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]I804:24011-200000266738

2018년 2월

교육학석사(수학교육)학위논문

정수환 $\mathbb{Z}$상의 Hurwitz 다항식의 기약성 연구

조선대학교 교육대학원

수학교육전공

서 예 림

조선대학교
CHOSUN UNIVERSITY

정수환 $\mathbb{Z}$상의 Hurwitz 다항식의 기약성 연구

On the irreduciblity of Hurwitz polynomials over $\mathbb{Z}$

2018년 2월

조선대학교 교육대학원

수학교육전공

서 예 림

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

정수환 $\mathbb{Z}$상의 Hurwitz 다항식의 기약성 연구

지도교수 오 동 렬

이 논문을 교육학석사(수학교육)학위 청구논문으로 제출함.

2017년 10월

조선대학교 교육대학원

수학교육전공

서 예 림

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

서예림의 교육학 석사학위 논문을 인준함.

심사위원장 조선대학교 교수 안 영 준 인

심사위원 조선대학교 교수 이 관 규 인

심사위원 조선대학교 교수 오 동 렬 인

2017년 12월

조선대학교 교육대학원

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

CONTENTS

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

ABSTRACT

On the irreduciblity of Hurwitz polynomials over $\mathbb{Z}$

Seo, Ye Lim
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 commutative ring theory. As generalizations of formal power series and polynomial rings, semigroup rings and graded rings are investigated. As another point of view of generalization of formal power series and polynomial rings, Keigher introduced Hurwitz power series rings and Hurwitz polynomial rings, respectively. Affer keigher many researches on the ring of Hurwitz power series and polynomial rings have been done. In this thesis, we introduce a Hurwitz polynomial ring and study the irreduciblity of Hurwitz polynomials over $\mathbb{Z}$ We also investigate the irreduciblilty of Hurwitz polynomials of higher degree greater than equal to 3 over the ring of integers. More precisely, by using a relation between Hurwitz polynomial over the ring of integers and usual polynomials over the ring of integers, we give a necessary and sufficient condition for Hurwitz polynomials of higher degree greater than equal to 3 over the ring of integers to be irreducible.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

제 1 장 소 개

단위원을 갖는 가환환(*commutative ring with unity*) 상에서 계수를 갖는 형식적 멱급수 환(*formal power series ring*) 과 다항식 환(*polynomial ring*)은 대수학 및 가환환 이론의 중요한 연구 대상중 하나이며 많은 응용성을 갖고 있다. 형식적 멱급수 환 및 다항식 환에 대한 연구는 1950년대부터 많은 수학자들에 의하여 활발히 이루어지고 있으며, 특히 다항식 환을 일반화한 반군 환(*semigroup ring*)과 등급 환(*graded ring*)에 대한 연구는 1970년대 후반부터 활발히 이루어지고 있다. 1980년대 중반부터 분수 체 K 를 갖는 정역 D에 대하여 두 다항식 환 $D[X]$와 $K[X]$사이에 존재하는 다항식 환의 연구를 위하여 합성 다항식 환이 소개 되었다. 즉 가환 환 D를 가환 환 R 의 확장(즉 $R \subseteq D$)이라 할 때, 합성 다항식 환 $R+XD[X]=\{f(x)\in D[X] \mid f(0)\in R\}$ 이 소개 되고 이에 대한 연구가 활발히 진행되고 있으며, 이를 확장한 합성 반군 환에 대한 연구 또한 현재까지 활발히 진행되고 있다.

1976년 Keigher [4]에 의하여 변형된 형식적 멱급수 환과 다항식 환이 소개되었으며, 이후 [5]에서 이 들을 Hurwitz 멱급수 환 및 다항식 환(*Hurwitz power serie ring*, *Hurwitz polynomial ring*)이라 이름 지었다. 1997년 이후 Hurwitz 멱급수 환 및 다항식 환에 대하여 기존의 멱급수 환 및 다항식환의 성질과 비교 분석한 많은 연구들이 이루어졌다 [1],[2],[8]. 특히 최근에 [6],[7]에서 네더리안 및 주 아이디얼에 대한 오름 사슬 조건을 만족하는 합성 Hurwitz 멱급수 환 및 다항식 환이 연구되어졌다. 또한 정학진 [10]의 연구 결과에서 정수 계수를 갖는 Hurwitz 다항식의 기약성에 대한 연구가 이루어졌다. 정확히 말하면 2차 정수 계수를 갖는 다항식의 잘 알려진 기약성을 이용하여 2차 정수 계수를 갖는 Hurwitz 다항식이 기약다항식이 되기 위한 동치조건을 규명하였다. Hurwitz 멱급수 환 및 다항식 환은 특별한 무게(weight)를 두 멱급수 또는 두 다항식의 곱셈의 계수에 주는 것으로 반군 환과는 다른 관점으로 기존의 멱급수 환과 다항식 환을 일반화한 것이다.

이 논문에서는 Hurwitz 다항식 환에 대한 간단한 성질을 소개하고 기존의 정수 계수를 갖는 다항식 환의 성질을 이용하여 정수 계수를 갖는 Hurwitz 다항식의 성질을 분석하였다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

2장에서는 다항식 환에 대한 잘 알려진 내용들을 간단히 소개 하고, 3장에서는 Hurwitz 다항식 환과 그 다항식 환의 간단한 대수적 성질들을 소개한다.
특히 4장에서는 정학진 [10]의 연구 결과를 확장하여 3차 이상의 정수 계수를 갖는 Hurwitz 다항식의 기약성을 소개한다. 특히 계수가 정수인 다항식의 기약성을 이용하여 계수가 정수인 Hurwitz 다항식의 기약성을 규명한다.
구체적으로 계수가 정수인 3차 Hurwitz 원시 다항식 $f(x)=a_3x^3+a_2x^2+\cdots+a_0$ 의 경우 $3\nmid a_3$이면 $f(x)$는 항상 기약 다항식이 됨을 보인다. 또한 $3|a_3$인 경우 특수한 조건을 만족하는 계수가 정수인 다항식을 이용해 $f(x)$가 기약 다항식이 되는 동치 조건들을 소개한다.
계수가 정수인 4차 Hurwitz 원시다항식 $f(x)=a_4x^4+a_3x^3+\cdots+a_0$ 의 경우 $4\nmid a_4$이고 $6\nmid a_4$이면 $f(x)$는 항상 기약 다항식이 됨을 보인다. 또한 $4|a_4$ 또는 $6|a_4$ 인 경우 특수한 조건을 만족하는 계수가 정수인 다항식을 이용해 $f(x)$가 기약 다항식이 되는 동치 조건들을 소개한다.
더 나아가 계수가 정수인 n차 Hurwitz 원시 다항식 $f(x)=a_nx^n+\cdots+a_ix^i+\cdots+a_0$ 의 경우 특수한 조건을 만족하는 계수가 정수인 다항식을 이용해 $f(x)$가 기약 다항식이 되는 동치 조건을 소개한다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

제 2 장 다항식환

이 장에서는 다항식환의 기본적인 정의와 성질 등을 소개한다.
이 장의 대부분의 결과들은 [3],[9]를 참고 하였으므로 증명은 가급적 생략하도록 하되 필요한 경우에만 간단하게 증명하도록 하겠다.

(정의 2.1) 공집합이 아닌 집합 R위에서 덧셈 $+$ 과 곱셈 $\cdot$ 이 정의되어 다음이 성립할 때, $(R, +, \cdot)$을 환$(ring)$ 이라고 한다. 임의의 $a, b, c \in R$에 대하여

1. $(R, +)$는 덧셈군이다.
   1) $(a+b)+c = a+(b+c)$ (결합법칙)
   2) $a+b = b+a$ (교환법칙)
   3) $a+0 = 0+a = a$인 원소 $0 \in R$ 이 존재 한다.
   4) $a+(-a) = (-a)+a = 0$ 인 a의 덧셈에 관한 역원 $-a \in R$ 이 존재한다.
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (결합법칙)
3. $a \cdot (b+c) = a \cdot b + a \cdot c$, $(a+b) \cdot c = a \cdot c + b \cdot c$ (분배법칙)

환$(R,+, \cdot)$을 덧셈과 곱셈에 대해 혼돈이 없을시 간단히 환R으로 표현한다.

(정의 2.2) 환 R에서 모든 원소 $a, b \in R$에 대하여 다음을 만족하면

$$a \cdot b = b \cdot a$$

R을 가환환$(commutative\ ring)$이라고 한다.

환에서 덧셈 항등원은 0으로 나타내고 곱셈 항등원(또는 단위원)은 1로 나타내도록 하며 덧셈 항등원과 곱셈항등원이 서로 다른 환만 다루도록 한다. 또한 앞으로 환 R의 임의의 $a, b \in R$의 곱 $a \cdot b$는 간략히 ab로 나타내도록 하자.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

(정의 2.3) 단위원 1 을 가진 가환환 R에서 임의의 $a,b \in R$에 대하여 다음이 만족하면

$$ab = 0 \Rightarrow a = 0 \text{ or } b = 0$$

R을 정역($integral\ domain$) 이라고 한다.

(정의 2.4) 단위원 1을 가진 가환환 R에서 영이 아닌 원소 $a \in R$에 대하여

$$ab = ba = 1$$

을 만족하는 $b \in R$이 존재 할 때, a 를 R의 단원($unit\ element$) 이라고 한다.
특히 b를 a의 역원($inverse$)이라고 하며 기호로는 $b = a^{-1}$ 으로 표현한다.

이때 단위원 1을 가진 가환환 R의 단원들의 집합은 다음과 같은 성질을 갖는다.

(정리 2.5) 단위원 1을 가진 가환환 R에서 단원 전체의 집합은 기호 $U(R)$로 표현하고 $U(R)$은 곱셈군을 이룬다.

증명 1) $1 \cdot 1 = 1$ 이므로 $1 = 1^{-1}$ 이다. 즉 $1 \in U(R) \neq \varnothing$ 이다. 또한 임의의 $a, b \in R$ 에 대해
$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$, $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = 1$
이 성립한다. 그러므로 $(ab)^{-1} = b^{-1}a^{-1}$ 의해 $ab \in U(R)$이다. $U(R)$은 곱셈에 대해 닫혀 있다.

2) $U(R) \subset R$ 이므로 결합법칙을 성립한다.

3) $1 \in U(R)$ 이 존재해서 $a \cdot 1 = 1 \cdot a = a$ 가 성립한다.

4) 임의의 $a \in R$ 에 대해 $aa^{-1} = a^{-1}a = 1$ 이므로 $a^{-1} \in U(R)$이 성립한다. 이때 역으로 a^{-1}의 역원은 a 이므로 $a \in U(R)$이 성립한다.

그러므로 1),2),3),4) 에 의해서 $U(R)$은 곱셈군을 이룬다. 이때, 단위원 1을 가진 가환환 R에서 $U(R)$을 R의 단원군($unit\,group$) 이라 한다. ■

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

(정의 2.6) 단위원 $1(\neq 0)$을 갖는 환 R에서

$$m \cdot 1 = 1+1+\cdots+1 = 0 \qquad (1\text{이 } m\text{개})$$

을 만족하는 양의 정수 m이 존재할 때, 위 조건을 만족하는 가장 작은 양의 정수 n을 환 R의 표수($characteristic$)라고 한며 기호로는 $ch(R) = n$ 이라 표현 한다. 한편, 모든 양의 정수 $m \in R$ 에 대해 $m \cdot 1 \neq 0$ 일 때, R을 표수가 0인 환이라고 한다.

(정의 2.7) 환 R과 부정원 x를 이용해 만든 다음 형태의 형식적인 무한합의 꼴을 R위의 다항식($polynomial$) 이라고 한다.

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots \qquad (a_i \in R)$$
$$(\text{유한개를 제외한 모든 } i\text{에 대하여 } a_i = 0)$$

이때 $i > n$ 인 모든 i에 대해 $a_i = 0$ 일 때

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

으로 표현되고, R위의 x에 관한 모든 다항식 전체의 집합을 기호로 $R[x]$라고 한다.

위의 정의에서 각각의 $a_0, a_1x, \cdots, a_nx^n$을 $f(x)$의 항($term$) 이라고 하며, a_0를 상수항이라고 한다. 또한 각항들에서 $a_0, a_1, \cdots, a_n$ 들은 $f(x)$의 계수($coefficient$)라고 하며, x^k의 계수는 a_k라고 한다. $(0 \leq k \leq n)$ 또한 다항식 중에서 상수항을 제외한 모든 계수가 0인 다항식$f(x) = a_0$ 를 상수다항식($constant\ polynomial$)이라고 하며 모든 계수가 0인 다항식$f(x) = 0$ 을 영다항식($zero\ polynomial$) 이라고 한다. $a_0 \in R$ 에 대하여 상수다항식 $f(x) = a_0 \in R[x]$ 으로 표현되므로 $R \subseteq R[x]$ 으로 생각한다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

(정리 2.8) 환 R위의 다항식 전체의 집합 $R[x]$에서, 덧셈 $+$ 과 곱셈 $\cdot$ 을 다음과 같이 정의 할 때, $R[x]$는 환을 이루고 환 $R[x]$를 R위의 다항식환(*polynomial ring*)이라고 하며 기호로는 $R[x]$ 로 표현된다.

$R[x]$에 속하는 임의의 두 다항식 $f(x), g(x)$

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \in R[x], (n \le m)$$

에 대하여

$$f(x) + g(x) := b_m x^m + \cdots + (b_n + a_n)x^n + \cdots + (b_1 + a_1)x + (b_0 + a_0)$$

$$f(x)g(x) := c_{n+m}x^{n+m} + \cdots + c_k x^k + \cdots + c_1 x + c_0$$

$$(c_k = \sum_{t=0}^{k} a_t b_{k-t} = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1}b_1 + a_k b_0)$$

증명 [3]의 정리 22.2 , [9]의 정리 3.5.2 참조 ■

(정의 2.9) 환 R위의 다항식

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \ , \ n \ge 0 \ , \ a_n \ \ne 0$$

에서 n을 $f(x)$의 차수(degree)라고 하고 기호로는 $\deg(f(x)) = n$ 으로 표시한다.
특히 a_n은 $f(x)$의 최고차항의 계수(*leading coefficient*)라고 한다.
특히 $a_n = 1$일 때 $f(x)$를 모닉 다항식(*monic polynomial*)이라고 한다.

(정리 2.10) 정역R의 표수는 0또는 소수 이다.

증명 만약 정역 R의 표수가 합성수인 n이라고 하자.
이때, $n = mk$, $1 < m \le k < n$ 이라고 하면,
정의 2.6 에 의해 $0 = 1 \cdot n = 1 \cdot (m \cdot k) = (1 \cdot m)(1 \cdot k)$이 성립하고 n이 표수이므로 n 보다 작은 m , k에 대하여 $1 \cdot m \ \ne 0$, $1 \cdot k \ \ne 0$ 인 모순이 생긴다.
■

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

(정의 2.11) 정역 D에서 영이 아니고 단원도 아닌 원소 p에 대해

$$p = ab \quad \Rightarrow \quad a \in U(D) \text{ or } b \in U(D)$$

일 때, p를 D의 기약($irreducible$) 이라 한다.

참고 정역 D상의 다항식환 $D[x]$에서 다항식 $f(x)$가 기약이면 $f(x)$를 기약다항식($irreducible\ \ polynomial$)이라고 한다. 또한 기약다항식이 아닌 경우 가약다항식($reducible\ polynomomial$)이라고 한다.

(정의 2.12) 정수환 $\mathbb{Z}$ 위의 최고차항의 계수가 0이 아닌 다항식

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x],\ n \geq 1$$

에서 모든 계수들의 최대공약수 $\gcd(a_n, a_{n-1}, \cdots, a_1, a_0)$를 $f(x)$의 내용($content$) 라고 한다. 기호 $c(f)$ 로 나타낸다.
특히 $c(f) = 1$ 이면, $f(x)$를 원시다항식($primitive\,polynomial$) 이라고 한다.

(정리 2.13) (Gauss의 보조정리) 정수환 $\mathbb{Z}$ 위의 두 원시다항식

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \in \mathbb{Z}[x]$$

에 대해 곱 $f(x)g(x)$도 정수환 $\mathbb{Z}$ 위에서 원시다항식이다.

증명 [9]의 정리 6.7.12 참조 ■

다음 정리 2.14는 잘 알려져 있는 내용이지만 제 4장의 '정수환 $\mathbb{Z}$상의 $h(\mathbb{Z})$의 기약다항식과 $\mathbb{Z}[x]$의 기약다항식 사이의 관계' 에서 중요한 역할을 하므로 증명하도록 하겠다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

(정리 2.14) 정수환 $\mathbb{Z}$ 위에서 $\deg(f(x)) = n \geq 1$ 인 다항식 $f(x) \in \mathbb{Z}[x]$가 유리수체 $\mathbb{Q}$위에서

$$f(x) = g(x)h(x) \ , \ 1 \leq \deg(g(x)) = s < n \ , \ 1 \leq \deg(h(x)) = r < n$$

로 인수분해 된다고 할 때, $f(x)$는 정수환 $\mathbb{Z}$ 위에서 다음과 같이 인수분해 된다.

$$f(x) = c(f)g_1(x)h_1(x) \ , \ \deg(g_1(x)) = s \ , \ \deg(h_1(x)) = r$$

더욱이 $f(x)$가 모닉 다항식이면 $g_1(x)$과 $h_1(x)$은 모닉 다항식이다.

증명 적당한 정수 $a_i, b_i, c_j, d_j \in \mathbb{Z}$, $b_i \geq 1$, $d_j \geq 1$ 에 대하여

$$g(x) = \sum_{i=0}^{r} \frac{a_i}{b_i} x^i \in \mathbb{Q}[x], \ h(x) = \sum_{j=0}^{s} \frac{c_j}{d_j} x^j \in \mathbb{Q}[x]$$

이라고 하고 $b = b_0 b_1 \cdots b_{r-1} b_r \geq 1$, $d = d_0 d_1 \cdots d_{s-1} d_s \geq 1$ 에 대해

$$g_0(x) = bg(x) \ , \ h_0(x) = dh(x)$$

이라고 하면, $g_0(x), h_0(x) \in \mathbb{Z}[x]$이고 $g_o(x)h_0(x) = bg(x)dh(x) = bdf(x)$ 가 성립한다. 또한

$$f_1(x) = \frac{1}{c(f)} f(x) \ , \ g_1(x) = \frac{1}{c(g_0)} g_0(x) \ , \ h_1(x) = \frac{1}{c(h_0)} h_0(x)$$

이라고 하면 다항식 $f_1(x)$, $g_1(x)$, $h_1(x) \in \mathbb{Z}[x]$ 는 원시 다항식이다. 또한

$$f(x) = c(f)f_1(x) \ , \ g_0(x) = c(g)g_1(x) \ , \ h_0(x) = c(h_0)h_1(x)$$

이고 가정에 의해

$$bdf(x) = g_0(x)h_0(x) = c(g_0)g_1(x)c(h_0)h_1(x) \ , \ bdf(x) = bdc(f)f_1(x)$$

이므로

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$bdc(f)f_1(x) = c(g_0)c(h_0)g_1(x)h_1(x)$$

가 성립한다. 또한 정리 2.13 에 의해서 $g_1(x)h_1(x)$는 원시 다항식이므로

$$bdc(f) = c(g_0)c(h_0)\ ,\ f_1(x) = g_1(x)h_1(x)$$

가 성립하다. 따라서 $f(x) = c(f)g_1(x)h_1(x)$ 이다. ■

특히 $f(x)$가 원시다항식인 $f(x) \in \mathbb{Z}[x], \deg(f(x)) \geq 1$인 경우 정리 2.14에 의해서 다음 따름정리 2.15이 성립함을 쉽게 알 수 있다.

(따름정리 2.15) 정수환 $\mathbb{Z}$ 위에서 $\deg(f(x)) = n \geq 1$ 인 원시다항식 $f(x) \in \mathbb{Z}[x]$에 대해서 다음 두 조건이 동치이다.

1. $f(x) \in \mathbb{Z}[x]$가 정수환 $\mathbb{Z}$ 위에서 기약이다.
2. $f(x) \in \mathbb{Z}[x]$가 유리수체 $\mathbb{Q}$ 위에서 기약이다.

참고 다항식 $f(x) \in \mathbb{Z}[x]$가 원시다항식 아닌 경우 따름정리 2.15은 성립하지 않는다.

$$\begin{aligned} f(x) &= 2x^2 + 2 \in \mathbb{Z}[x] \\ &= 2\,(x^2 + 1) \end{aligned}$$

위와 같은 경우 $2 \in U(\mathbb{Q})$ 이므로 $f(x)$는 유리수체 $\mathbb{Q}$위에서 기약이 아니지만 $2 \notin U(\mathbb{Z})$ 이기 때문에 $f(x)$는 정수환 $\mathbb{Z}$ 위에서 기약이다. 즉 원시다항식이라는 조건을 주지 않으면 따름정리 2.15에 만족하지 않는 예시가 생긴다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

제 3 장 Hurwitz 다항식의 정의 및 성질

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

환 R에서 계수를 갖는 다항식 집합 $R[x]$에 두 연산 $+$, $*$ 을 다음과 같이 정의한다. 환 R위의 임의의 두 다항식 $f(x), g(x)$

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \,, (n \le m)$$

에 대하여

$$f(x) + g(x) := b_m x^m + \cdots + (b_n + a_n)x^n + \cdots + (b_1 + a_1)x + (b_0 + a_0)$$

$$f(x) * g(x) := c_{n+m}x^{n+m} + \cdots + c_i x^i + \cdots + c_1 x + c_0$$

$$(c_i = \sum_{t=0}^{i} \binom{i}{t} a_t b_{i-t} = \binom{i}{0} a_0 b_i + \cdots + \binom{i}{k} a_k b_{i-k} + \cdots + \binom{i}{i} a_i b_0 \,, k \le i)$$

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

증명 [5]참조 ■

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

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

한편 가환환 R에 대한 $R[x]$의 대수적 성질은 많이 알려진 반면 $h(R)$에 대한 대수적 성질은 잘 알려져 있지 않으므로 $h(R)$에 대해 간단히 살펴보도록 하자.

(정리 3.2) 곱셈항등원 1을 가진 가환환 R에서 다음 두 조건은 동치이다.

1. R은 표수가 0인 정역이다.
2. $h(R)$은 정역이다.

증명 [10]의 정리 3.2의 내용을 참조 하였고 다시 한번 증명 하도록 한다.
(1)⟹(2) 임의의 $f(x), g(x) \in h(R)$에 대하여
$f(x) = a_n x^n + \cdots + a_i x^i + \cdots + a_0$, $g(x) = b_m x^m + \cdots + b_j x^j + \cdots + b_0$
$(\deg(f(x)) = n, \deg(g(x)) = m,\ n, m \neq 0)$이라 하면
$f(x) * g(x) = c_{n+m} x^{n+m} + \cdots + c_k x^k + \cdots + c_0$ 이다.
이때

$$c_{n+m} = \binom{n+m}{0} a_0 b_{n+m} \cdots + \binom{n+m}{n-1} a_{n-1} b_{m+1}$$
$$+ \binom{n+m}{n} a_n b_m + \binom{n+m}{n+1} a_{n+1} b_{m-1} + \cdots + \binom{n+m}{n+m} a_{n+m} b_0$$

$$a_{n+1} = a_{n+2} = \cdots = a_{n+m} = 0,\ b_{m+1} = b_{m+2} = \cdots = b_{n+m} = 0$$

이므로 $c_{n+m} = \binom{n+m}{n} a_n b_m$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.

(2)⟹(1) 다항식환 $h(R)$을 정역이라 하자.
ⅰ) 가환환 R은 정역이다.
가환환 $R \subset h(R)$이므로 임의의 $a, b \in R$ 에 대하여 $a, b \in h(R)$이다. 또한 $a \cdot b = a * b = 0$이 성립 하고 $h(R)$은 정역이므로 $a = 0$ 이거나 $b = 0$ 이다. 그러므로 R은 정역이다.

ⅱ) 가환환 R의 표수는 0이다.
만약 $ch(R) \neq 0$ 하자. ⅰ) 에 따르면 R은 정역이므로 정리 2.10에 의해 $ch(R) = p$ (p:소수) 이다. 영 다항식이 아닌 $x, x^{p-1} \in h(R)$에 대하여

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$x * x^{p-1} = \binom{p}{1} x^p = px^p = (p \cdot 1)x^p = 0$$

이므로 $h(R)$은 정역이 아닌 모순이 생긴다. 그러므로 정역 R의 표수가 0이다.

i), ii)에 의해 $h(R)$을 정역이라 하면 R은 표수가 0인 정역이다. ■

(정리 3.3) 표수가 0인 정역R에 대하여 다음이 성립한다.

$$U(h(R)) \ = \ U(R)$$

증명 영 다항식이 아닌 두 다항식 $f(x), g(x) \in U(h(R))$가 존재한다고 하자.
$f(x) * g(x) = g(x) * f(x) = 1$, $h(R)$은 정역이므로
$\deg(1) = \deg(f(x) * g(x)) = \deg(f(x)) + \deg(g(x)) = 0$
즉, $\deg(f(x)) = \deg(g(x)) = 0$ 이므로, $f(x)$와 $g(x)$는 상수 다항식이다.
또한 $f(x) * g(x) = g(x) * f(x) = 1$ 이므로, $f(x)$, $g(x) \in U(R)$이다. ■

Hurwitz 다항식환의 기약일 조건은 정의 2.13와 정리 3.2에 의해 알 수 있다. 즉, $ch(R) = 0$, 정역인 R 위의 $h(R)$에서 영다항식이 아니고 단원도 아닌 다항식 $f(x)$에 대해

$$f(x) \ = \ g(x) * h(x) \Rightarrow g(x) \in U(h(R)) \text{ or } h(x) \in U(h(R)) \quad (g(x), h(x) \in h(R))$$

일 때 다항식 $f(x)$가 $h(R)$의 기약이라 한다. 혹은 $f(x)$를 $h(R)$에서의 기약다항식이라고 한다.

한편 정리 3.3에 의해 $U(h(\mathbb{Z})) = U(\mathbb{Z}) = \{-1, 1\}$이므로 간단한 사실을 알 수 있다.
다항식 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_i x^i + \cdots + a_1 x + a_0 \in h(\mathbb{Z})$에 대해
$\gcd(a_n, a_{n-1}, \cdots, a_i, \cdots, a_1, a_0) = d \neq 1$ 이면 $f(x)$는 다음과 같이 나타난다.

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_i x^i + \cdots + a_1 x + a_0$$

$$= d * (a_n{}' x^n + a_{n-1}{}' x^{n-1} + \cdots + a_i{}' x^i + \cdots + a_1{}' x + a_0{}'), (a_i = d a_i{}')$$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

이때 d , $(a_n{}'x^n + a_{n-1}{}'x^{n-1} + \cdots + a_i{}'x^i + \cdots + a_1{}'x + a_0{}') \not\in U(h(\mathbb{Z}))$ 이다.
따라서 원시 다항식이 아닌 다항식 $f(x)$가 $h(\mathbb{Z})$에서 기약이 아님을 알 수 있다.

그러므로 $h(\mathbb{Z})$위에서 기약을 판별 할 때 원시다항식 에서만 확인하자.

(정리 3.4) 원시다항식

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_i x^i + \cdots + a_1 x + a_0 \in h(\mathbb{Z}) \text{ , } (n \geq 2, a_n \neq 0)$$

에 대하여 $|a_n| < n$ 이면, 다항식 $f(x)$는 $h(\mathbb{Z})$에서 기약이다.

증명 만약, $|a_n| < n$ 일 때, $f(x)$가 $h(\mathbb{Z})$에서 기약이 아니라고 하자.
$f(x)$가 $h(\mathbb{Z})$위에서 기약이 아닌 원시다항식이므로 $f(x)$는 상수다항식이 아닌
적당한 두 다항식
$(b_s x^s + b_{s-1}x^{s-1} + \cdots + b_1 + b_0), (c_m x^m + c_{m-1}x^{m-1} + \cdots + c_1 + c_0) \in h(\mathbb{Z})$,
$s + m = n$, $(1 \leq s, m \leq n)$ 존재해서 $f(x)$는 다음과 같이 나타난다. $(b_s , c_m \neq 0)$

$$\begin{aligned} f(x) &= (b_s x^s + b_{s-1}x^{s-1} + \cdots + b_1 + b_0) * (c_m x^m + c_{m-1}x^{m-1} + \cdots + c_1 + c_0) \\ &= \binom{s+m}{s} b_s c_m x^{s+m} + \cdots + \sum_{k=0}^{i} \binom{i}{k} b_k c_{m-k} x^i + \cdots + (b_1 c_0 + b_0 c_1)x + b_0 c_0 \\ &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_i x^i + \cdots + a_1 x + a_0 \end{aligned}$$

즉,

$$a_n = \binom{s+m}{s} b_s c_m = \binom{n}{s} b_s c_m \text{ , } n \leq \binom{n}{s}, 1 \leq |b_s|, 1 \leq |c_m|$$

그러므로

$$\binom{n}{s} |b_s||c_m| = \left|\binom{n}{s} b_s c_m\right| = |a_n| \geq n$$

따라서 $|a_n| < n$ 에 대한 모순이 생긴다. 그러므로 $f(x)$는 $h(\mathbb{Z})$에서 기약이다. ■

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

(정리 3.5) 소수 p에 대해 $\deg(f(x)) = p^n$인 원시다항식

$$f(x) = a_{p^n}x^{p^n} + \cdots + a_i x^i + \cdots + a_0 \in h(\mathbb{Z})$$

에 대하여 $a_{p^n} \neq 0$, $p \nmid a_{p^n}$ 이면, 다항식 $f(x)$는 $h(\mathbb{Z})$에서 기약이다.

증명 만약 $p \nmid a_{p^n}$ 일 때 $f(x)$가 $h(\mathbb{Z})$에서 기약이 아니라고 하자.
$f(x)$가 $h(\mathbb{Z})$위에서 기약이 아닌 원시다항식이므로 $f(x)$는 상수다항식이 아닌 적당한 두 다항식

$$(b_s x^s + b_{s-1}x^{s-1} + \cdots + b_1 + b_0), (c_m x^m + c_{m-1}x^{m-1} + \cdots + c_1 + c_0) \in h(\mathbb{Z}),$$

$s + m = p^n$ 존재해서 $f(x)$는 다음과 같이 나타난다. $(b_s , c_m \neq 0)$

$$\begin{aligned} f(x) &= (b_s x^s + b_{s-1}x^{s-1} + \cdots + b_1 + b_0) * (c_m x^m + c_{m-1}x^{m-1} + \cdots + c_1 + c_0) \\ &= \binom{s+m}{s} b_s c_m x^{s+m} + \cdots + \sum_{k=0}^{i} \binom{i}{k} b_k c_{m-k} x^i + \cdots + (b_1 c_0 + b_0 c_1)x + b_0 c_0 \\ &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_i x^i + \cdots + a_1 x + a_0 \end{aligned}$$

즉,

$$a_n = \binom{s+m}{s} b_s c_m = \binom{p^n}{s} b_s c_m \ , \ p \mid \binom{p^n}{s}$$

이므로

$$p \mid a_{p^n}$$

따라서 $p \nmid a_{p^n}$ 에 대한 모순이 생긴다. 그러므로 다항식 $f(x)$가 $h(\mathbb{Z})$에서 기약이다. ■

(따름 정리 3.6) 소수 p에 대해 $\deg(f(x)) = p$ 인 원시다항식

$$f(x) = a_p x^p + \cdots + a_i x^i + \cdots + a_0 \in h(\mathbb{Z})$$

에 대하여 $a_p \neq 0$, $p \nmid a_p$ 이면, 다항식 $f(x)$는 $h(\mathbb{Z})$에서 기약이다.

증명 정리 3.5에서 $n = 1$일 때 [10]의 정리 4.4를 따름정리로 얻을 수 있다. ■

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

제 4 장 정수환 $\mathbb{Z}$상의 $h(\mathbb{Z})$의 기약다항식과 $\mathbb{Z}[x]$의 기약다항식 사이의 관계

이 장에서는 정수계수를 갖는 Hurwitz 다항식의 기약판별법을 알아보도록 하자. 다항식 $f(x) \in \mathbb{Z}[x]$에 대한 인수분해는 다루기 쉬우므로, $f(x) \in \mathbb{Z}[x]$의 기약성을 이용하여 Hurwitz 다항식의 기약성을 살펴보도록 하자.

임의의 $a \in \mathbb{Z}$에 대해 $a = pq = p * q = a$ 이 성립하므로 계수가 정수인 상수다항식은 $h(\mathbb{Z})$와 $\mathbb{Z}[x]$에서 모두 기약이거나 기약이 아니다. 이와 마찬가지로 임의의 a_1 , $a_0 \in \mathbb{Z}$ 에 대하여 $(a_1 \neq 0)$

$$b(c_1 x + c_0) = bc_1 x + bc_0 = a_1 x + a_0 = bc_1 x + bc_0 = \binom{1}{0} bc_1 x + \binom{0}{0} bc_0 = b * (c_1 x + c_0)$$

가 성립하므로 계수가 정수인 일차다항식은 $h(\mathbb{Z})$와 $\mathbb{Z}[x]$에서 모두 기약 이거나 기약이 아니다. 정수계수를 갖는 2차 Hurwitz 다항식의 기약성에 대한 연구결과는 [10]의 정리 4.3에 잘 나와 있으나 이 논문의 완비성을 위하여 간단히 언급하도록 하자.

원시다항식 $f(x) = a_2 x^2 + a_1 x + a_0 \in h(\mathbb{Z})$는 정리 3.5에 의해 $2 \nmid a_2$이면 기약이므로 $2 | a_2$인 경우를 살펴보도록 하자.

(정리 4.1) 임의의 a_2 , a_1 , $a_0 \in \mathbb{Z}$ 에 대해 $a_2 \neq 0$, $\gcd(2a_2 , a_1 , a_0) = 1$ 이면, 다음 두 조건은 동치이다.

1. $f(x) = 2a_2 x^2 + a_1 x + a_0 \in h(\mathbb{Z})$에서 기약이다.
2. $g(x) = a_2 x^2 + a_1 x + a_0 \in \mathbb{Z}[x]$에서 기약이다.

증명 [10]의 정리 4.3 참조 ■

2차 원시다항식 $g(x) = a_2 x^2 + a_1 x + a_0 \in \mathbb{Z}[x]$의 경우 정수해의 존재유무로 $g(x)$의 기약성을 쉽게 알 수 있다. 그러므로 정리 3.5와 정리 4.1에 의하여 정수 계수를 갖는 2차 Hurwitz 원시 다항식 $f(x) = a_2 x^2 + a_1 x + a_0 \in h(\mathbb{Z})$의 경우의 기약성을 쉽

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

게 알 수 있다.

정수계수를 갖는 3차 Hurwitz 다항식의 기약성에 대해 알아보도록 하자.
다항식 $f(x)=a_3x^3+a_2x^2+a_1x+a_0 \in h(\mathbb{Z})$는 정리 3.5에 의해 $3 \nmid a_3$이면 기약이므로 $3 \mid a_3$인 경우 $f(x)$의 기약성에 대해 알아보도록 하자.

(정리 4.2) 임의의 $a_3, a_2, a_1, a_0 \in \mathbb{Z}$ 에 대해, $a_3 \neq 0$, $\gcd(3a_3, a_2, a_1, a_0)=1$, $2|a_3, 2|a_2$ 이면 다음 두 조건이 동치이다.

1. $f(x) = 3a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$ 에서 기약이다.
2. $g(x) = \frac{1}{2}a_3x^3 + \frac{1}{2}a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ 에서 기약이다.

증명 (1)⇒(2)다항식 $f(x)$가 $h(\mathbb{Z})$ 에서 기약 일 때 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약이 아니라고 하자. $\gcd(3a_3, a_2, a_1, a_0)=1$이면 $\gcd(\frac{1}{2}a_3, \frac{1}{2}a_2, a_1, a_0)=1$ 이다. $g(x)$가 $\mathbb{Z}[x]$위에서 기약이 아닌 원시다항식이므로 $g(x)$는 상수다항식이 아닌 두 개의 정수환다항식의 곱으로 표현된다.
그러므로 적당한 $b_1, b_0, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $g(x)$는 다음과 같이 나타난다.

$$\begin{aligned} g(x) &= (b_1x+b_0)(c_2x^2+c_1x+c_0) \quad (b_1 \neq 0, c_2 \neq 0) \\ &= b_1c_2x^3 + (b_1c_1+b_0c_2)x^2 + (b_1c_0+b_0c_1)x + b_0c_0 \\ &= \frac{1}{2}a_3x^3 + \frac{1}{2}a_2x^2 + a_1x + a_0 \end{aligned}$$

따라서,

$$a_3 = 2b_1c_2, a_2 = 2(b_1c_1+b_0c_2), a_1 = (b_1c_0+b_0c_1), a_0 = b_0c_0 \quad -①$$

이때 식 ①을 $f(x)$의 계수에 대입하면, $f(x)$는 다음과 같이 나타난다.

$$\begin{aligned} f(x) &= 3a_3x^3 + a_2x^2 + a_1x + a_0 \\ &= 3(2b_1c_2)x^3 + 2(b_1c_1+b_0c_2)x^2 + (b_1c_0+b_0c_1)x + b_0c_0 \end{aligned}$$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$= \binom{3}{1} b_1 (2c_2) x^3 + \left(\binom{2}{1} b_1 c_1 + \binom{2}{0} b_0 (2c_2) \right) x^2 + \left(\binom{1}{1} b_1 c_0 + \binom{1}{0} b_0 c_1 \right) x + \binom{0}{0} b_0 c_0$$

$$= (b_1 x + b_0) * (2c_2 x^2 + c_1 x + c_0) \in h(\mathbb{Z})$$

이는 $f(x)$가 기약이라는 가정에 모순이 생긴다. 따라서 $f(x)$가 $h(\mathbb{Z})$에서 기약일 때 $g(x)$가 $\mathbb{Z}[x]$에서 기약 이다.

(2)⟹(1) 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약 일 때, 다항식 $f(x)$가 $h(\mathbb{Z})$에서 기약이 아니라고 하자. $f(x)$는 $h(\mathbb{Z})$위에서 기약이 아닌 원시다항식 이므로 $f(x)$는 상수다항식이 아닌 두 개의 Hurwitz다항식의 곱으로 표현된다.
그러므로 적당한 $b_1, b_0, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $f(x)$는 다음과 같이 나타난다.

$$f(x) = (b_1 x + b_0) * (c_2 x^2 + c_1 x + c_0) \qquad (b_1 \neq 0, c_2 \neq 0)$$

$$= \binom{3}{1} b_1 c_2 x^3 + \left(\binom{2}{1} b_1 c_1 + \binom{2}{0} b_0 c_2 \right) x^2 + \left(\binom{1}{1} b_1 c_0 + \binom{1}{0} b_0 c_1 \right) x + \binom{0}{0} b_0 c_0$$

$$= 3b_1 c_2 x^3 + (2b_1 c_1 + b_0 c_2) x^2 + (b_1 c_0 + b_0 c_1) x + b_0 c_0$$

$$= 3a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

따라서,

$$a_3 = b_1 c_2, a_2 = (2b_1 c_1 + b_0 c_2), a_1 = (b_1 c_0 + b_0 c_1), a_0 = b_0 c_0 \quad -②$$

이때 식 ②를 $g(x)$의 계수에 대입하면, $g(x)$는 다음과 같이 나타난다.

$$g(x) = \frac{1}{2} a_3 x^3 + \frac{1}{2} a_2 x^2 + a_1 x + a_0$$

$$= \frac{1}{2} b_1 c_2 x^3 + \frac{1}{2} (2b_1 c_1 + b_0 c_2) x^2 + (b_1 c_0 + b_0 c_1) x + b_0 c_0$$

$$= \frac{1}{2} \{ b_1 c_2 x^3 + (2b_1 c_1 + b_0 c_2) x^2 + 2(b_1 c_0 + b_0 c_1) x + 2b_0 c_0 \}$$

$$= \frac{1}{2} [b_1 c_2 x^3 + \{ b_1 (2c_1) + b_0 c_2 \} x^2 + \{ b_1 (2c_0) + b_0 (2c_1) \} x + b_0 (2c_0)]$$

$$= \frac{1}{2} (b_1 x + b_0)(c_2 x^2 + 2c_1 x + 2c_0)$$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

이때 원시다항식 $g(x)$는 유리수체 $\mathbb{Q}$위에서 인수분해 되므로 정리 2.14에 의해 정수환 $\mathbb{Z}$위에서 $g(x)$는 인수분해 된다. 따라서 모순이다. 그러므로 $g(x)$가 $\mathbb{Z}[x]$에서 기약일 때 $f(x)$가 $h(\mathbb{Z})$에서 기약이다. ■

한편 정리 4.2에서 원식다항식 $f(x) = 3a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$에 대한 기약성은 $2|a_3$, $2|a_2$인 경우를 살펴보았으므로 이번에는 $2 \nmid a_3$, $2|a_2$인 경우 $f(x)$의 기약성에 대해 살펴보도록 하자.

(정리 4.3) 임의의 $a_3, a_2, a_1, a_0 \in \mathbb{Z}$ 에 대해,
$a_3 \neq 0$, $\gcd(3a_3, a_2, a_1, a_0) = 1$, $2 \nmid a_3, 2|a_2, 2|a_1, 4|a_0$ 이면 다음 두 조건이 동치이다.

1. $f(x) = 3a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$ 에서 기약이다.
2. $g(x) = a_3x^3 + \frac{1}{2}a_2x^2 + \frac{1}{2}a_1x + \frac{1}{4}a_0 \in \mathbb{Z}[x]$ 에서 기약이다.

증명(1)⟹(2) 다항식 $f(x)$가 $h(\mathbb{Z})$ 에서 기약 일 때 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약이 아니라고 하자. $\gcd(3a_3, a_2, a_1, a_0) = 1$이면 $\gcd(a_3, \frac{1}{2}a_2, \frac{1}{2}a_1, \frac{1}{4}a_0) = 1$이다.
$g(x)$가 $\mathbb{Z}[x]$위에서 기약이 아닌 원시다항식이므로 $g(x)$는 상수다항식이 아닌 두 개의 정수환다항식의 곱으로 표현된다.
이 때, 적당한 $b_1, b_0, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $g(x)$는 다음과 같이 나타난다.

$$\begin{aligned} g(x) &= (b_1x + b_0)(c_2x^2 + c_1x + c_0) \qquad (b_1 \neq 0, c_2 \neq 0) \\ &= b_1c_2x^3 + (b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\ &= a_3x^3 + \frac{1}{2}a_2x^2 + \frac{1}{2}a_1x + \frac{1}{4}a_0 \end{aligned}$$

따라서,

$$a_3 = b_1c_2,\ a_2 = 2(b_1c_1 + b_0c_2),\ a_1 = 2(b_1c_0 + b_0c_1),\ a_0 = 4b_0c_0 \quad -③$$

이때 식 ③을 $f(x)$의 계수에 대입하면, $f(x)$는 다음과 같이 나타난다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$
\begin{aligned}
f(x) &= 3a_3x^3 + a_2x^2 + a_1x + a_0 \\
&= 3b_1c_2x^3 + 2(b_1c_1 + b_0c_2)x^2 + 2(b_1c_0 + b_0c_1)x + 4b_0c_0 \\
&= \binom{3}{1}b_1c_2x^3 + \left\{\binom{2}{1}b_1c_1 + \binom{2}{0}(2b_0)c_2\right\}x^2 \\
&\quad + \left\{\binom{1}{1}b_1(2c_0) + \binom{1}{0}(2b_0)c_1\right\}x + \binom{0}{0}(2b_0)(2c_0) \\
&= (b_1x + 2b_0) * (c_2x^2 + c_1x + 2c_0)
\end{aligned}
$$

이는 $f(x)$는 $h(\mathbb{Z})$에서 기약이 아닌 모순이 생긴다. 따라서 $f(x)$가 $h(\mathbb{Z})$에서 기약일 때 $g(x)$가 $\mathbb{Z}[x]$에서 기약 이다.

(2)⟹(1) 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약 일 때, 다항식 $f(x)$가 $h(\mathbb{Z})$에서 기약이 아니라고 하자. $f(x)$는 $h(\mathbb{Z})$위에서 기약이 아닌 원시다항식 이므로 $f(x)$는 상수다항식이 아닌 두 개의 Hurwitz다항식의 곱으로 표현된다.
이 때, 적당한 $b_1, b_0, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $f(x)$는 다음과 같이 나타난다.

$$
\begin{aligned}
f(x) &= (b_1x + b_0) * (c_2x^2 + c_1x + c_0) \qquad (b_1 \neq 0, c_2 \neq 0) \\
&= \binom{3}{1}b_1c_2x^3 + \left(\binom{2}{1}b_1c_1 + \binom{2}{0}b_0c_2\right)x^2 + \left(\binom{1}{1}b_1c_0 + \binom{1}{0}b_0c_1\right)x + \binom{0}{0}b_0c_0 \\
&= 3b_1c_2x^3 + (2b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\
&= 3a_3x^3 + a_2x^2 + a_1x + a
\end{aligned}
$$

따라서,

$$a_3 = b_1c_2,\ a_2 = (2b_1c_1 + b_0c_2),\ a_1 = (b_1c_0 + b_0c_1),\ a_0 = b_0c_0 \quad - ④$$

이때 식 ④를 $g(x)$에 대입하면, $g(x)$는 다음과 같이 나타난다.

$$
\begin{aligned}
g(x) &= a_3x^3 + \frac{1}{2}a_2x^2 + \frac{1}{2}a_1x + \frac{1}{4}a_0 \\
&= b_1c_2x^3 + \frac{1}{2}(2b_1c_1 + b_0c_2)x^2 + \frac{1}{2}(b_1c_0 + b_0c_1)x + \frac{1}{4}b_0c_0 \\
&= \frac{1}{4}\left\{4b_1c_2x^3 + 2(2b_1c_1 + b_0c_2)x^2 + 2(b_1c_0 + b_0c_1)x + b_0c_0\right\}
\end{aligned}
$$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$= \frac{1}{4}\begin{bmatrix}(2b_1)(2c_2)x^3 + \{(2b_1)(2c_1)+b_0(2c_2)\}x^2 \\ + \{(2b_1)c_0 + b_0(2c_1)\}x + b_0c_0\end{bmatrix}$$

$$= \frac{1}{4}(2b_1x + b_0)(2c_2x^2 + 2c_1x + c_0)$$

이때 원시다항식 $g(x)$는 유리수체 $\mathbb{Q}$위에서 인수분해 되므로 정리 2.14에 의해 정수환 $\mathbb{Z}$위에서 $g(x)$는 인수분해 된다. 따라서 모순이다. 그러므로 $g(x)$가 $\mathbb{Z}[x]$에서 기약일 때 $f(x)$가 $h(\mathbb{Z})$에서 기약이다. ■

한편 정리 4.3에서 원식다항식 $f(x) = 3a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$에 대한 기약성은 $2 \nmid a_3$, $2 \mid a_2$인 경우를 살펴보았으므로 이번에는 $2 \nmid a_3$, $2 \nmid a_2$인 경우 $f(x)$의 기약성에 대해 살펴보도록 하자.

이때 다음 정리를 증명하기 위한 몇 가지 보조정리를 소개 하겠다.

(보조정리 4.4) (Euclidean의 보조정리) 임의의 $a, b, c \in \mathbb{Z}$ 에 대해 $\gcd(a, b) = 1$, $a|bc$ 이면 $a|c$ 이다.

증명 $\gcd(a,b) = 1$이므로 적당한 $x, y \in \mathbb{Z}$ 존재해서 $ax + by = 1$이다. 또한 $a|bc$ 이므로 적당한 $a' \in \mathbb{Z}$ 존재해서 $aa' = bc$이다. 즉, $c = acx + bcy = acx + aa'y = a(cx + a'y)$ 이므로 $a|c$ 이다. ■

(보조정리 4.5) 임의의 $a, b, c, d \in \mathbb{Z}$ 에 대해 $\gcd(a, b) = 1$, $ab|(ac + bd)$ 이면 $b|c$ 이고 $a|d$ 이다.

증명 조건에 의해 $ab|(ac + bd)$ 이면 $a|(ac + bd)$ 이므로 $a|bd$ 성립한다.
이 때, $\gcd(a, b) = 1$ 이므로 Euclidean의 보조정리에 의해 $a|d$이다.
또한 $b|(ac + bd)$도 같은 방식으로 하면 $b|c$도 성립한다. ■

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

(정리 4.6) 임의의 $a_3, a_2, a_1, a_0 \in \mathbb{Z}$ 에 대해, $a_3 \neq 0$, $\gcd(3a_3, a_2, a_1, a_0) = 1$ $2 \nmid a_3, 2 \nmid a_2, 2 | a_1, 2 | a_0, 4 \nmid a_0$ 이면 다음 두 조건이 동치이다.

1. $f(x) = 3a_3x^3 + a_2x^2 + \frac{1}{2}a_1x + \frac{1}{2}a_0 \in h(\mathbb{Z})$ 에서 기약이다.
2. $g(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ 에서 기약이다.

증명 (1)⟹(2) 다항식 $f(x)$가 $h(\mathbb{Z})$ 에서 기약 일 때, 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약이 아니라고 하자. $\gcd(3a_3, a_2, a_1, a_0) = 1$이면 $\gcd(a_3, a_2, a_1, a_0) = 1$이다. $g(x)$가 $\mathbb{Z}[x]$위에서 기약이 아니고 원시다항식이므로 $g(x)$는 상수다항식이 아닌 두 개의 정수환다항식의 곱으로 표현된다.
그러므로 적당한 $b_1, b_0, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $g(x)$는 다음과 같이 나타난다.

$$\begin{aligned} g(x) &= (b_1x + b_0)(c_2x^2 + c_1x + c_0) \quad (b_1 \neq 0, c_2 \neq 0) \\ &= b_1c_2x^3 + (b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\ &= a_3x^3 + a_2x^2 + a_1x + a_0 \end{aligned}$$

따라서,

$$a_3 = b_1c_2 \ , \ a_2 = (b_1c_1 + b_0c_2) \ , \ a_1 = (b_1c_0 + b_0c_1) \ , \ a_0 = b_0c_0 \quad -⑤$$

이때 ⑤식을 $f(x)$의 계수에 대입하면 $f(x)$는 다음과 같이 나타난다.

$$\begin{aligned} f(x) &= 3a_3x^3 + a_2x^2 + \frac{1}{2}a_1x + \frac{1}{2}a_0 \\ &= 3b_1c_2x^3 + (b_1c_1 + b_0c_2)x^2 + \frac{1}{2}(b_1c_0 + b_0c_1)x + \frac{1}{2}b_0c_0 \\ &= \frac{1}{2}\left\{6b_1c_2x^3 + 2(b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0\right\} \\ &= \frac{1}{2}\left[\begin{aligned} &\binom{3}{1}b_1(2c_2)x^3 + \left\{\binom{2}{1}b_1c_1 + \binom{2}{0}b_0(2c_2)\right\}x^2 \\ &\qquad + \left(\binom{1}{1}b_1c_0 + \binom{1}{0}b_0c_1\right)x + \binom{0}{0}b_0c_0 \end{aligned}\right] \\ &= \frac{1}{2}(b_1x + b_0) * (2c_2x^2 + c_1x + c_0) \quad - ⑥ \end{aligned}$$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

또한 조건에 의해 $2 \nmid a_3, 2 \nmid a_2, 2 | a_1, 2 | a_0, 4 \nmid a_0$ 이므로 다음을 만족한다.

$$\begin{cases} 2 \nmid b_1 c_2 \\ 2 \nmid (b_1 c_1 + b_0 c_2) \\ 2 \mid (b_1 c_0 + b_0 c_1) \\ 2 \mid b_0 c_0 \\ 4 \nmid b_0 c_0 \end{cases}$$

$2 | b_0 c_0$, $4 \nmid b_0 c_0$ 이므로 $2 \mid b_0$, $2 \nmid c_0$ 또는 $2 \nmid b_0$, $2 \mid c_0$이다.

I. $2 \mid b_0$, $2 \nmid c_0$인 경우 조건 $2 \mid (b_1 c_0 + b_0 c_1)$을 만족해야 하므로 보조정리 4.4, 보조정리 4.5에 의해 $2 | b_1$이다. 하지만 조건 $2 \nmid b_1 c_2$ 에 의해 모순이다.

II. $2 \nmid b_0$, $2 \mid c_0$인 경우 조건 $2 \mid (b_1 c_0 + b_0 c_1)$을 만족해야 하므로 보조정리 4.4, 보조정리 4.5에 의해 $2 | c_1$ 이다. 이때 $c_1 = 2c_1{}', c_0 = 2c_0{}'$ 이라고 하고 식 ⑥에 대입하면 $f(x)$는 다음과 같이 나타난다.

$$f(x) = \frac{1}{2}(b_1 x + b_0) * (2c_2 x^2 + 2c_1{}' x + 2c_0{}') \Rightarrow (b_1 x + b_0) * (c_2 x^2 + c_1{}' x + c_0{}') \in h(\mathbb{Z})$$

또한 $b_1 \neq 0$, $c_2 \neq 0$ 이므로 $(b_1 x + b_0), (c_2 x^2 + c_1{}' x + c_0{}') \notin U(h(\mathbb{Z}))$ 이다.
그러므로 모든 조건을 만족했을 때 $f(x)$는 $h(\mathbb{Z})$에서 기약이라는 가정에 모순이 생긴다. 따라서 $f(x)$가 $h(\mathbb{Z})$에서 기약이면 $g(x)$는 $\mathbb{Z}[x]$에서 기약이다.

(2)⟹(1) 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약 일 때, 다항식 $f(x)$가 $h(\mathbb{Z})$에서 기약이 아니라고 하자. $\gcd(3a_3, a_2, a_1, a_0) = 1$이면 $\gcd(3a_3, a_2, \frac{1}{2}a_1, \frac{1}{2}a_0) = 1$ 이다.
$f(x)$가 $h(\mathbb{Z})$위에서 기약인 원시다항식이므로 $f(x)$는 상수다항식이 아닌 두 개의 Hurwitz다항식의 곱으로 표현된다.
이 때, 적당한 $b_1, b_0, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $f(x)$는 다음과 같이 나타난다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$f(x) = (b_1 x + b_0) * (c_2 x^2 + c_1 x + c_0) \qquad (b_1 \neq 0, c_2 \neq 0)$$

$$= \binom{3}{1} b_1 c_2 x^3 + \left(\binom{2}{1} b_1 c_1 + \binom{2}{0} b_0 c_2\right) x^2 + \left(\binom{1}{1} b_1 c_0 + \binom{1}{0} b_0 c_1\right) x + \binom{0}{0} b_0 c_0$$

$$= 3b_1 c_2 x^3 + (2b_1 c_1 + b_0 c_2) x^2 + (b_1 c_0 + b_0 c_1) x + b_0 c_0$$

$$= 3a_3 x^3 + a_2 x^2 + \frac{1}{2} a_1 x + \frac{1}{2} a_0$$

따라서,

$$a_3 = b_1 c_2 \ , \ a_2 = (2b_1 c_1 + b_0 c_2) \ , \ a_1 = 2(b_1 c_0 + b_0 c_1) \ , \ a_0 = 2b_0 c_0 \quad -⑦$$

이때 식 ⑦을 $g(x)$의 계수에 대입하면 $g(x)$는 다음과 같이 나타난다.

$$g(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

$$= b_1 c_2 x^3 + (2b_1 c_1 + b_0 c_2) x + 2(b_1 c_0 + b_0 c_1) x + 2b_0 c_0$$

$$= b_1 c_2 x^3 + \{b_1 (2c_1) + b_0 c_2\} x + \{b_1 (2c_0) + b_0 (2c_1)\} x + b_0 (2c_0)$$

$$= (b_1 x + b_0)(c_2 x^2 + 2c_1 x + 2c_0) \in \mathbb{Z}[x]$$

이는 $g(x)$가 $\mathbb{Z}[x]$에서 기약이 아니라는 모순이 생긴다. 따라서 $g(x)$가 $\mathbb{Z}[x]$에서 기약이면, $f(x)$가 $h(\mathbb{Z})$에서 기약이다. ■

지금부터는 정수계수를 갖는 4차 Hurwitz 다항식의 기약성에 대해 알아보도록 하자. 먼저 간단한 사실로부터 출발하도록 하자.

(보조정리 4.7) 원시 다항식

$$f(x) = a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 \in h(\mathbb{Z})$$

에 대하여 $4 \nmid a_4$ 이고 $6 \nmid a_4$이면, 다항식 $f(x)$는 $h(\mathbb{Z})$에서 기약이다.

증명 만약 $f(x)$가 $h(\mathbb{Z})$에서 기약이 아니라고 하자.
$f(x)$는 $h(\mathbb{Z})$위에서 기약이 아닌 원시다항식 이므로 $f(x)$는 상수다항식이 아닌 두 개의 Hurwitz 다항식의 곱으로 표현된다. 그러므로 $f(x)$는 일차식과 삼차식 또는

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

이차식과 이차식으로 인수분해 된다.

Ⅰ. $f(x)=g(x)*h(x)$, $\deg(g(x))=1, \deg(h(x))=3$,$g(x),h(x)\in h(\mathbb{Z})$인 경우 적당한 $b_1, b_0, c_3, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $f(x)$는 다음과 같이 나타난다.

$$\begin{aligned} f(x) &= (b_1x+b_0)*(c_3x^3+c_2x^2+c_1x+c_0) \qquad (b_1\neq 0, c_3\neq 0) \\ &= \binom{4}{1}b_1c_3x^4+\left(\binom{3}{1}b_1c_2+\binom{3}{0}b_0c_3\right)x^3 \\ &\quad +\left(\binom{2}{1}b_1c_1+\binom{2}{0}b_0c_2\right)x^2+\left(\binom{1}{1}b_1c_0+\binom{1}{0}b_0c_1\right)x+\binom{0}{0}b_0c_0 \\ &= 4b_1c_3x^4+(3b_1c_2+b_0c_3)x^3 \\ &\quad +(2b_1c_1+b_0c_2)x^2+(b_1c_0+b_0c_1)x+b_0c_0 \end{aligned}$$

따라서 $a_4=4b_1c_3$ 이므로 $4\mid a_4$이다.

Ⅱ. $f(x)=g(x)*h(x)$, $\deg(g(x))=2, \deg(h(x))=2$,$g(x),h(x)\in h(\mathbb{Z})$인 경우 적당한 $b_2, b_1, b_0, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $f(x)$는 다음과 같이 나타난다.

$$\begin{aligned} f(x) &= (b_2x^2+b_1x+b_0)*(c_2x^2+c_1x+c_0) \qquad (b_2\neq 0, c_2\neq 0) \\ &= \binom{4}{2}b_2c_2x^4+\left(\binom{3}{2}b_2c_1+\binom{3}{1}b_1c_2\right)x^3 \\ &\quad +\left(\binom{2}{2}b_2c_0+\binom{2}{1}b_1c_1+\binom{2}{0}b_0c_2\right)x^2+\left(\binom{1}{1}b_1c_0+\binom{1}{0}b_0c_1\right)x+\binom{0}{0}b_0c_0 \\ &= 6b_2c_2x^4+(3b_2c_1+3b_1c_2)x^3 \\ &\quad +(b_2c_0+2b_1c_1+b_0c_2)x^2+(b_1c_0+b_0c_1)x+b_0c_0 \end{aligned}$$

따라서 $a_4=6b_2c_2$ 이므로 $6\mid a_4$이다.
Ⅰ,Ⅱ에 의해 $f(x)$가 $h(\mathbb{Z})$에서 기약이 아닐 때 $4\mid a_4$이거나 $6\mid a_4$이다.
따라서 $4\nmid a_4$ 이고 $6\nmid a_4$이면, 다항식 $f(x)$는 $h(\mathbb{Z})$에서 기약이다. ■

보조정리 4.7로부터 원시다항식 $f(x)=a_4x^4+a_3x^3+a_2x^2+a_1x+a_0\in h(\mathbb{Z})$에 대

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

해 $4 \nmid a_4$ 이고 $6 \nmid a_4$이면 기약임을 알 수 있다. 그러므로 $4 \mid a_4$ 또는 $6 \mid a_4$인 경우 $f(x)$의 기약성에 대해 알아보자.

먼저 $4 \mid a_4$인 경우 $f(x)$의 기약성을 살펴보자.

(정리 4.8) 임의의 $a_4, a_3, a_2, a_1, a_0 \in \mathbb{Z}$ 에 대해,
$a_4 \neq 0$, $\gcd(4a_4, a_3, a_2, a_1, a_0) = 1$, $6 \mid a_4$, $6 \mid a_3$, $2 \mid a_2$ 이면 다음 두 조건이 동치이다.

1. $f(x) = 4a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$ 에서 기약이다.
2. $g(x) = \frac{1}{6}a_4x^4 + \frac{1}{6}a_3x^3 + \frac{1}{2}a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ 에서 기약이다.

증명(1)⟹(2) 다항식 $f(x)$가 $h(\mathbb{Z})$ 에서 기약 일 때 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약이 아니라고 하자. $\gcd(4a_4, a_3, a_2, a_1, a_0) = 1$이면 $\gcd(\frac{1}{6}a_4, \frac{1}{6}a_3, \frac{1}{2}a_2, a_1, a_0) = 1$ 이다. $g(x)$가 $\mathbb{Z}[x]$위에서 기약이 아니고 원시다항식이므로 $g(x)$는 상수다항식이 아닌 두 개의 정수환다항식의 곱으로 표현된다.
그러므로 $g(x)$는 일차식과 삼차식 또는 이차식과 이차식으로 인수분해 된다.

Ⅰ. $g(x) = h(x)k(x)$, $\deg(h(x)) = 1, \deg(k(x)) = 3$,$h(x), k(x) \in \mathbb{Z}[x]$인 경우
적당한 $b_1, b_0, c_3, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $g(x)$는 다음과 같이 나타난다.

$$\begin{aligned} g(x) &= (b_1x + b_0)(c_3x^3 + c_2x^2 + c_1x + c_0) \qquad (b_1 \neq 0, c_3 \neq 0) \\ &= b_1c_3x^4 + (b_1c_2 + b_0c_3)x^2 + (b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\ &= \frac{1}{6}a_4x^4 + \frac{1}{6}a_3x^3 + \frac{1}{2}a_2x^2 + a_1x + a_0 \end{aligned}$$

따라서,

$$\begin{cases} a_4 = 6b_1c_3 \ , \ a_3 = 6(b_1c_2 + b_0c_3) \\ a_2 = 2(b_1c_1 + b_0c_2) \ , \ a_1 = (b_1c_0 + b_0c_1) \ , \ a_0 = b_0c_0 \end{cases} \quad - ⑧$$

이때 식 ⑧을 $f(x)$의 계수에 대입하면, $f(x)$는 다음과 같이 나타난다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$
\begin{aligned}
f(x) &= 4a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \\
&= 24b_1c_3x^4 + 6(b_1c_2 + b_0c_3)x^3 + 2(b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\
&= \binom{4}{1}b_1(6c_3)x^4 + \left\{\binom{3}{1}b_1(2c_2) + \binom{3}{0}b_0(6c_3)\right\}x^3 \\
&\quad + \left\{\binom{2}{1}b_1c_1 + \binom{2}{0}b_0(2c_2)\right\}x^2 + \left(\binom{1}{1}b_1c_0 + \binom{1}{0}b_0c_1\right)x + \binom{0}{0}b_0c_0 \\
&= (b_1x + b_0) * (6c_3x^3 + 2c_2x^2 + c_1x + c_0)
\end{aligned}
$$

이는 $f(x)$는 $h(\mathbb{Z})$에서 기약이 아니라는 가정에 모순이다.

Ⅱ. $g(x) = h(x)k(x)$, $\deg(h(x)) = 2$, $\deg(k(x)) = 2$,$h(x), k(x) \in \mathbb{Z}[x]$인 경우 적당한 $b_2, b_1, b_0, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $g(x)$는 다음과 같이 나타난다.

$$
\begin{aligned}
g(x) &= (b_2x^2 + b_1x + b_0)(c_2x^2 + c_1x + c_0) \qquad (b_2 \neq 0, c_2 \neq 0) \\
&= b_2c_2x^4 + (b_2c_1 + b_1c_2)x^3 + (b_2c_0 + b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\
&= \frac{1}{6}a_4x^4 + \frac{1}{6}a_3x^3 + \frac{1}{2}a_2x^2 + a_1x + a_0
\end{aligned}
$$

따라서,

$$
\begin{cases}
a_4 = 6b_2c_2 \ , \ a_3 = 6(b_2c_1 + b_1c_2) \\
a_2 = 2(b_2c_0 + b_1c_1 + b_0c_2) \ , \ a_1 = (b_1c_0 + b_0c_1) \ , \ a_0 = b_0c_0
\end{cases} \qquad - ⑨
$$

이때 식 ⑨를 $f(x)$의 계수에 대입하면 $f(x)$는 다음과 같이 나타난다.

$$
\begin{aligned}
f(x) &= 4a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \\
&= 24b_2c_2x^4 + 6(b_2c_1 + b_1c_2)x^3 + 2(b_2c_0 + b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\
&= \binom{4}{2}(2b_2)(2c_2)x^4 + \left\{\binom{3}{2}(2b_2)c_1 + \binom{3}{1}b_1(2c_2)\right\}x^3 \\
&\quad + \left\{\binom{2}{2}(2b_2)c_0 + \binom{2}{1}b_1c_1 + \binom{2}{0}b_0(2c_2)\right\}x^2 + \left(\binom{1}{1}b_1c_0 + \binom{1}{0}b_0c_1\right)x + \binom{0}{0}b_0c_0 \\
&= (2b_2x^2 + b_1x + b_0) * (2c_2x^2 + c_1x + c_0)
\end{aligned}
$$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

이는 $f(x)$는 $h(\mathbb{Z})$에서 기약이라는 가정에 모순이다.

Ⅰ,Ⅱ 에 의해서 $f(x)$가 $h(\mathbb{Z})$에서 기약일 때 $g(x)$가 $\mathbb{Z}[x]$에서 기약 이다.

(2)⟹(1) 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약 일 때, 다항식 $f(x)$가 $h(\mathbb{Z})$에서 기약이 아니라고 하자. $f(x)$는 $h(\mathbb{Z})$위에서 기약이 아닌 원시다항식 이므로 $f(x)$는 상수다항식이 아닌 두 개의 Hurwitz다항식의 곱으로 표현된다. 그러므로 $f(x)$는 일차식과 삼차식 또는 이차식과 이차식으로 인수분해 된다.

Ⅰ. $f(x)=h(x)*k(x)$, $\deg(h(x))=1, \deg(k(x))=3$,$h(x),k(x)\in h(\mathbb{Z})$인 경우 적당한 $b_1, b_0, c_3, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $f(x)$는 다음과 같이 나타난다.

$$
\begin{aligned}
f(x) &= (b_1x+b_0)*(c_3x^3+c_2x^2+c_1x+c_0) \qquad (b_1\neq 0, c_3\neq 0)\\
&= \binom{4}{1}b_1c_3x^4+\left(\binom{3}{1}b_1c_2+\binom{3}{0}b_0c_3\right)x^3\\
&\quad +\left(\binom{2}{1}b_1c_1+\binom{2}{0}b_0c_2\right)x^2+\left(\binom{1}{1}b_1c_0+\binom{1}{0}b_0c_1\right)x+\binom{0}{0}b_0c_0\\
&= 4b_1c_3x^4+(3b_1c_2+b_0c_3)x^3\\
&\quad +(2b_1c_1+b_0c_2)x^2+(b_1c_0+b_0c_1)x+b_0c_0\\
&= 4a_4x^4+a_3x^3+a_2x^2+a_1x+a_0
\end{aligned}
$$

따라서,

$$
\begin{cases} a_4=b_1c_3\ ,\ a_3=(3b_1c_2+b_0c_2) \\ a_2=(2b_1c_1+b_0c_2)\ ,\ a_1=(b_1c_0+b_0c_1)\ ,\ a_0=b_0c_0 \end{cases} \quad - ⑩
$$

이때 식 ⑩을 $g(x)$의 계수에 대입하면 $g(x)$는 다음과 같이 나타난다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$
\begin{aligned}
g(x) &= \frac{1}{6}a_4x^4 + \frac{1}{6}a_3x^3 + \frac{1}{2}a_2x^2 + a_1x + a_0 \\
&= \frac{1}{6}b_1c_3x^4 + \frac{1}{6}(3b_1c_2 + b_0c_3)x^3 \\
&\quad + \frac{1}{2}(2b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\
&= \frac{1}{6}\left\{\begin{array}{l} b_1c_3x^4 + (3b_1c_2 + b_0c_3)x^3 \\ \quad + 3(2b_1c_1 + b_0c_2)x^2 + 6(b_1c_0 + b_0c_1)x + 6b_0c_0 \end{array}\right\} \\
&= \frac{1}{6}\left[\begin{array}{l} b_1c_3x^4 + \{b_1(3c_2) + b_0c_3\}x^3 \\ \quad + \{b_1(6c_1) + b_0(3c_2)\}x^2 + \{b_1(6c_0) + b_0(6c_1)\}x + b_0(6c_0) \end{array}\right] \\
&= \frac{1}{6}(b_1x + b_0)(c_3x^3 + 3c_2x^2 + 6c_1x + 6c_0)
\end{aligned}
$$

이때 원시다항식 $g(x)$는 유리수체 $\mathbb{Q}$위에서 인수분해 되므로 정리 2.14에 의해 $g(x)$는 정수환 $\mathbb{Z}$위에서 일차식과 삼차식으로 인수분해 된다. 따라서 모순이다.

Ⅱ. $f(x) = h(x) * k(x)$, $\deg(h(x)) = 2, \deg(k(x)) = 2$,$h(x), k(x) \in h(\mathbb{Z})$인 경우 적당한 $b_2, b_1, b_0, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $f(x)$는 다음과 같이 나타난다.

$$
\begin{aligned}
f(x) &= (b_2x^2 + b_1x + b_0) * (c_2x^2 + c_1x + c_0) \qquad (b_2 \neq 0, c_2 \neq 0) \\
&= \binom{4}{2}b_2c_2x^4 + \left(\binom{3}{2}b_2c_1 + \binom{3}{1}b_1c_2\right)x^3 \\
&\quad + \left(\binom{2}{2}b_2c_0 + \binom{2}{1}b_1c_1 + \binom{2}{0}b_0c_2\right)x^2 + \left(\binom{1}{1}b_1c_0 + \binom{1}{0}b_0c_1\right)x + \binom{0}{0}b_0c_0 \\
&= 6b_2c_2x^4 + (3b_2c_1 + 3b_1c_2)x^3 \\
&\quad + (b_2c_0 + 2b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\
&= 4a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0
\end{aligned}
$$

따라서,

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$\begin{cases} a_4 = \frac{3}{2}b_2c_2 \ , \ a_3 = (3b_2c_1 + 3b_1c_2) \\ a_2 = (b_2c_0 + 2b_1c_1 + b_0c_2) \ , \ a_1 = (b_1c_0 + b_0c_1) \ , \ a_0 = b_0c_0 \end{cases} \quad - ⑪$$

이때 식 ⑪을 $g(x)$의 계수에 대입하면, $g(x)$는 다음과 같이 나타난다.

$$\begin{aligned} g(x) &= \frac{1}{6}a_4x^4 + \frac{1}{6}a_3x^3 + \frac{1}{2}a_2x^2 + a_1x + a_0 \\ &= \frac{1}{6} \cdot \frac{3}{2}b_2c_2x^4 + \frac{1}{6} \cdot 3(b_2c_1 + b_1c_2)x^3 \\ &\quad + \frac{1}{2}(b_2c_0 + 2b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\ &= \frac{1}{4}b_2c_2x^4 + \frac{1}{2}(b_2c_1 + b_1c_2)x^3 \\ &\quad + \frac{1}{2}(b_2c_0 + 2b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\ &= \frac{1}{4}\left\{ \begin{array}{l} b_2c_2x^4 + 2(b_2c_1 + b_1c_2)x^3 \\ \quad + 2(b_2c_0 + 2b_1c_1 + b_0c_2)x^2 + 4(b_1c_0 + b_0c_1)x + 4b_0c_0 \end{array} \right\} \\ &= \frac{1}{4}\left[\begin{array}{l} b_2c_2x^4 + \{b_2(2c_1) + (2b_1)c_2\}x^3 \\ + \{b_2(2c_0) + (2b_1)(2c_1) + (2b_0)c_2\}x^2 \\ + \{(2b_1)(2c_0) + (2b_0)(2c_1)\}x + (2b_0)(2c_0) \end{array} \right] \\ &= \frac{1}{4}(b_2x^2 + 2b_1x + 2b_0)(c_2x^2 + 2c_1x + 2c_0) \end{aligned}$$

이때 원시다항식 $g(x)$는 유리수체 $\mathbb{Q}$위에서 인수분해 되므로 정리 2.14에 의해 $g(x)$는 정수환 $\mathbb{Z}$위에서 이차식과 이차식으로 인수분해 된다. 따라서 모순이다.

Ⅰ,Ⅱ에 의해 $g(x)$가 $\mathbb{Z}[x]$에서 기약일 때 $f(x)$가 $h(\mathbb{Z})$에서 기약이다. ■

한편 정리 4.8에서 원시다항식 $f(x) = 4a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$가

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$6 \mid a_4$인 경우를 살펴보았다. 다음으로 $6 \nmid a_4$인 경우 $f(x)$의 기약성에 대해 살펴보려고 했지만 해결하지 못하였다. 그러므로 $3 \nmid a_4$인 경우 $f(x)$의 기약성에 대해서만 살펴보도록 하자.

(보조정리 4.9) 기약이 아닌 원시다항식

$$f(x) = 4a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$$

에서 $3 \nmid a_4$ 이면 적당한 두 개의 기약 다항식

$$b_1x + b_0 \ , \ c_3x^3 + c_2x^2 + c_1x + c_0 \in h(\mathbb{Z})$$

가 존재해서

$$f(x) = (b_1x + b_0) * (c_3x^3 + c_2x^2 + c_1x + c_0) \ , \ (b_1 \neq 0, c_3 \neq 0)$$

로 표현 된다.

증명 만약 $f(x)$가 이차식과 이차식으로 인수분해 되면 $6 \mid 4a_4$ 이다. 이때 $3 \mid a_4$이므로 모순이 생긴다. 따라서 $f(x)$는 일차식과 삼차식으로 인수분해 된다. ■

(정리 4.10) 임의의 $a_4, a_3, a_2, a_1, a_0 \in \mathbb{Z}$ 에 대해
$a_4 \neq 0$, $\gcd(4a_4, a_3, a_2, a_1, a_0) = 1$, $3 \nmid a_4$, $2 \mid a_4$, $6 \mid a_3$, $6 \mid a_2$, $9 \mid a_1$, $27 \mid a_0$
이고

$$g(x) = \frac{1}{2}a_4x^4 + \frac{1}{6}a_3x^3 + \frac{1}{6}a_2x^2 + \frac{1}{9}a_1x + \frac{1}{27}a_0 \in \mathbb{Z}[x]$$

$$f(x) = 4a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$$

라고 하면 $g(x)$가 $\mathbb{Z}[x]$에서 기약 일 때 $f(x)$는 $h(\mathbb{Z})$에서 기약이다.

증명 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약일 때, 다항식 $f(x)$가 $h(\mathbb{Z})$에서 기약이 아니라고 하자. 이때 $f(x) = 4a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$ 에서 $3 \nmid a_4$ 이므로
보조정리 4.9에 의해서 적당한 두 개의 기약 다항식
$b_1x + b_0$, $c_3x^3 + c_2x^2 + c_1x + c_0 \in h(\mathbb{Z})$가 존재해서
$f(x) = (b_1x + b_0) * (c_3x^3 + c_2x^2 + c_1x + c_0)$로 표현 된다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$
\begin{aligned}
f(x) &= (b_1x + b_0) * (c_3x^3 + c_2x^2 + c_1x + c_0) \\
&= \binom{4}{1}b_1c_3x^4 + \left(\binom{3}{1}b_1c_2 + \binom{3}{0}b_0c_3\right)x^3 \\
&\quad + \left(\binom{2}{1}b_1c_1 + \binom{2}{0}b_0c_2\right)x^2 + \left(\binom{1}{1}b_1c_0 + \binom{1}{0}b_0c_1\right)x + \binom{0}{0}b_0c_0 \\
&= 4b_1c_3x^4 + (3b_1c_2 + b_0c_3)x^3 \\
&\quad + (2b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\
&= 4a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0
\end{aligned}
$$

따라서,

$$
\begin{cases} a_4 = b_1c_3 \ , \ a_3 = (3b_1c_2 + b_0c_3) \\ a_2 = (2b_1c_1 + b_0c_2) \ , \ a_1 = (b_1c_0 + b_0c_1) \ , \ a_0 = b_0c_0 \end{cases} \quad -⑫
$$

이때 식 ⑫를 $g(x)$에 대입하면, $g(x)$는 다음과 같이 나타난다.

$$
\begin{aligned}
g(x) &= \frac{1}{2}a_4x^4 + \frac{1}{6}a_3x^3 + \frac{1}{6}a_2x^2 + \frac{1}{9}a_1x + \frac{1}{27}a_0 \\
&= \frac{1}{2}b_1c_3x^4 + \frac{1}{6}(3b_1c_2 + b_0c_3)x^3 \\
&\quad + \frac{1}{6}(2b_1c_1 + b_0c_2)x^2 + \frac{1}{9}(b_1c_0 + b_0c_1)x + \frac{1}{27}b_0c_0 \\
&= \frac{1}{54}\left\{\begin{array}{l} 27b_1c_3x^4 + 9(3b_1c_2 + b_0c_3)x^3 \\ + 9(2b_1c_1 + b_0c_2)x^2 + 6(b_1c_0 + b_0c_1)x + 2b_0c_0 \end{array}\right\} \\
&= \frac{1}{54}\left[\begin{array}{l} (3b_1)(9c_3)x^4 \\ \quad + \{(3b_1)(9c_2) + b_0(9c_3)\}x^3 + \{(3b_1)(6c_1) + b_0(9c_2)\}x^2 \\ \quad\quad + \{(3b_1)(2c_0) + b_0(6c_1)\}x + b_0(2c_0) \end{array}\right] \\
&= \frac{1}{54}(3b_1x + b_0)(9c_3x^3 + 9c_2x^2 + 6c_1x + 2c_0)
\end{aligned}
$$

이때 $g(x)$는 유리수체 $\mathbb{Q}$위에서 인수분해 되므로 정리 2.14에 의해 정수환 $\mathbb{Z}$위에

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

서 $g(x)$는 인수분해 된다. 따라서 모순이다. 그러므로 $g(x)$가 $\mathbb{Z}[x]$에서 기약일 때 $f(x)$가 $h(\mathbb{Z})$에서 기약이다. ■

한편, 정리 4.10에서 $f(x)$가 $h(\mathbb{Z})$에서 기약일 때 $g(x)$가 $\mathbb{Z}[x]$에서 기약인 것은 성립할 것 같으나 밝히지는 못했다. 이에 대한 후속 연구가 필요할 것으로 보인다.

지금부터는 원시다항식 $f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$에 대해 $6 \mid a_4$인 경우 $f(x)$의 기약성을 살펴보도록 하자.

(정리 4.11) 임의의 $a_4, a_3, a_2, a_1, a_0 \in \mathbb{Z}$ 에 대해,
$a_4 \neq 0$, $\gcd(6a_4, a_3, a_2, a_1, a_0) = 1$, $4 \mid a_4$, $6 \mid a_3$, $2 \mid a_2$ 이면 다음 두 조건이 동치이다.

1. $f(x) = 6a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$ 에서 기약이다.
2. $g(x) = \frac{1}{4}a_4x^4 + \frac{1}{6}a_3x^3 + \frac{1}{2}a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ 에서 기약이다.

증명(1)⇒(2) 다항식 $f(x)$가 $h(\mathbb{Z})$ 에서 기약 일 때 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약이 아니라고 하자. $\gcd(6a_4, a_3, a_2, a_1, a_0) = 1$이면 $\gcd(\frac{1}{4}a_4, \frac{1}{6}a_3, \frac{1}{2}a_2, a_1, a_0) = 1$이다. $g(x)$가 $\mathbb{Z}[x]$위에서 기약이 아닌 원시다항식이므로 $g(x)$는 상수다항식이 아닌 두 개의 정수환다항식의 곱으로 표현된다.
그러므로 $g(x)$는 일차식과 삼차식 또는 이차식과 이차식으로 인수분해 된다.

Ⅰ. $g(x) = h(x)k(x)$, $\deg(h(x)) = 1, \deg(k(x)) = 3$,$h(x), k(x) \in \mathbb{Z}[x]$인 경우
적당한 $b_1, b_0, c_3, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $g(x)$는 다음과 같이 나타난다.

$$\begin{aligned} g(x) &= (b_1x + b_0)(c_3x^3 + c_2x^2 + c_1x + c_0) \qquad (b_1 \neq 0, c_3 \neq 0) \\ &= b_1c_3x^4 + (b_1c_2 + b_0c_3)x^3 + (b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\ &= \frac{1}{4}a_4x^4 + \frac{1}{6}a_3x^3 + \frac{1}{2}a_2x^2 + a_1x + a_0 \end{aligned}$$

따라서,

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$\begin{cases} a_4 = 4b_1c_3 \ , \ a_3 = 6(b_1c_2 + b_0c_3) \\ a_2 = 2(b_1c_1 + b_0c_2) \ , \ a_1 = (b_1c_0 + b_0c_1) \ , \ a_0 = b_0c_0 \end{cases} \quad - ⑬$$

이때 식 ⑬을 $f(x)$의 계수에 대입하면, $f(x)$는 다음과 같이 나타난다.

$$\begin{aligned} f(x) &= 6a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \\ &= 24b_1c_3x^4 + 6(b_1c_2 + b_0c_3)x^3 + 2(b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\ &= \binom{4}{1}b_1(6c_3)x^4 + \left\{\binom{3}{1}b_1(2c_2) + \binom{3}{0}b_0(6c_3)\right\}x^3 \\ &\quad + \left\{\binom{2}{1}b_1c_1 + \binom{2}{0}b_0(2c_2)\right\}x^2 + \left\{\binom{1}{1}b_1c_0 + \binom{1}{0}b_0c_1\right\}x + \binom{0}{0}b_0c_0 \\ &= (b_1x + b_0) * (6c_3x^3 + 2c_2x^2 + c_1x + c_0) \end{aligned}$$

이는 $f(x)$는 $h(\mathbb{Z})$에서 기약이 아니라는 가정에 모순이다.

Ⅱ. $g(x) = h(x)k(x)$, $\deg(h(x)) = 2, \deg(k(x)) = 2$ $, h(x), k(x) \in \mathbb{Z}[x]$인 경우
적당한 $b_2, b_1, b_0, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $g(x)$는 다음과 같이 나타난다.

$$\begin{aligned} g(x) &= (b_2x^2 + b_1x + b_0)(c_2x^2 + c_1x + c_0) \qquad (b_2 \neq 0, c_2 \neq 0) \\ &= b_2c_2x^4 + (b_2c_1 + b_1c_2)x^3 + (b_2c_0 + b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\ &= \frac{1}{4}a_4x^4 + \frac{1}{6}a_3x^3 + \frac{1}{2}a_2x^2 + a_1x + a_0 \end{aligned}$$

따라서,

$$\begin{cases} a_4 = 4b_2c_2 \ , \ a_3 = 6(b_2c_1 + b_1c_2) \\ a_2 = 2(b_2c_0 + b_1c_1 + b_0c_2) \ , \ a_1 = (b_1c_0 + b_0c_1) \ , \ a_0 = b_0c_0 \end{cases} \quad - ⑭$$

이때 식 ⑭를 $f(x)$의 계수에 대입하면 $f(x)$는 다음과 같이 나타난다.

$$\begin{aligned} f(x) &= 6a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \\ &= 24b_2c_2x^4 + 6(b_2c_1 + b_1c_2)x^3 + 2(b_2c_0 + b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \end{aligned}$$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$= \binom{4}{2}(2b_2)(2c_2)x^4 + \left\{\binom{3}{2}(2b_2)c_1 + \binom{3}{1}b_1(2c_2)\right\}x^3$$

$$+ \left\{\binom{2}{2}(2b_2)c_0 + \binom{2}{1}b_1c_1 + \binom{2}{0}b_0(2c_2)\right\}x^2 + \left(\binom{1}{1}b_1c_0 + \binom{1}{0}b_0c_1\right)x + \binom{0}{0}b_0c_0$$

$$= (2b_2x^2 + b_1x + b_0) * (2c_2x^2 + c_1x + c_0) \in h(\mathbb{Z})$$

이는 $f(x)$는 $h(\mathbb{Z})$에서 기약이라는 가정에 모순이다.

Ⅰ,Ⅱ 에 의해서 $f(x)$가 $h(\mathbb{Z})$에서 기약일 때 $g(x)$가 $\mathbb{Z}[x]$에서 기약 이다.

(2)⟹(1) 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약 일 때, 다항식 $f(x)$가 $h(\mathbb{Z})$에서 기약이 아니라고 하자. $f(x)$는 $h(\mathbb{Z})$위에서 기약이 아닌 원시다항식 이므로 $f(x)$는 상수다항식이 아닌 두 개의 Hurwitz다항식의 곱으로 표현된다. 그러므로 $f(x)$는 일차식과 삼차식 또는 이차식과 이차식으로 인수분해 된다.

Ⅰ. $f(x) = h(x) * k(x)$, $\deg(h(x)) = 1, \deg(k(x)) = 3$,$h(x), k(x) \in h(\mathbb{Z})$인 경우 적당한 $b_1, b_0, c_3, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $f(x)$는 다음과 같이 나타난다.

$$f(x) = (b_1x + b_0) * (c_3x^3 + c_2x^2 + c_1x + c_0) \qquad (b_1 \neq 0, c_3 \neq 0)$$

$$= \binom{4}{1}b_1c_3x^4 + \left(\binom{3}{1}b_1c_2 + \binom{3}{0}b_0c_3\right)x^3$$

$$+ \left(\binom{2}{1}b_1c_1 + \binom{2}{0}b_0c_2\right)x^2 + \left(\binom{1}{1}b_1c_0 + \binom{1}{0}b_0c_1\right)x + \binom{0}{0}b_0c_0$$

$$= 4b_1c_3x^4 + (3b_1c_2 + b_0c_3)x^3$$

$$+ (2b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0$$

$$= 6a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

따라서,

$$\begin{cases} a_4 = \frac{2}{3}b_1c_3 \ , \ a_3 = (3b_1c_2 + b_0c_2) \\ a_2 = (2b_1c_1 + b_0c_2) \ , \ a_1 = (b_1c_0 + b_0c_1) \ , \ a_0 = b_0c_0 \end{cases} \qquad - ⑮$$

이때 식 ⑮을 $g(x)$의 계수에 대입하면 $g(x)$는 다음과 같이 나타난다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$g(x) = \frac{1}{4}a_4x^4 + \frac{1}{6}a_3x^3 + \frac{1}{2}a_2x^2 + a_1x + a_0$$

$$= \frac{1}{4} \cdot \frac{2}{3}b_1c_3x^4 + \frac{1}{6}(3b_1c_2 + b_0c_3)x^3$$

$$+ \frac{1}{2}(2b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0$$

$$= \frac{1}{6}\left\{\begin{array}{l} b_1c_3x^4 + (3b_1c_2 + b_0c_3)x^3 \\ \quad + 3(2b_1c_1 + b_0c_2)x^2 + 6(b_1c_0 + b_0c_1)x + 6b_0c_0 \end{array}\right\}$$

$$= \frac{1}{6}\left[\begin{array}{l} b_1c_3x^4 + \{b_1(3c_2) + b_0c_3\}x^3 \\ \quad + \{b_1(6c_1) + b_0(3c_2)\}x^2 + \{b_1(6c_0) + b_0(6c_1)\}x + b_0(6c_0) \end{array}\right]$$

$$= \frac{1}{6}(b_1x + b_0)(c_3x^3 + 3c_2x^2 + 6c_1x + 6c_0)$$

이때 원시다항식 $g(x)$는 유리수체 $\mathbb{Q}$위에서 인수분해 되므로 정리 2.14에 의해 정수환 $\mathbb{Z}$위에서 $g(x)$는 일차식과 삼차식으로 인수분해 된다. 따라서 모순이다.

Ⅱ. $f(x) = h(x) * k(x)$, $\deg(h(x)) = 2, \deg(k(x)) = 2$ $, h(x), k(x) \in h(\mathbb{Z})$인 경우 적당한 $b_2, b_1, b_0, c_2, c_1, c_0 \in \mathbb{Z}$에 대해 $f(x)$는 다음과 같이 나타난다.

$$f(x) = (b_2x^2 + b_1x + b_0) * (c_2x^2 + c_1x + c_0) \qquad (b_2 \neq 0, c_2 \neq 0)$$

$$= \binom{4}{2}b_2c_2x^4 + \left(\binom{3}{2}b_2c_1 + \binom{3}{1}b_1c_2\right)x^3$$

$$+ \left(\binom{2}{2}b_2c_0 + \binom{2}{1}b_1c_1 + \binom{2}{0}b_0c_2\right)x^2 + \left(\binom{1}{1}b_1c_0 + \binom{1}{0}b_0c_1\right)x + \binom{0}{0}b_0c_0$$

$$= 6b_2c_2x^4 + (3b_2c_1 + 3b_1c_2)x^3$$

$$+ (b_2c_0 + 2b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0$$

$$= 6a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

따라서,

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$\begin{cases} a_4 = b_2c_2 \ , \ a_3 = (3b_2c_1 + 3b_1c_2) \\ a_2 = (b_2c_0 + 2b_1c_1 + b_0c_2) \ , \ a_1 = (b_1c_0 + b_0c_1) \ , \ a_0 = b_0c_0 \end{cases} \quad - ⑯$$

이때 식 ⑯을 $g(x)$의 계수에 대입하면, $g(x)$는 다음과 같이 나타난다.

$$\begin{aligned} g(x) &= \frac{1}{4}a_4x^4 + \frac{1}{6}a_3x^3 + \frac{1}{2}a_2x^2 + a_1x + a_0 \\ &= \frac{1}{4}b_2c_2x^4 + \frac{1}{6}\cdot 3(b_2c_1 + b_1c_2)x^3 \\ &\quad + \frac{1}{2}(b_2c_0 + 2b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\ &= \frac{1}{4}b_2c_2x^4 + \frac{1}{2}(b_2c_1 + b_1c_2)x^3 \\ &\quad + \frac{1}{2}(b_2c_0 + 2b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0 \\ &= \frac{1}{4}\left\{ \begin{array}{l} b_2c_2x^4 + 2(b_2c_1 + b_1c_2)x^3 \\ \quad + 2(b_2c_0 + 2b_1c_1 + b_0c_2)x^2 + 4(b_1c_0 + b_0c_1)x + 4b_0c_0 \end{array} \right\} \\ &= \frac{1}{4}\left[\begin{array}{l} b_2c_2x^4 + \{b_2(2c_1) + (2b_1)c_2\}x^3 \\ \quad + \{b_2(2c_0) + (2b_1)(2c_1) + (2b_0)c_2\}x^2 \\ \quad + \{(2b_1)(2c_0) + (2b_0)(2c_1)\}x + (2b_0)(2c_0) \end{array} \right] \\ &= \frac{1}{4}(b_2x^2 + 2b_1x + 2b_0)(c_2x^2 + 2c_1x + 2c_0) \end{aligned}$$

이때 원시다항식 $g(x)$는 유리수체 $\mathbb{Q}$위에서 인수분해 되므로 정리 2.14에 의해 $g(x)$는 정수환 $\mathbb{Z}$위에서 이차식과 이차식으로 인수분해 된다. 따라서 모순이다.

Ⅰ,Ⅱ에 의해 $g(x)$가 $\mathbb{Z}[x]$에서 기약일 때 $f(x)$가 $h(\mathbb{Z})$에서 기약이다. ■

한편 정리 4.11는 원시다항식 $f(x) = 6a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$가 $4 \mid a_4$인 경우를 살펴보았다. 다음으로 $4 \nmid a_4$인 경우 $f(x)$의 기약성을 살펴보려고 했지만 해결하지 못했다. 그러므로 $2 \nmid a_4$인 경우 $f(x)$의 기약성에 대해서만 살펴보도

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

록 하자.

(보조정리 4.12) 환 $h(\mathbb{Z})$에서 기약이 아닌

$$f(x) = 6a_4x^4 + 3a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$$

에서 $2 \nmid a_4$ 이면 적당한 두 개의 기약 다항식

$$(b_2x^2 + b_1x + b_0)\ ,\ (c_2x^2 + c_1x + c_0) \in h(\mathbb{Z})$$

가 존재해서

$$f(x) = (b_2x^2 + b_1x + b_0) * (c_2x^2 + c_1x + c_0)$$

로 표현 된다.

증명 만약 $f(x)$가 일차식과 삼차식으로 인수분해 되면 $4 \mid a_4$이다. 이때 $2 \mid a_4$ 이므로 모순이 생긴다. 따라서 $f(x)$는 이차식과 이차식으로 인수분해 된다. ■

(정리 4.13) 임의의 $(a_4, a_3, a_2, a_1, a_0 \in \mathbb{Z})$ 에 대해,
$a_4 \neq 0$, $\gcd(6a_4, a_3, a_2, a_1, a_0) = 1$, $2 \nmid a_4$, $2 \mid a_2$, $2 \mid a_1$, $4 \mid a_0$ 이고

$$g(x) = a_4x^4 + a_3x^3 + \frac{1}{2}a_2x^2 + \frac{1}{2}a_1x + \frac{1}{4}a_0 \in \mathbb{Z}[x]$$
$$f(x) = 6a_4x^4 + 3a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$$

라고 하면 $g(x)$가 $\mathbb{Z}[x]$에서 기약 일 때 $f(x)$는 $h(\mathbb{Z})$에서 기약이다.

증명 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약일 때, 다항식 $f(x)$는 $h(\mathbb{Z})$에서 기약이 아니라고 해보자.
이 때 $f(x) = 6a_4x^4 + 3a_3x^3 + a_2x^2 + a_1x + a_0 \in h(\mathbb{Z})$, $2 \nmid a_4$ 인 기약이 아닌 다항식 이므로 보조정리 4.12에 의해 적당한 두 개의 기약 다항식
$(b_2x^2 + b_1x + b_0)$, $(c_2x^2 + c_1x + c_0) \in h(\mathbb{Z})$가 존재해서
$f(x) = (b_2x^2 + b_1x + b_0) * (c_2x^2 + c_1x + c_0)$로 표현 된다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$f(x) = (b_2x^2 + b_1x + b_0) * (c_2x^2 + c_1x + c_0) \qquad (b_2 \neq 0, c_2 \neq 0)$$

$$= \binom{4}{2}b_2c_2x^4 + \left(\binom{3}{2}b_2c_1 + \binom{3}{1}b_1c_2\right)x^3$$

$$+ \left(\binom{2}{2}b_2c_0 + \binom{2}{1}b_1c_1 + \binom{2}{0}b_0c_2\right)x^2 + \left(\binom{1}{1}b_1c_0 + \binom{1}{0}b_0c_1\right)x + \binom{0}{0}b_0c_0$$

$$= 6b_2c_2x^4 + (3b_2c_1 + 3b_1c_2)x^3$$

$$+ (b_2c_0 + 2b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0$$

$$= 6a_4x^4 + 3a_3x^3 + a_2x^2 + a_1x + a_0$$

따라서,

$$\begin{cases} a_4 = b_2c_2 \ , \ a_3 = (b_1c_2 + b_2c_1) \\ a_2 = (b_2c_0 + 2b_1c_1 + b_0c_2) \ , \ a_1 = (b_1c_0 + b_0c_1) \ , \ a_0 = b_0c_0 \end{cases} \qquad -⑰$$

이때 식 ⑰을 $g(x)$에 대입하면, $g(x)$는 다음과 같이 나타난다.

$$g(x) = a_4x^4 + a_3x^3 + \frac{1}{2}a_2x^2 + \frac{1}{2}a_1x + \frac{1}{4}a_0$$

$$= b_2c_2x^4 + (b_1c_2 + b_2c_1)x^3$$

$$+ \frac{1}{2}(b_2c_0 + 2b_1c_1 + b_0c_2)x^2 + \frac{1}{2}(b_1c_0 + b_0c_1)x + \frac{1}{4}b_0c_0$$

$$= \frac{1}{4}\left\{\begin{array}{l} 4b_2c_2x^4 + 4(b_1c_2 + b_2c_1)x^3 \\ + 2(b_2c_0 + 2b_1c_1 + b_0c_2)x^2 + 2(b_1c_0 + b_0c_1)x + b_0c_0 \end{array}\right\}$$

$$= \frac{1}{4}\left[\begin{array}{l} (2b_2)(2c_2)x^4 + \{(2b_1)(2c_2) + (2b_2)(2c_1)\}x^3 \\ + \{(2b_2)c_0 + (2b_1)(2c_1) + b_0(2c_2)\}x^2 \\ + \{(2b_1)c_0 + b_0(2c_1)\}x + b_0c_0 \end{array}\right]$$

$$= \frac{1}{4}(2b_2x^2 + 2b_1x + b_0)(2c_2x^2 + 2c_1x + c_0)$$

이때 $g(x)$는 유리수체 $\mathbb{Q}$위에서 인수분해 되므로 정리 2.14에 의해 $g(x)$는 정수환

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$\mathbb{Z}$위에서도 인수분해 된다. 따라서 모순이다. 그러므로 $g(x)$가 $\mathbb{Z}[x]$에서 기약일 때 $f(x)$가 $h(\mathbb{Z})$에서 기약이다. ■

한편, $f(x)$가 $h(\mathbb{Z})$에서 기약일 때 $g(x)$가 $\mathbb{Z}[x]$에서 기약인 것은 성립할 것 같으나 밝히지는 못했다. 이에 대한 후속 연구가 필요할 것으로 보인다.

지금까지 정수계수를 갖는 4차 Hurwitz 다항식의 기약성에 대해 알아보았다. 4차 이상의 고차 Hurwitz 다항식의 기약성은 알아내는 것이 쉽지 않다. 하지만 앞선 내용을 토대로 정수계수를 갖는 n차 Hurwitz 다항식의 기약성을 다음과 같이 알 수 있다.

(정리 4.14) 적당한 a_n , a_{n-1} ,$\cdots$, a_i ,$\cdots$, a_1 , $a_0 \in \mathbb{Z}$에 대해, $(n \geq 2)$ $a_n \neq 0$, $\gcd(na_n, a_{n-1}, \cdots, a_i, \cdots, a_0) = 1$, $(n-1)!|a_n$, $i!|a_i$ $(0 \leq i \leq n-1)$이면 다음 두 조건이 동치이다.

1. $f(x) = na_nx^n + a_{n-1} + \cdots + a_ix^i + \cdots + a_0 \in h(\mathbb{Z})$에서 기약 이다.
2. $g(x) = \frac{1}{(n-1)!}a_nx^n + \frac{1}{(n-1)!}a_{n-1}x^{n-1} + \cdots + \frac{1}{i!}a_ix^i + \cdots + a_0 \in \mathbb{Z}[x]$에서 기약이다.

증명 (1)⟹(2) 다항식 $f(x)$가 $h(\mathbb{Z})$에서 기약 일 때 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약이 아니라고 하자.

$\gcd(na_n, \cdots, a_i, \cdots, a_0) = 1$이면 $\gcd(\frac{1}{(n-1)!}a_n, \frac{1}{(n-1)!}a_{n-1}, \cdots, \frac{1}{i!}a_i, \cdots, a_0) = 1$ 이다. $g(x)$가 $\mathbb{Z}[x]$위에서 기약이 아닌 원시다항식이므로 $g(x)$는 상수다항식이 아닌 두 개의 정수환다항식의 곱으로 표현된다.

$1 \leq s \leq n-1$, $1 \leq t \leq n-1$, $s+t=n$ 을 만족하는 s , t 에 대해 적당한 두 다항식

$$(b_sx^s + \cdots + b_jx^j + \cdots + b_0), (c_tx^t + \cdots + c_kx^k + \cdots + c_0) \in \mathbb{Z}[x]$$

이 존재해서 $g(x)$는 다음과 같이 나타난다.

$$g(x) = (b_sx^s + \cdots + b_jx^j + \cdots + b_0)(c_tx^t + \cdots + c_kx^k + \cdots + c_0) \quad (b_s \neq 0, c_t \neq 0)$$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$= b_s c_t x^n + (b_s c_{t-1} + b_{s-1} c_t) x^{n-1}$$

$$+ \cdots + (b_i c_0 + \cdots + b_k c_{i-k} + \cdots + b_0 c_i) x^i + \cdots + (b_1 c_0 + b_0 c_1) x + b_0 c_0$$

$$= \frac{1}{(n-1)!} a_n x^n + \frac{1}{(n-1)!} a_{n-1} x^{n-1} + \cdots + \frac{1}{i!} a_i x^i + \cdots + a_1 x + a_0$$

따라서,

$$\begin{cases} a_n = (n-1)! b_s c_t \\ a_i = i!(b_i c_0 + \cdots + b_k c_{i-k} + \cdots + b_0 c_i), (0 \le i \le n-1, k \le i) \end{cases} \quad -⑱$$

이때 식 ⑱를 $f(x)$의 계수에 대입하면 $f(x)$는 다음과 같이 나타난다.

$$f(x) = n a_n x^n + \cdots + a_i x^i + \cdots + a_0$$

$$= n! b_s c_t x^n + (n-1)!(b_s c_{t-1} + b_{s-1} c_t) x^{n-1} +$$

$$\cdots + i!(b_i c_0 + \cdots + b_k c_{i-k} + \cdots + b_0 c_i) x^i + \cdots + (b_1 c_0 + b_0 c_1) x + b_0 c_0$$

$$= \frac{n!}{s!t!} s!t! b_s c_t x^n$$

$$+ \left\{ \frac{(n-1)!}{s!(t-1)!} s!(t-1)! b_s c_{t-1} + \frac{(n-1)!}{(s-1)!t!} (s-1)!t! b_{s-1} c_t \right\} x^{n-1}$$

$$+ \cdots + \left\{ \frac{i!}{i!0!} i!0! b_i c_0 + \cdots + \frac{i!}{k!(i-k)!} k!(i-k)! b_k c_{i-k} + \cdots + \frac{i!}{0!i!} 0!i! b_0 c_i \right\} x^i$$

$$+ \cdots + \left\{ \frac{1!}{1!0!} 1!0! b_1 c_1 + \frac{1!}{0!1!} 0!1! b_0 c_1 \right\} x + \frac{0!}{0!0!} 0!0! b_0 c_0$$

$$= \binom{n}{s} (s! b_s)(t! c_t) x^n$$

$$+ \left\{ \binom{n-1}{s} (s! b_s)((t-1)! c_{t-1}) + \binom{n-1}{s-1} ((s-1)! b_{s-1})(t! c_t) \right\} x^{n-1}$$

$$+ \cdots + \left\{ \binom{i}{i} (i! b_i)(0! c_0) + \cdots + \binom{i}{k} (k! b_k)((i-k)! c_{i-k}) + \cdots + \binom{i}{0} (0! b_0)(i! c_i) \right\} x^i$$

$$+ \cdots + \left\{ \binom{1}{1} (1! b_1)(0! c_0) + \binom{1}{0} (0! b_0)(1! c_1) \right\} x + \binom{0}{0} (0! b_0)(0! c_0)$$

$$= (s! b_s x^s + \cdots + j! b_j x^j + \cdots + 0! b_0) * (t! c_t x^t + \cdots + k! c_k x^k + \cdots + 0! c_0)$$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

이는 $f(x)$가 $h(\mathbb{Z})$에서 기약이라는 가정에 모순이 생긴다. 따라서 $f(x)$가 $h(\mathbb{Z})$에서 기약이면 $g(x)$도 $\mathbb{Z}[x]$에서 기약이다.

(2)⟹(1) 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약 일 때 다항식 $f(x)$가 $h(\mathbb{Z})$에서 기약이 아니라고 하자.
$f(x)$는 $h(\mathbb{Z})$위에서 기약이 아닌 원시다항식이므로 $f(x)$는 상수다항식이 아닌 두 개의 Hurwitz 다항식의 곱으로 표현된다.

$1 \le s \le n-1$, $1 \le t \le n-1$, $s+t=n$ 을 만족하는 s , t 에 대해 적당한 두 다항식

$$(b_s x^s + \cdots + b_j x^j + \cdots + b_0), (c_t x^t + \cdots + c_k x^k + \cdots + c_0) \in h(\mathbb{Z})$$

이 존재해서 $f(x)$는 다음과 같이 표현된다.

$$f(x) = (b_s x^s + \cdots + b_j x^j + \cdots + b_0) * (c_t x^t + \cdots + c_k x^k + \cdots + c_0) \quad (b_s \neq 0, c_t \neq 0)$$

$$= \binom{n}{s} b_s c_t x^n + \left(\binom{n-1}{s} b_s c_{t-1} + \binom{n-1}{s-1} b_{s-1} c_t \right) x^{n-1}$$

$$+ \cdots + \left(\binom{i}{i} b_i c_0 + \cdots + \binom{i}{k} b_k c_{i-k} + \cdots + \binom{i}{0} b_0 c_i \right) x^i$$

$$+ \cdots + \left(\binom{1}{1} b_1 c_0 + \binom{1}{0} b_0 c_1 \right) x + \binom{0}{0} b_0 c_0$$

$$= n a_n x^n + a_{n-1} x^{n-1} + \cdots + a_i x^i + \cdots + a_1 + a_0$$

따라서,

$$\begin{cases} a_n = \dfrac{(n-1)!}{s!t!} b_s c_t \\ a_i = \left\{ \binom{i}{i} b_i c_0 + \cdots + \binom{i}{k} b_k c_{i-k} + \cdots + \binom{i}{0} b_0 c_i \right\}, (0 \le i \le n-1, k \le i) \end{cases} \quad -⑲$$

이때 식 ⑲을 $g(x)$의 계수에 대입하면 $g(x)$는 다음과 같이 나타난다.

$$g(x) = \frac{1}{(n-1)!} a_n x^n + \frac{1}{(n-1)!} a_{n-1} x^{n-1} + \cdots + \frac{1}{i!} a_i x^i + \cdots + a_1 x + a_0$$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$= \frac{1}{(n-1)!}\frac{(n-1)!}{s!t!}b_s c_t x^n + \frac{1}{(n-1)!}\left\{\frac{(n-1)!}{s!(t-1)!}b_s c_t + \frac{(n-1)!}{(s-1)!t!}b_{s-1}c_t\right\}x^{n-1}$$

$$+ \cdots + \frac{1}{i!}\left\{\frac{i!}{i!0!}b_i c_0 + \cdots + \frac{i!}{k!(i-k)!}b_k c_{i-k} + \cdots + \frac{i!}{0!i!}b_0 c_i\right\}x^i$$

$$+ \cdots + \frac{1}{1!}\left\{\frac{1!}{1!0!}b_1 c_0 + \frac{1!}{0!1!}b_0 c_1\right\}x + \frac{1}{0!}\frac{0!}{0!0!}b_0 c_0$$

$$= \frac{1}{s!t!}b_s c_t x^n + \left\{\frac{1}{s!(t-1)!}b_s c_t + \frac{1}{(s-1)!t!}b_{s-1}c_t\right\}x^{n-1}$$

$$+ \cdots + \left\{\frac{1}{i!0!}b_i c_0 + \cdots + \frac{1}{k!(i-k)!}b_k c_{i-k} + \cdots + \frac{1}{0!i!}b_0 c_i\right\}x^i$$

$$+ \cdots + \left\{\frac{1}{1!0!}b_1 c_0 + \frac{1}{0!1!}b_0 c_1\right\}x + \frac{1}{0!0!}b_0 c_0$$

$$= \left(\frac{1}{s!}b_s\right)\left(\frac{1}{t!}c_t\right)x^n + \left\{\left(\frac{1}{s!}b_s\right)\left(\frac{1}{(t-1)!}c_{t-1}\right) + \left(\frac{1}{(s-1)!}b_{s-1}\right)\left(\frac{1}{t!}c_t\right)\right\}x^{n-1}$$

$$+\cdots+ \left\{\left(\frac{1}{i!}b_i\right)\left(\frac{1}{0!}c_0\right)+\cdots+\left(\frac{1}{k!}b_k\right)\left(\frac{1}{(i-k)!}c_{i-k}\right)+\cdots+\left(\frac{1}{0!}b_0\right)\left(\frac{1}{i!}c_i\right)\right\}x^i$$

$$+ \cdots+ \left\{\left(\frac{1}{1!}b_1\right)\left(\frac{1}{0!}c_0\right) + \left(\frac{1}{0!}b_0\right)\left(\frac{1}{1!}c_1\right)\right\}x + \left(\frac{1}{0!}b_0\right)\left(\frac{1}{0!}c_0\right)$$

$$= \left(\frac{1}{s!}b_s x^s + \cdots + \frac{1}{j!}b_j x^j + \cdots + \frac{1}{0!}b_0\right)\left(\frac{1}{t!}c_t x^t + \cdots + \frac{1}{k!}c_k x^k + \cdots + \frac{1}{0!}c_0\right)$$

$$= \frac{1}{s!t!}\left({}_sP_0 b_s x^s + \cdots + {}_sP_{s-j}b_j x^j + \cdots + {}_sP_s b_0\right)\left({}_tP_0 c_t x^t + \cdots + {}_tP_{t-k}c_k x^k + \cdots + {}_tP_t c_0\right)$$

이때 원시다항식 $g(x)$는 유리수체 $\mathbb{Q}$위에서 인수분해 되므로 정리 2.14에 의해 정수환 $\mathbb{Z}$위에서 $g(x)$는 인수분해 된다. 따라서 모순이다. 그러므로 $g(x)$가 $\mathbb{Z}[x]$에서 기약일 때 $f(x)$가 $h(\mathbb{Z})$에서 기약이다. ■

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

(따름정리 4.15) 적당한 a_n , a_{n-1} ,⋯, a_i ,⋯, a_1 , $a_0 \in \mathbb{Z}$에 대해,
$a_n \neq 0$, $\gcd((n-1)!a_n, a_{n-1},\cdots, a_i, \cdots, a_0) = 1$, $n | a_n$, $i! | a_i$ $(0 \leq i \leq n-1)$이면 다음 두 조건이 동치이다.

1. $f(x) = (n-1)!a_n x^n + a_{n-1}x^{n-1} + \cdots + a_i x^i + \cdots + a_0 \in h(\mathbb{Z})$에서 기약 이다.
2. $g(x) = \frac{1}{n}a_n x^n + \frac{1}{(n-1)!}a_{n-1}x^{n-1} \cdots + \frac{1}{i!}a_i x^i + \cdots + a_0 \in \mathbb{Z}[x]$에서 기약이다.

증명 (1)⟹(2) 다항식 $f(x)$가 $h(\mathbb{Z})$에서 기약 일 때 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약이 아니라고 하자.

$\gcd((n-1)!a_n, \cdots, a_i, \cdots, a_0) = 1$이면 $\gcd(\frac{1}{n}a_n, \frac{1}{(n-1)!}a_{n-1}, \cdots, \frac{1}{i!}a_i, \cdots, a_0) = 1$ 이다.

$g(x)$가 $\mathbb{Z}[x]$위에서 기약이 아닌 원시다항식이므로 $g(x)$는 상수다항식이 아닌 두 개의 정수환다항식의 곱으로 표현된다.

$1 \leq s \leq n-1$, $1 \leq t \leq n-1$, $s+t=n$ 을 만족하는 s , t 에 대해 적당한 두 다항식

$$(b_s x^s + \cdots + b_j x^j + \cdots + b_0), (c_t x^t + \cdots + c_k x^k + \cdots + c_0) \in \mathbb{Z}[x]$$

이 존재해서 $g(x)$는 다음과 같이 나타난다.

$$g(x) = (b_s x^s + \cdots + b_j x^j + \cdots + b_0)(c_t x^t + \cdots + c_k x^k + \cdots + c_0) \quad (b_s \neq 0, c_t \neq 0)$$

$$= b_s c_t x^n + (b_s c_{t-1} + b_{s-1}c_t)x^{n-1}$$

$$+ \cdots + (b_i c_0 + \cdots + b_k c_{i-k} + \cdots + b_0 c_i)x^i + \cdots + (b_1 c_0 + b_0 c_1)x + b_0 c_0$$

$$= \frac{1}{n}a_n x^n + \frac{1}{(n-1)!}a_{n-1}x^{n-1} + \cdots + \frac{1}{i!}a_i x^i + \cdots + a_1 x + a_0$$

따라서,

$$\begin{cases} a_n = n b_s c_t \\ a_i = i!(b_i c_0 + \cdots + b_k c_{i-k} + \cdots + b_0 c_i), (0 \leq i \leq n-1, k \leq i) \end{cases} \quad -⑳$$

이때 식 ⑳를 $f(x)$의 계수에 대입하면 $f(x)$는 다음과 같이 나타난다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$
\begin{aligned}
f(x) &= (n-1)!a_n x^n + \cdots + a_i x^i + \cdots + a_0 \\
&= n!b_s c_t x^n + (n-1)!(b_s c_{t-1} + b_{s-1}c_t)x^{n-1} + \\
&\qquad \cdots + i!(b_i c_0 + \cdots + b_k c_{i-k} + \cdots + b_0 c_i)x^i + \cdots + (b_1 c_0 + b_0 c_1)x + b_0 c_0 \\
&= \frac{n!}{s!t!} s!t!b_s c_t x^n \\
&\quad + \left\{ \frac{(n-1)!}{s!(t-1)!} s!(t-1)!\, b_s c_{t-1} + \frac{(n-1)!}{(s-1)!t!}(s-1)!t!b_{s-1}c_t \right\} x^{n-1} \\
&\quad + \cdots + \left\{ \frac{i!}{i!0!} i!0!b_i c_0 + \cdots + \frac{i!}{k!(i-k)!} k!(i-k)!b_k c_{i-k} + \cdots + \frac{i!}{0!i!} 0!i!b_0 c_i \right\} x^i \\
&\quad + \cdots + \left\{ \frac{1!}{1!0!} 1!0!\, b_1 c_1 + \frac{1!}{0!1!} 0!1!b_0 c_1 \right\} x + \frac{0!}{0!0!} 0!0!b_0 c_0 \\
&= \binom{n}{s}(s!b_s)(t!c_t)x^n \\
&\quad + \left\{ \binom{n-1}{s}(s!b_s)((t-1)!c_{t-1}) + \binom{n-1}{s-1}((s-1)!b_{s-1})(t!c_t) \right\} x^{n-1} \\
&\quad + \cdots + \left\{ \binom{i}{i}(i!b_i)(0!c_0) + \cdots + \binom{i}{k}(k!b_k)((i-k)!c_{i-k}) + \cdots + \binom{i}{0}(0!b_0)(i!c_i) \right\} x^i \\
&\quad + \cdots + \left\{ \binom{1}{1}(1!b_1)(0!c_0) + \binom{1}{0}(0!b_0)(1!c_1) \right\} x + \binom{0}{0}(0!b_0)(0!c_0) \\
&= (s!b_s x^s + \cdots + j!b_j x^j + \cdots + 0!b_0) * (t!c_t x^t + \cdots + k!c_k x^k + \cdots + 0!c_0)
\end{aligned}
$$

이는 $f(x)$가 $h(\mathbb{Z})$에서 기약이라는 가정에 모순이 생긴다. 따라서 $f(x)$가 $h(\mathbb{Z})$에서 기약이면 $g(x)$도 $\mathbb{Z}[x]$에서 기약이다.

(2)⟹(1) 다항식 $g(x)$가 $\mathbb{Z}[x]$에서 기약 일 때 다항식 $f(x)$가 $h(\mathbb{Z})$에서 기약이 아니라고 하자.
$f(x)$는 $h(\mathbb{Z})$위에서 기약이 아닌 원시다항식이므로 $f(x)$는 상수다항식이 아닌 두 개의 Hurwitz 다항식의 곱으로 표현된다.

$1 \le s \le n-1$, $1 \le t \le n-1$, $s+t=n$ 을 만족하는 s , t 에 대해 적당한 두 다항식

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$(b_s x^s + \cdots + b_j x^j + \cdots + b_0), (c_t x^t + \cdots + c_k x^k + \cdots + c_0) \in h(\mathbb{Z})$$

이 존재해서 $f(x)$는 다음과 같이 표현된다.

$$f(x) = (b_s x^s + \cdots + b_j x^j + \cdots + b_0) * (c_t x^t + \cdots + c_k x^k + \cdots + c_0) \quad (b_s \neq 0, c_t \neq 0)$$

$$= \binom{n}{s} b_s c_t x^n + \left(\binom{n-1}{s} b_s c_{t-1} + \binom{n-1}{s-1} b_{s-1} c_t \right) x^{n-1}$$

$$+ \cdots + \left\{ \binom{i}{i} b_i c_0 + \cdots + \binom{i}{k} b_k c_{i-k} + \cdots + \binom{i}{0} b_0 c_i \right\} x^i$$

$$+ \cdots + \left\{ \binom{1}{1} b_1 c_0 + \binom{1}{0} b_0 c_1 \right\} x + \binom{0}{0} b_0 c_0$$

$$= (n-1)! a_n x^n + a_{n-1} x^{n-1} + \cdots + a_i x^i + \cdots + a_0$$

따라서,

$$\begin{cases} a_n = \dfrac{n}{s!t!} b_s c_t \\ a_i = \left\{ \binom{i}{i} b_i c_0 + \cdots + \binom{i}{k} b_k c_{i-k} + \cdots + \binom{i}{0} b_0 c_i \right\}, (0 \leq i \leq n-1, k \leq i) \end{cases} \quad -㉑$$

이때 식 ㉑을 $g(x)$의 계수에 대입하면 $g(x)$는 다음과 같이 나타난다.

$$g(x) = \frac{1}{n} a_n x^n + \frac{1}{(n-1)!} a_{n-1} x^{n-1} + \cdots + \frac{1}{i!} a_i x^i + \cdots + a_1 x + a_0$$

$$= \frac{1}{n} \frac{n}{s!t!} b_s c_t x^n + \frac{1}{(n-1)!} \left\{ \frac{(n-1)!}{s!(t-1)!} b_s c_t + \frac{(n-1)!}{(s-1)!t!} b_{s-1} c_t \right\} x^{n-1}$$

$$+ \cdots + \frac{1}{i!} \left\{ \frac{i!}{i!0!} b_i c_0 + \cdots + \frac{i!}{k!(i-k)!} b_k c_{i-k} + \cdots + \frac{i!}{0!i!} b_0 c_i \right\} x^i$$

$$+ \cdots + \frac{1}{1!} \left\{ \frac{1!}{1!0!} b_1 c_0 + \frac{1!}{0!1!} b_0 c_1 \right\} x + \frac{1}{0!} \frac{0!}{0!0!} b_0 c_0$$

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

$$= \frac{1}{s!t!}b_s c_t x^n + \left\{ \frac{1}{s!(t-1)!}b_s c_t + \frac{1}{(s-1)!t!}b_{s-1}c_t \right\} x^{n-1}$$

$$+ \cdots + \left\{ \frac{1}{i!0!}b_i c_0 + \cdots + \frac{1}{k!(i-k)!}b_k c_{i-k} + \cdots + \frac{1}{0!i!}b_0 c_i \right\} x^i$$

$$+ \cdots + \left\{ \frac{1}{1!0!}b_1 c_0 + \frac{1}{0!1!}b_0 c_1 \right\} x + \frac{1}{0!0!}b_0 c_0$$

$$= \left(\frac{1}{s!}b_s\right)\left(\frac{1}{t!}c_t\right)x^n + \left\{ \left(\frac{1}{s!}b_s\right)\left(\frac{1}{(t-1)!}c_{t-1}\right) + \left(\frac{1}{(s-1)!}b_{s-1}\right)\left(\frac{1}{t!}c_t\right) \right\} x^{n-1}$$

$$+\cdots+ \left\{ \left(\frac{1}{i!}b_i\right)\left(\frac{1}{0!}c_0\right)+\cdots+\left(\frac{1}{k!}b_k\right)\left(\frac{1}{(i-k)!}c_{i-k}\right)+\cdots+\left(\frac{1}{0!}b_0\right)\left(\frac{1}{i!}c_i\right) \right\} x^i$$

$$+ \cdots+ \left\{ \left(\frac{1}{1!}b_1\right)\left(\frac{1}{0!}c_0\right) + \left(\frac{1}{0!}b_0\right)\left(\frac{1}{1!}c_1\right) \right\} x + \left(\frac{1}{0!}b_0\right)\left(\frac{1}{0!}c_0\right)$$

$$= \left(\frac{1}{s!}b_s x^s + \cdots+ \frac{1}{j!}b_j x^j + \cdots + \frac{1}{0!}b_0\right)\left(\frac{1}{t!}c_t x^t + \cdots + \frac{1}{k!}c_k x^k + \cdots + \frac{1}{0!}c_0\right)$$

$$= \frac{1}{s!t!}\left({}_sP_0\, b_s x^s + \cdots + {}_sP_{s-j}\, b_j x^j + \cdots + {}_sP_s\, b_0\right)\left({}_tP_0\, c_t x^t + \cdots + {}_tP_{t-k}\, c_k x^k + \cdots + {}_tP_t\, c_0\right)$$

이때 원시다항식 $g(x)$는 유리수체 $\mathbb{Q}$위에서 인수분해 되므로 정리 2.14에 의해 정수환 $\mathbb{Z}$위에서 $g(x)$는 인수분해 된다. 따라서 모순이다. 그러므로 $g(x)$가 $\mathbb{Z}[x]$에서 기약일 때 $f(x)$가 $h(\mathbb{Z})$에서 기약이다. ■

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

참고문헌

[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] J.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] J.W. Lim and D.Y. Oh, Composite Hurwitz rings satisfying the ascending chain conditions on principal ideals, Kyungpook Math. J. 56 (2016) 1115-1123.

[7] J.W. Lim and D.Y. Oh, Chain conditions on composite Hurwitz series rings, Open Mathematics, 15 (2017) 1161-1170.

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

[9] 김응태 · 박승안, 현대대수학 제8판, 경문사 (2011).

[10] 정학진, Hurwitz 다항식 환의 대수적 성질 연구, 조선대학교 석사학위 논문 (2016).

Collection @ chosun