차수의 값이 어떻게 달라지는지 다음 정리를 통해 살펴보자.

정리 3.3 환 R을 곱셈항등원을 가진 가환환이라 하자. 임의의 $f(x), g(x) \in h(R)$에 대하여 다음이 성립한다.
(1) $ch(R) \neq 0$ 일 때

1. $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$
2. $\deg(f * g) \leq \deg(f) + \deg(g)$

(2) $ch(R) = 0$ 일 때

1. $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$
2. $\deg(f * g) \leq \deg(f) + deg(g)$
3. R이 정역이면, $\deg(f * g) = \deg(f) + \deg(g)$

증명 $f(x) = \sum_{i=0}^{n} a_ix^i,\ g(x) = \sum_{j=0}^{m} b_jx^j \in h(R)\ (n \leq m)$이라 하자.
(1) $ch(R) = k\ (k \in \mathbb{N})$ 일 때
1. i) $n = m$ 이고 $k|(a_n + b_m)$이면 $f(x) + g(x) = (a_0 + b_0) + \cdots\ + (a_{n-1} + b_{m-1})x^{m-1}$ 이므로 $\deg(f+g) < m = \max\{\deg(f), \deg(g)\}$
ii) $n = m$ 이고 $k \nmid (a_n + b_m)$이면 $f(x) + g(x) = (a_0 + b_0) + \cdots + (a_n + b_m)x^m\ (a_n + b_m \neq 0)$ 이므로 $\deg(f+g) = m = \max\{\deg(f), \deg(g)\}$
iii)$n \neq m$ 이면 $f(x) + g(x) = (a_0 + b_0) + \cdots + b_mx^m\ (b_m \neq 0)$이므로 $\deg(f+g) = m = \max\{\deg(f), \deg(g)\}$
따라서 i), ii), iii)에 의해 $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$이다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

2. $f(x) * g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + \binom{n+m}{n} a_nb_mx^{n+m}$이다.
$k|\binom{n+m}{n} a_nb_m$ 이면 $\deg(f * g) < n + m = \deg(f) + \deg(g)$
$k \nmid \binom{n+m}{n} a_nb_m$이면 $\deg(f * g) = n + m = \deg(f) + \deg(g)$
따라서 $\deg(f * g) \leq \deg(f) + \deg(g)$ 이다.
(2) $ch(R) = 0$ 일 때
1. i) $n = m$ 이고 $a_n = -b_m$ 이면 $f(x) + g(x) = (a_0 + b_0) + \cdots + (a_{n-1} + b_{m-1})x^{m-1}$ 이므로 $\deg(f + g) < m = \max\{\deg(f), \deg(g)\}$
ii) $n = m$ 이고 $a_n \neq b_m$이면 $f(x) + g(x) = (a_0 + b_0) + \cdots + (a_n + b_m)x^m$ $(a_n + b_m \neq 0)$이므로 $\deg(f + g) = m = \max\{\deg(f), \deg(g)\}$
iii)$n \neq m$ 이면 $f(x) + g(x) = (a_0 + b_0) + \cdots + b_mx^m$ $(b_m \neq 0)$이므로 $\deg(f + g) = m = \max\{\deg(f), \deg(g)\}$
따라서 i), ii), iii)에 의해 $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$이다.
2. $f(x) * g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + \binom{n+m}{n} a_nb_mx^{n+m}$이다.
$\binom{n+m}{n} a_nb_m = 0$이면 $\deg(f * g) < n + m = \deg(f) + \deg(g)$
$\binom{n+m}{n} a_nb_m \neq 0$이면 $\deg(f * g) = n + m = \deg(f) + \deg(g)$
따라서 $\deg(f * g) \leq \deg(f) + \deg(g)$ 이다.
3. R이 정역이면 $a_n \neq 0, b_m \neq 0$ 일 때, $\binom{n+m}{n} a_nb_m \neq 0$이므로 $\deg(f*g) = \deg(f)+\deg(g)$이다.

체 F위에서의 다항식환 $F[x]$는 나눗셈알고리즘이 성립하였고 이를 통해서 $F[x]$가 유클리드 정역(ED)임을 보였다. 이제 체 F위에서의 Hurwitz 다항식환 $h(F)$가 나눗셈 알고리즘이 성립하는 지를 살펴보고 성립한다면 $h(F)$ 또한 유클리드 정역인지를 알아보도록 하자. 먼저 체 F의 표수가 0이 아니면 $h(F)$는 정역이 아니므로 표수가 0일 때 만 살펴보도록 하자.

보조정리 3.4 체F의 표수가 0이면 임의의 $f(x), g(x) \in h(F)$ 에 대하여 $f(x) = q(x) * g(x) + r(x)$, $r(x) = 0$ 또는 $0 \leq \deg(r(x)) < \deg(g(x))$ 인 다항식 $q(x), r(x) \in h(F)$가 유일하게 존재한다.

증명 F가 표수가 0인 체이므로 정리 3.2 에 의해 $h(F)$는 정역이다.
나눗셈 정리가 성립하기 위해서는 $f(x), g(x) \in h(F)$, $g(x) \neq 0$에 대하여
$f(x) = q(x) * g(x) + r(x) \quad \big(r(x) = 0 \text{ or } 0 \leq \deg(r(x)) < \deg(g(x))\big)$ 인
다항식 $q(x), r(x) \in h(F)$가 유일하게 존재해야 한다.
(존재성)
$i)$ $\deg(f(x)) < \deg(g(x))$인 경우 $q(x) = 0, r(x) = f(x)$라고 놓으면 성립
$ii)$ $g(x) = a\big(a \in h(F), a \neq 0\big)$인 경우 $q(x) = a^{-1}f(x), r(x) = 0$으로 두면 성립
$iii)$ $\deg(f(x)) \geq \deg(g(x)) \geq 1$일 때, $f(x) = a_0 + a_1x + \cdots + a_nx^n, g(x) = b_0 + b_1x + \cdots + b_mx^m$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

라 하자.
F은 체이므로 $b_m^{-1}\binom{n}{m}^{-1} \in F$이고 $f(x) = \left(b_m^{-1}\binom{n}{m}^{-1} a_n x^{n-m}\right) * g(x) + p(x)$ 인 다항식 $p(x) \in h(F)$가 존재하고 이때 $\deg(p(x)) \leq n-1 < n$ 이다.
다시 $p(x)$에 대하여 위의 절차를 되풀이 하면 $p(x) = q_1(x) * g(x) + r(x)$ $\big(r(x) = 0 \ or \ 0 \leq \deg(r(x)) < \deg(g(x))\big)$인 $q_1(x), r(x) \in h(F)$가 존재하고 여기서 $q(x) = \frac{a_n}{\binom{n}{m} b_m} \cdot x^{n-m} + q_1(x)$ 이라고 하면 $f(x) = q(x) * g(x) + r(x)$이다.
(유일성)
$f(x) = q_1(x) * g(x) + r_1(x), \ \ f(x) = q_2 * g(x) + r_2(x)$라고 하자.
그러면 $q_1(x) * g(x) + r_1(x) = q_2 * g(x) + r_2(x)$ 이고 $q_1(x) * g(x) - q_2(x) * g(x) = r_2(x) - r_1(x)$ 이면
$(q_1(x) - q_2(x)) * g(x) = r_2(x) - r_1(x)$ 이다. 이때 $\deg(g(x)) > \deg(r_2(x) - r_1(x))$이고 $g(x) \neq 0$ 이므로
$q_1(x) - q_2(x) = 0$ 이고 $r_2(x) - r_1(x) = 0$이다. 따라서 $q_1(x) = q_2(x), r_1(x) = r_2(x)$이다. 즉 $q(x), r(x) \in h(F)$ 은 유일하다. 따라서 정리가 성립한다.

정리 3.5 체F의 표수가 0이면 $h(F)$은 유클리드 정역(ED)이다.

증명 체F의 표수가 0이면 정리 3.2에 의해 $h(F)$는 정역이다.
이제 유클리드 노름이 존재하는지를 보이자.
$\upsilon : h(F) \to W, \ W = \{n \in \mathbb{Z} \mid n \geq 0\}, \ \upsilon\big(h(x)\big) = 2^{deg(h(x))}$(단, $2^{-\infty} = 0$)
$i)$ 보조정리 3.4에 의해 $h(x), g(x) \in h(F), g(x) \neq 0$에 대하여 $h(x) = q(x) * g(x) + r(x)\big(r(x) = 0 \ or \ \deg(r(x)) < \deg(g(x))\big)$를 만족하는 $q(x), r(x) \in h(F)$가 존재하므로 $\upsilon\big(r(x)\big) < \upsilon\big(g(x)\big)$를 만족한다. $ii) h(x) = 0 \in h(F) \Leftrightarrow \upsilon\big(0\big) = 2^{-\infty}$
$h_1(x), h_2(x) \in h(F), h_2(x) \neq 0$

$$\begin{aligned} \Rightarrow \ \upsilon\big(h_1(x)\big) &= 2^{deg(h_1(x))} \leq 2^{deg(h_1(x)) + deg(h_2(x))} = 2^{deg(h_1(x) * h_2(x))} \\ &= \upsilon\big(h_1(x) * h_2(x)\big) \end{aligned}$$

즉, $\upsilon(h_1(x)) \leq \upsilon\big(h_1(x) * h_2(x)\big)$이다.
따라서 $i), ii)$를 만족하므로 정의 2.15에 의해 유클리드 노름 υ이 존재해서 $h(F)$는 유클리드 정역이다.

체F의 표수가 0인이면 $h(F)$가 유클리드정역이므로 정리 2.16에 의해 $h(F)$는 주아이디얼 정역이다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

유리수체 $\mathbb{Q}$위의 다항식환 $\mathbb{Q}[x]$는 주아이디얼 정역이다. 또한 유리수체 $\mathbb{Q}$는 표수가 0이므로 $h(\mathbb{Q})$ 또한 주아이디얼 정역이다. 그러나 임의의 $f(x) \in F[x]$에 대하여, $f(x)$로 생성되는 다항식환의 주아이디얼 $\langle f(x) \rangle$ 와 $f(x)$로 생성되는 Hurwitz다항식환의 주아이디얼 $\langle f(x) \rangle$는 서로 다르다. 예를 들면 $\mathbb{Q}[x]$에서 $x^2+2x+1=(x+1)(x+1)$ 이므로 $x^2+2x+1 \in \langle x+1 \rangle$ 이다. 이제 임의의 $h(x) \in h(\mathbb{Q})$에 대하여 $(x+1)*h(x) \neq x^2+2x+1$ 임을 보이자. 먼저 $\mathbb{Q}$는 표수가 0인 체이므로 $h(\mathbb{Q})$는 정역이다. 따라서 $\deg(h(x)) \geq 2$ 이면 $\deg((x+1)h(x)) > 2$ 이므로 $h(x)$는 일차다항식이다. $h(x)=ax+b$라 하자. $(x+1)*(ax+b)=2ax^2+(a+b)x+b$ 이므로 $b=1, a=\frac{1}{2}$이다. 그러면 $a+b=\frac{3}{2} \neq 2$ 이므로 $x^2+2x+1 \notin \langle x+1 \rangle$ 이다.
위의 방법과 같은 방법을 적용하면 $f(x)$가 상수다항식이 아닌 경우 $\langle f(x) \rangle = \{f(x)g(x) | g(x) \in \mathbb{Q}[x]\} \neq \langle f(x) \rangle = \{f(x)*h(x) | h(x) \in h(\mathbb{Q})\}$ 가 성립한다.

우리에게 잘 알려진 이항정리는 $(ax+b)^n = \binom{n}{0}a^nx^n + \binom{n}{1}a^{n-1}bx^{n-1} + \cdots + \binom{n}{n-1}ab^{n-1}x + \binom{n}{n}b^n$ 이다. 위에서 설명 하였듯이 똑같은 $f(x) \in F[x]$에 의해 생성된 두 주아이디얼은 다른 형태를 가지고 있다. 따라서 이항정리 또한 다른 형태를 가지고 유추 할 수 있다. Hurwitz다항식에서의 이항정리는 어떠한 형태로 나타나는지 살펴보도록 하자.

정리 3.6 *Hurwitz*다항식환에서의 이항정리는 다음과 같다.

$$\begin{aligned}(ax+b)^n &= n!a^nx^n + (n-1)!\binom{n}{n-1}a^{n-1}bx^{n-1} + \cdots + 1!\binom{n}{1}ab^{n-1}x + b^n \\ &= a^nx^n + \frac{n!}{1!}a^{n-1}bx^{n-1} + \cdots + \frac{n!}{i!}a^{n-i}b^ix^{n-i} + \cdots + \frac{n!}{(n-1)!}ab^{n-1}x + b^n\end{aligned}$$

증명
$n=1$ 이면 $ax+b=1!ax+b$ 이므로 성립
$n=k$ 일 때 $(ax+b)^k = k!a^kx^k + (k-1)!\binom{k}{k-1}a^{k-1}bx^{k-1} + \cdots + 1!\binom{k}{1}ab^{k-1}x + b^k$ 이 성립한다고 가정하자.
$n=k+1$ 이면
$(ax+b)^k * (ax+b) = c_{k+1}x^{k+1} + c_kx^k + \cdots + c_1x + c_0$ 이고 $c_i = \binom{i}{i-1}(i-1)!\binom{k}{i-1}a^ib^{k+1-i}x^i + i!\binom{k}{i}a^ib^{k+1-i}x^i$
$= \left\{\binom{k}{i-1} + \binom{k}{i}\right\}i!a^ib^{k+1-i}x^i = \binom{k+1}{i}i!a^ib^{k+1-i}x^i$ 이므로
$(ax+b)^{k+1} = (k+1)!a^{k+1}x^{k+1} + (k)!\binom{k+1}{k}a^kbx^k + \cdots + 1!\binom{k+1}{2}a^2b^{k-1}x^2 + \binom{k+1}{1}ab^kx + b^{k+1}$ 이 성립한다.
따라서 수학적 귀납법에 의해 모든 자연수 n에 대하여
$(ax+b)^n = n!a^nx^n + (n-1)!\binom{n}{n-1}a^{n-1}bx^{n-1} + \cdots + 1!\binom{n}{1}ab^{n-1}x + b^n$
이 성립한다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

제 4 장

Hurwitz 다항식 기약판별법

이 장에서는 Hurwitz다항식 $f(x)$가 $h(R)$에서 언제 기약이 되는지를 알아보려한다. 그 중 기약에 대해 잘 알려진 정수환 $\mathbb{Z}$ 위의 다항식환 $\mathbb{Z}[x]$ 와 Hurwitz다항식환 $h(\mathbb{Z})$의 관계를 살펴보도록 하자.
표수가 0인 정역 R에 대하여 $h(R)$에서의 가역원은 다음과 같다. 영다항식이 아닌 $f(x) \in h(R)$가 가역원이라 하자. 그러면 적당한 $g(x) \in h(R)$이 존재해서 $g(x) * f(x) = 1$이므로 정리 3.3에 의해 $0 = \deg 1 = \deg(f(x) * g(x)) = \deg(f(x)) + \deg(g(x))$이 성립한다. 이때 $\deg(f(x)) \geq 0$, $\deg(g(x)) \geq 0$ 이므로 $\deg f(x) = 0$, $\deg g(x) = 0$이다. 따라서 $h(R)$의 가역원은 상수다항식 즉, R에서의 가역원이다.

보조정리 4.1 $h(\mathbb{Z})$에서의 가역원은 $\mathbb{Z}$에서의 가역원이다. 즉, $1, -1$ 뿐이다.

정리 4.2 임의의 $a, b \in \mathbb{Z}(a \neq 0)$에 대하여 다음 조건은 동치이다.
(1) a와 b가 서로소이다. 즉 $(a, b) = 1$
(2) $ax + b$가 $\mathbb{Z}[x]$에서 기약이다
(3) $ax + b$가 $h(\mathbb{Z})$에서 기약이다.

증명 (1) $\Rightarrow$ (2) $ax + b = c(mx + n)$을 만족하는 $c, m, n \in \mathbb{Z}[x]$가 존재한다고 하자.
$c(mx + n) = cmx + cn$ 이므로 $cm = a$, $cn = b$이고 가정에 의해 $(a, b) = 1$이므로 $c = \pm 1$ 뿐이다. 이때 ± 1은 보조정리 4.1에 의하여 $\mathbb{Z}$에서 가역원이므로 정의 2.11에 의해 $ax + b$는 $\mathbb{Z}[x]$에서 기약이다.
(2) $\Rightarrow$ (3) $ax + b = c * (mx + n)$을 만족하는 $c, m, n \in \mathbb{Z}$가 존재한다고 하자.
$c * (mx + n) = cn + \binom{1}{0} cmx = cn + cmx$ 이므로 $cm = a$, $cn = b$이다. 이때 $ax + b = cmx + cn = c(mx + n) \in \mathbb{Z}[x]$이므로 가정에 의해 기약이므로 $c = \pm 1$뿐이다. 따라서 정의 2.11에 의해 $ax + b$는 $h(\mathbb{Z})$에서 기약이다.
(3) $\Rightarrow$ (1) $(a, b) = c \neq 1$이라 하자. 그러면 $a = cm$, $b = cn$을 만족하는 적당한 $m, n \in \mathbb{Z}$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

이 존재한다. 따라서 $ax+b = cmx+cn = c*(mx+n)$이고 이때 c와 $mx+n$는 $h(\mathbb{Z})$에서 가역원이 아니므로 정의 2.11에 의해 $ax+b$는 $h(\mathbb{Z})$에서 기약이 아니다. 따라서 $ax+b$가 $h(\mathbb{Z})$에서 기약이면 $(a,b)=1$이다.

정리 4.2의 동치관계와 같이 이차다항식에서도 동치관계임을 알아보자. $f(x)=ax^2+bx+c \in \mathbb{Z}[x]$에 대하여 $(a,b,c)\neq 1$ 이면 $f(x)$는 $\mathbb{Z}[x], h(\mathbb{Z})$에서 항상 기약이 아니므로 $(a,b,c)=1$인 경우를 살펴보도록 하자. 이차다항식 x^2+2x+1는 $\mathbb{Z}[x]$에서는 기약이 아니지만 $h(\mathbb{Z})$에서는 기약이다. 따라서 정리 4.2에서의 동치조건은 이차다항식인 경우에는 만족하지 않는다. 하지만 이차다항식에서도 다음과 같은 동치조건이 있다.

정리 4.3 임의의 $a,b,c \in \mathbb{Z}(a\neq 0)$에 대하여 다음 두 조건은 동치이다.
(1) $2ax^2+bx+c$가 $h(\mathbb{Z})$에서 기약이다
(2) ax^2+bx+c가 $\mathbb{Z}[x]$에서 기약이다.

증명 (1) $\Rightarrow$ (2) ax^2+bx+c 가 $\mathbb{Z}[x]$에서 기약이 아니라고 하자. 적당한 $m_1,n_1,m_2,n_2 \in \mathbb{Z}$ 가 존재해서 $ax^2+bx+c=(m_1x+n_1)(m_2x+n_2)$이다. $ax^2+bx+c=m_1m_2x^2+(m_1n_2+m_2n_1)x+n_1n_2$이고 이때 $2m_1m_2x^2+(m_1n_2+m_2n_1)x+n_1n_2=(m_1x+n_1)*(m_2x+n_2)$이므로 $2ax^2+bx+c$는 $h(\mathbb{Z})$에서 기약이 아니다. 따라서 $2ax^2+bx+c$가 $h(\mathbb{Z})$에서 기약이면 ax^2+bx+c가 $\mathbb{Z}[x]$에서 기약이다.

(2) $\Rightarrow$ (3) $2ax^2+bx+c$가 $h(\mathbb{Z})$에서 기약이 아니라고 하자. $m_1,n_1,m_2,n_2 \in \mathbb{Z}$ 가 존재해서 $2ax^2+bx+c=(m_1x+n_1)*(m_2x+n_2)$ 이다. $2ax^2+bx+c=2m_1m_2x^2+(m_1n_2+m_2n_1)x+n_1n_2$이고 이때 $m_1m_2x^2+(m_1n_2+m_2n_1)x+n_1n_2=(m_1x+n_1)(m_2x+n_2)$ 이므로 ax^2+bx+c 는 $\mathbb{Z}[x]$에서 기약이 아니다. 따라서 ax^2+bx+c가 $\mathbb{Z}[x]$에서 기약이면 $2ax^2+bx+c$가 $h(\mathbb{Z})$에서 기약이다.

$h(\mathbb{Z})$에서는 이차다항식이 기약인지 아닌지 판별하려면 약간의 계산을 필요로 한다. 하지만 $\mathbb{Z}[x]$에서는 이차다항식이 기약인지 아닌지 쉽게 판별할 수 있다. 따라서 정리 4.3의 동치조건을 이용하면 $h(\mathbb{Z})$에서 이차다항식이 기약인지 아닌지는 쉽게 판별할 수 있다.

예제 4.1 $2x^2+2x+1$의 경우 x^2+2x+1이 $\mathbb{Z}[x]$에서 기약이 아니므로 정리 4.3에 의해 $2x^2+2x+1$는 $h(\mathbb{Z})$에서 기약이 아니다. 또한 $4x^2+6x+3$의 경우 $2x^2+6x+3$이 $\mathbb{Z}[x]$에서 기약이므로 정리 4.3에의해 $4x^2+6x+3$는 $h(\mathbb{Z})$에서 기약이다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

삼차다항식의 동치조건도 살펴보려했으나 이 논문에서는 $h(\mathbb{Z})$와 $\mathbb{Z}[x]$에서의 동치조건을 찾을 수가 없었다. 이제 $h(\mathbb{Z})$에서 기약이 되는 조건을 살펴보자. 먼저 고차다항식에서는 다음과 같은 방법으로 기약임을 판별할 수 있다.

정리 4.4 차수가 소수인 임의의 $f(x) \in h(\mathbb{Z})$에 대하여 $deg(f(x)) = p$(p는 소수), 최고차항의 계수를 a_p라 하자. 이때 $p \nmid a_p$ 이면 $f(x)$는 기약이다.

증명 다항식 $f(x) = a_p x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0 \in h(\mathbb{Z})$ $(a_0, a_1, \cdots, a_p \in \mathbb{Z},\ p \nmid a_n)$가 $h(\mathbb{Z})$에서 기약이 아니라고 하자. 그러면 적당한 두 다항식 $g(x), h(x) \in h(\mathbb{Z})$ 가 존재해서 $g(x) = b_s x^s + b_{s-1}x^{s-1} + \cdots + b_1 x + b_0$, $h(x) = c_t x^t + c_{t-1}x^{t-1} + \cdots + c_1 x + c_0$, $(0 < s, t < p,\ s+t = p)$ 이고 $f(x) = g(x) * h(x) = b_0 c_0 + (\binom{1}{0} b_0 c_1 + \binom{1}{1} b_1 c_0)x + \cdot + \binom{p}{s} b_s c_t x^p$ 이다. 최고차항의 계수 $a_p = \binom{p}{s} b_s t_s$이고 $\binom{p}{s} | a_p$이다. 이때 $p | \binom{p}{s}$ 이므로 $p | a_p$ 이고 이는 $p \nmid a_p$에 모순이므로 $f(x)$는 기약이다.

예제 4.2 $2x^3 + 4x^2 - 5x - 1$의 차수는 3이고 최고차항의 계수는 2 이므로 $3 \nmid 2$ 가되어 정리 4.4에 의해 $h(\mathbb{Z})$에서 기약이다.
하지만 $2x^3 + 4x^2 - 5x - 1 = (x-1)(2x^2 + 6x + 1)$이므로 $\mathbb{Z}[x]$에서는 기약이 아니다. 따라서 $\mathbb{Z}[x]$에서는 정리 4.4이 성립하지 않는다.

$f(x) \in h(\mathbb{Z})$ 차수가 소수가 아니거나 소수이지만 최고차항의 계수의 약수가 아닐 때는 기약인지 어떻게 판별할 것인가?

$f(x) \in \mathbb{Z}[x]$가 기약인지 아닌지 판별하는 가장 간단한 방법으로 유리수체 $\mathbb{Q}$위에서 해의 존재유무를 통하여 알 수 있다. 즉, 유리수체 $\mathbb{Q}$위에서 $f(x)$의 해가 존재하면 $f(x)$는 가약이다. 이 방법이 $h(\mathbb{Z})$에서도 성립하는지 확인하여 보자. 먼저 $x^2 + 2x + 1 \in h(\mathbb{Z})$는 기약다항식이다. 하지만 $x^2 + 2x + 1$는 $\mathbb{Q}$위에서 해 $x = -1$를 가진다. 따라서 해가 존재한다고 해서 가약이 되는 것은 아니다. 또한 $2x^2 + 2x + 1 \in h(\mathbb{Z})$는 기약다항식이 아니지만 $\mathbb{Q}$위에서 해를 가지지 않는다. 이를 통해 $f(x) \in h(\mathbb{Z})$가 기약일 조건은 해의 존재성과는 관계가 없음을 알 수 있다.

앞서 다항식환 $\mathbb{Z}[x]$에서는 기약임을 확인할 수 있는 특별한 판정법인 Eisenstein의 기약판정법이 있었다. 이 판정법이 $h(\mathbb{Z})$에서도 적용이 되는지 확인해보자.

정리 4.5 $f(x) \in \mathbb{Z}[x]$이고 r, s는 $f(x)$의 차수보다 작은 두 정수라고 하자. 이때 다음 두 조건은 동치이다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

1. $f(x)$가 $\mathbb{Z}[x]$에서 차수가 각각 r, s인 두 다항식의 곱으로 표현된다.

2. $f(x)$가 $\mathbb{Q}[x]$에서 차수가 각각 r, s인 두 다항식의 곱으로 표현된다.

증명 [3], [7]

참고 $h(\mathbb{Z})$에서는 정리 4.5가 성립함을 알 수 없다.

정리 4.6 다항식 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in h(\mathbb{Z}),\ n \geq 1$ 에 대하여 적당한 소수p 가 존재해서 $p \nmid a_n,\ p|a_{n-1}, \cdots,\ p|a_1,\ p|a_0,\ p^2 \nmid a_0$이면, $f(x)$는 유리수체 $h(\mathbb{Q})$위에서 기약이다.

증명 다항식 $f(x) \in h(\mathbb{Z})$가 $h(\mathbb{Q})$위에서 기약이 아니라고 가정하자. 그러면 $f(x)$는 일차이상의 두 다항식의 곱으로 나타낼 수 있다. 즉, 적당한 $b_s, b_{s-1}, \cdots, b_1, b_0, c_t, c_{t-1}, \cdots, c_1, c_0$에 대하여 다음과 같이 인수분해된다. $f(x) = (b_s x^s + b_{s-1}x^{s-1} + \cdots + b_1 x + b_0)(c_t x^t + c_{t-1}x^{t-1} + \cdots + c_1 x + c_0)$ $(0 < s, t < n,\ \ s + t = n)$
한편, 소수 p에 대하여 $p|a_0, p^2 \nmid a_0$이고 $a_0 = b_0 c_0$이므로 b_0, c_0중에서 단 하나만 p의 배수이다. $p|b_0, p \nmid c_0$라 가정하자. 이 경우에 $a_n = \binom{n}{s} b_s c_t, p \nmid a_n$ 이므로 $p \nmid \binom{n}{s}, p \nmid b_s, p \nmid c_t$이다. 그러므로 $b_0, b_1, \cdots, b_s$에서 $p|b_0, p \nmid b_s$ 이므로 이들 중 처음으로 p의 배수가 아닌 것을 b_r이라고 하면, $p \nmid b_r, 1 \leq r \leq s < n$이다. $a_r = \binom{r}{r} b_r c_0 + \binom{r}{r-1} b_{r-1} c_1 + \cdots + \binom{r}{1} b_1 c_{r-1} + \binom{r}{0} b_0 c_r$ 이고 여기서 $p \nmid b_r, p|b_{r-1}, \cdots, p|b_1, p|b_0$ 이므로 $p \nmid a_r$ 이되어 가정에 모순이다. 따라서 $f(x) \in h(\mathbb{Z})$는 유리수체 $h(\mathbb{Q})$위에서 기약이다.

그 예로 $5x^5 + 6x^2 + 6x + 6 \in h(\mathbb{Z})$의 차수는 최고차항의 계수이므로 기약인지 알 수 없다. 하지만 정리 4.6에 의해 $5x^5 + 6x^2 + 6x + 6$는 $h(\mathbb{Q})$에서 기약임을 알 수 있다.

참고 $\mathbb{Z}[x]$에서는 다항식 $f(x)$가 $\mathbb{Q}$위에서 기약이면 정리 4.5에 의해 $\mathbb{Z}$에서도 기약이다. 이러한 조건을 사용하여 정리 2.12의 Eisenstein의 기약판정법을 통해 $\mathbb{Q}$에서 기약임을 보임으로써 정리 4.5에 의해서 $f(x)$가 $\mathbb{Z}$에서 기약임을 말할 수 있다. 하지만 $h(\mathbb{Z})$에서는 정리 4.5가 성립함을 알 수 없기 때문에 정리 4.6를 통해 f(x)가 $h(\mathbb{Q})$에서 기약이되더라도 $h(\mathbb{Z})$에서는 기약임을 알 수가 없다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

참고 문헌

[1] A. Benhissi, Ideal structure of Hurwitz series ring, Contrib. Alg. Geom. 48 (1997), 251-256.

[2] A. Benhissi and F. Koja, Basic properties of Hurwitz series ring, Ric. Mat. 61 (2012), 255-273.

[3] John B. Fraleigh, First Course in Abstract Algebra 7, Addison Wesley (2002) 강영욱·강병련 옮김, 현대대수학 제7판, 피어슨 코리아 (2009).

[4] W.F. Keigher, Adjunctions and comonads in differential algebra, Pacific J. Math. 59 (1975), 99-112.

[5] W.F. Keigher, On the ring of Hurwitz series, Comm. Algebra 25 (1997), 1845-1859.

[6] Z. Liu, Hermite and PS-rings of Hurwitz series, Comm. Algebra 28 (2000), 299-305.

[7] 김응태 · 박승안, 현대대수학 제8판, 경문사 (2011).

Collection @ chosun