$F[x]$에서 계산

추상대수학(abstract algebra)

4.1 다항식 계산과 나눗셈 알고리즘

$$x^2+3x-5,\ 6x^3-3x^2+7x+4,\ x^{12}-1$$

: 실수계수를 갖는 다항식들

R은 임의의 환이라 하자. R의 원소를 계수로 갖는 다항식(polynomial with coefficients in R)은

$$a_0+a_1x+a_2x^2+a_3x^3+\ldots+a_nx^n$$

꼴의 식(expression)이다. 여기서 $a_i\in R$.

각 a_i를 이 다항식의 계수(coefficient)

x를 부정원(indeterminate)[R위에서 초월원(transcendental element)]이라 한다.

이점에서, "무엇이 부정원인가?"

첫째 :

"마치 부정원 x를 환 R의 원인 것처럼 이 x를 취급한다" ?

그러면 $a_0+a_1x+a_2x^2+\ldots+a_nx^n$꼴의 식은 의미가 있다.

둘째 : x를 다항식 자체에 있는 실체(entity)로 취급한다.

즉, 주어진 환 R에 대하여, 부분환으로 R을 포함하고 다음의 성질을 만족하고 특별한 원 x를 포함하는 ($R[x]$로 표시되는) 더 큰 환이 존재함을 증명할 수 있다. 더 큰 환 $R[x]$의 원을 다항식이라 하고 특별한 원 x를 부정원이라 한다.

(i) $xa=ax\ \ \forall a\in R$,

(ii) $R[x]$의 모든 원은

$$a_0+a_1x+a_2x^2+\ldots+a_nx^n$$

꼴로 쓰여질 수 있다. 여기서 $n\geq 0$이고 $a_i\in R$,

(iii) (ii)에서와 같은 $R[x]$의 원들의 표시는 다음의 의미에서

유일하다: $n \le m$이고

$$a_0 + a_1x + a_2x^2 + \dots a_nx^n = b_0 + b_1x + b_2x^2 + \dots + b_mx^m$$

이면,

$i \le n$에 대하여 $a_i = b_i$이고

$i > n$에 대하여 $b_i = 0_R$이다.

임의의 환의 원과 영원 0_R의 곱은 바로 0_R이므로, 다항식에서 영계수를 갖는 항들은 생략되거나 필요에 따라서 삽입될 수 있다.

▌보기 4.1.1▐ $\mathbb{R}[x]$에서 다항식 $2+0x-x^2+0x^3+5x^4$은 보통 $2-x^2+5x^4$으로 쓴다. 우리가 다항식 $1+x^2$과 $4+x+2x^3$을 위와 같은 거듭제곱으로 나태내고 싶으면, 우리는 다음과 같이 쓴다:

$$1+0x+x^2+0x^3 \text{과 } 4+x+0x+2x^3.$$

■

▌보기 4.1.2▐ $f(x) = 1+5x-x^2+4x^3+2x^4$과 $g(x) = 4+2x+x^2+x^3$이 $\mathbb{Z}_7[x]$의 원이면, 교환, 결합과 분배법칙은 다음의 결과를 보여준다 :

$$f(x)+g(x) = (1+5x-x^2+4x^3+2x^4)+(4+2x+3x^2+x^3+0x^4)$$
$$= (1+4)+(5+2)x+(-1+3)x^2+(4+1)x^3+(2+0)x^4$$
$$= 5+0x+2x^2+5x^3+2x^4 = 5+2x^2+5x^3+2x^4. \quad ■$$

▌보기 4.1.3▐ $\mathbb{Q}[x]$에서 $1-7x+x^2$과 $2+3x$의 곱은 분배법칙을 반복하여 사용함으로써 얻어진다 :

$$(1-7x+x^2)(2+3x) = 1(2+3x)-7x(2+3x)+x^2(2+3x)$$
$$= 1(2)+1(3x)-7x(2)-7x(3x)+x^2(2)+x^2(3x)$$
$$= 2+3x-14x-21x^2+2x^2+3x^3$$

$$= 2-11x-19x^2+3x^3. \quad ■$$

다항식덧셈(polynomial addition)

$$(a_0+a_1x+a_2x^2+\cdots+a_nx^n)+(b_0+b_1x+b_2x^2+\cdots+b_mx^m),\ m<n$$
$$= (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_n+b_n)x^n, b_i = 0, m<i$$

다항식곱셈(polynomial multiplication)

$$(a_0+a_1x+a_2x^2+\dots+a_nx^n)(b_0+b_1x+b_2x^2+\dots+b_mx^m)$$
$$= a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1+a_2b_0)x^2+\cdots+a_nb_mx^{n+m}$$

각 $k \geq 0$에 대하여, 이 곱에서 x^k의 계수는

$$a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \cdots + a_{k-2}b_2 + a_{k-1}b_1 + a_kb_0 = \sum_{i=0}^{k} a_ib_{k-i}$$

여기서 $i > n$이면 $a_i = 0_R$이고 $j > m$이면 $b_j = 0_R$ 이다.

$R[x]$에서 곱셈에 대한 이 설명으로부터, R이 가환환이면 $R[x]$ 역시 가환환이 된다는 것은 쉬운 결과다(예제 4.1.1).

R이 곱의 항등원 1_R을 가지면, 1_R은 역시 $R[x]$의 곱의 항등원이다(유제 4.1.1).

정의 4.1.1

$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$은 $a_n \neq 0_R$인 $R[x]$에서 다항식이라 하자. 그러면 a_n을 $f(x)$의 최고차계수(leading coefficient)라 한다. 이때, 정수 n을 $f(x)$의 차수(degree)라 하고, "$\deg f(x)$"로 나타낸다. 다른 말로하면, $\deg f(x)$는 영이 아닌 계수와 함께 나타나는 x의 가장 큰 지수이고, 이 계수는 최고차계수다.

▌보기 4.1.4 ▐ $3 - x + 4x^2 - 7x^3 \in \mathbb{R}[x]$의 차수는 3이고, 이것의

최고차 계수는 -7이다.

$\deg(3 + 5x) = 1$이고

$\deg(x^{12}) = 12$.

$2 + x + 4x^2 - 0x^3 + 0x^5$의 차수는 2(영아닌 계수를 갖는 x의 가장 큰 지수)이고 이것의 최고차계수는 4이다. ■

환 R은 다항식 환 $R[x]$의 부분환이다.

R의 원을 $R[x]$의 상수다항식(constant polynomial)이라 한다.

$R[x]$에서 차수 0인 다항식은 정확하게 영이 아닌 상수다항식들이다.

상수다항식 $\mathbf{0_R}$은 차수를 갖지 않는다

는 사실에 주목하라(x의 어떠한 거듭제곱도 영이 아닌 계수와 함께 나타나지 않기 때문이다).

정리 4.1.2

R은 정역이고 $f(x)$와 $g(x)$는 $R[x]$의 영이 아닌 다항식이라 하자. 그러면 $\deg[f(x)g(x)] = \deg f(x) + \deg g(x)$.

►증명◄ $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$이고

$g(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m$이라 하자. 여기서

$a_n \neq 0_R$이고 $b_m \neq 0_R$. 그러면

$\deg f(x) = n$이고 $\deg g(x) = m$. 한편,

$$f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_2b_0 + a_1b_1 + a_2b_0)x^2 + \cdots + a_nb_mx^{n+m}$$

이 영이 아닌 계수를 가질 수 있는 x의 가장 큰 지수는

$n+m$이다. 그런데 R은 정역이고 $a_n \neq 0_R$, $b_m \neq 0_R$ 이므로, $a_nb_m \neq 0_R$이다. 따라서 $f(x)g(x)$는 영이 아닌 다항식이고

$$\deg[f(x)g(x)] = n + m = \deg f(x) + \deg g(x). \quad \blacksquare$$

따름정리 4.1.2

R이 정역이면, $R[x]$ 역시 정역이다.

►증명◄ R은 항등원이 있는 가환환이므로, $R[x]$역시 항등원이 있는 가환환이다(예제 4.1.1과 유제 4.1.1). 정리 4.1.2에 의해

$f(x) \neq 0, \deg f(x) = n$ $g(x) \neq 0, \deg g(x) = m$이면

$$\deg[f(x)g(x)] = \deg f(x) + \deg g(x)$$

이므로 $\deg[f(x)g(x)] = m+n$이다. 즉, $f(x)g(x) \neq 0$이다. 따라서 $R[x]$는 정역이다. $\blacksquare$

정리 4.1.2의 증명에서 R이 정역이 아니고 임의의 환 R일 때 $f(x)$, $g(x)$와 $f(x)g(x)$가 영이 아닌 다항식이면

$$\deg[f(x)g(x)] \leq \deg f(x) + \deg g(x)$$

임을 알 수 있다.

또한 환이 영인수를 가지면

$$\deg[f(x)g(x)] < \deg f(x) + \deg g(x)$$

도 가능하다. 예컨대, $\mathbb{Z}_6[x]$에서, $2x^4$은 차수 4를 갖고 $1+3x^2$은

차수 2를 갖는다. 그러나 이들의 곱은 차수 $4+2=6$을 갖지 않는다 :

$$2x^4(1+3x^2) = 2x^4 + 2\cdot 3x^6 = 2x^4 + 0x^6 = 2x^4$$

이다.

이장의 나머지에서 우리의 주된 관심은 ($\mathbb{Q}$, $\mathbb{R}$ 또는 $\mathbb{Z}_5$와 같은) 체 F에서 계수를 갖는 다항식들일 것이다. 이장의 머릿말에서 주의하였듯이, 정역 $F[x]$는 정수들의 정역 $\mathbb{Z}$와 많은 성질을 공유한다.

정리 4.1.3 $F[x]$에서 나눗셈 알고리즘

F는 체고 $f(x), g(x) \in F[x]$라 하자. 여기서 $g(x) \neq 0_F$이다. 그러면 꼭 하나의 다항식 $q(x)$와 $r(x)$가 존재하여 $f(x) = g(x)q(x) + r(x)$이고 $r(x) = 0_F$ 또는 $\deg r(x) < \deg g(x)$을 만족한다.

이 정리와 $\mathbb{Z}$에서 나눗셈 알고리즘 (정리 1.1.1)

임의의 정수 a와 $b > 0$에 대하여,

$\exists$ 꼭하나의 정수 q와 r $s.t.\ a = bq + r$ 이고 $0 \leq r < b$

을 비교하라. 여기에서 유일한 변화는 $\mathbb{Z}$에서 "$r < b$"와 같은 명

제를 $F(x)$애서 차수를 포함하는 명제로 바꾼 것이다. 여러분은 아마도 나눗셈 알고리즘을 사용하여 이와 같은 나눗셈 문제를 확인하였다. 여기서 여러분은 쉽사리 $f(x) = g(x)q(x) + r(x)$임을 증명할 수 있다:

$$\begin{array}{rl} & \frac{3}{2}x^2 + x + 1 \quad \leftarrow \text{몫 } q(x) \\ \text{나눗식 } g(x) \quad 2x^3+1 \;\Big| & 3x^5 + 2x^4 + 2x^3 + 4x^2 + x - 2 \quad \leftarrow \text{나뉨식 } f(x) \\ & \underline{3x^5 + \quad\quad \frac{3}{2}x^2} \quad \leftarrow \left(\frac{3}{2}x^2\right)g(x) \end{array}$$

$$\begin{array}{rl} & \\ \hline & 2x^4 + 2x^3 + \frac{5}{2}x^2 + x - 2 \quad \leftarrow f(x) - \left(\frac{3}{2}x^2\right)g(x) \\ & \underline{2x^4 \quad\quad\quad + x} \\ & 2x^3 + \frac{5}{2}x^2 \quad\quad - 2 \\ & \underline{2x^3 \quad\quad\quad + 1} \\ & \frac{5}{2}x^2 \quad\quad - 3 \quad \leftarrow \text{나머지 } r(x) \end{array}$$

예제 | 4.1.1 R이 가환환이면, $R[x]$ 역시 가환환임을 증명하라.

►풀이◄ $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ 와

$g(x) = b_0 + b_1x + \cdots + b_mx^m \in R[x]$을 임의로 택한다. 그러면 각 $k \geq 0$에 대하여, $f(x)g(x)$에서 x^k의 계수는 $a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0$ 이고 R이 가환환이므로 $\sum_{i=0}^{k} a_ib_{k-i} = \sum_{i=0}^{k} b_{k-i}a_i$이다. 즉, $g(x)f(x)$에서 x^k의 계수와 같다. $R[x]$는 가환환이다. ■

유제 4.1.1 R이 항등원 1_R을 가지면, 1_R은 역시 $R[x]$의 항등원임을 보여라.

예제 4.1.2 $\mathbb{Z}_2[x]$에 속하는 모든 3차 다항식을 열거하라.

►풀이◄ $x^3, x^3+x^2, x^3+x, x^3+x^2+x, x^3+1, x^3+x^2+1,$
$x^3+x+1, x^3+x^2+x+1.$

■

유제 4.1.2 $\mathbb{Z}_3[x]$에 속하는 3보다 더 작은 차수를 갖는 모든 다항

식을 열거하라.

예제 4.1.3 $\mathbb{Q}[x]$에서 $f(x)=3x^4-2x^3+6x^2-x+2$와 $g(x)=x^2+x+1$라 하자. $f(x)=g(x)q(x)+r(x)$이고, $r(x)=0$ 또는 $\deg r(x)<\deg g(x)$인 다항식 $q(x)$와 $r(x)$을 구하라.

[풀이] $q(x)=3x^2-5x+8,\ r(x)=-4x-6.$ ■

유제 4.1.3-1 $f(x)=g(x)q(x)+r(x)$이고, $r(x)=0$ 또는 $\deg r(x)<\deg g(x)$인 다항식 $q(x)$와 $r(x)$을 구하라. $\mathbb{Z}_5[x]$에서

$f(x)=2x^4+x^2-x+1$과 $g(x)=2x-1$이다.

유제 4.1.3-2 $f(x)=x^6+3x^5+4x^2-3x+2,$이고, $g(x)=x^2+2x-3\in Z_7[x]$이다. $f(x)/g(x)$의 몫과 나머지를 구하여라.

예제 4.1.4 $\varphi: R[x]\to R$은 $R[x]$의 각 다항식을 이 다항식의 상수항(R의 원)으로 대응하는 함수라 하자. φ는 환들의 전사준동형사상임을 증명하라.

►풀이◄ 임의로 $R[x]$의 원 $f(x)=a_0+a_1x+\ \cdots\ +a_nx^n$과 $g(x)=b_0+b_1x+\ \cdots\ +b_mx^m$을 택한다. 여기서 $n\le m$과 가정하여도 일반성을 잃지 않는다. 그러면 $f(x)+g(x)$의 상수항은 a_0+b_0이고 $f(x)g(x)$의 상수항은 a_0b_0이다. 그래서

$$\varphi(f(x)+g(x))=a_0+b_0=\varphi(f(x))+\varphi(g(x)),$$
$$\varphi(f(x)g(x))=a_0b_0=\varphi(f(x))\varphi(g(x)).$$

그래서 φ는 준동형사상이다. φ가 전사함수임은 분명하다. 따라서 φ는 전사준동형사상이다. ■

유제 4.1.4 $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$는 $\mathbb{Z}[x]$의 다항식 $a_0 + a_1x + \cdots + a_kx^k$를 다항식 $[a_0] + [a_1]x + \cdots + [a_k]x^k$으로 대응하는 함수라 하자. 여기서 $[a]$는 $\mathbb{Z}_n$에 속하는 정수 a의 합동류를 나타낸다. φ는 환들의 전사준동형사상임을 증명하라.

예제 | 4.1.5 다음의 각 명제가 참인지 거짓인지를 말하라.

(a) 다항식 $(a_0 + a_1x + \cdots + a_nx^n) \in R[x]$가 0_R이다 $\Leftrightarrow$. 각 $i = 0, 1, \cdots, n$에 대하여 $a_i = 0_R$이다.

(b) R이 가환환이면, $R[x]$ 역시 가환환이다.

(c) R이 환이고 $f(x), g(x) \in R[x]$의 차수가 각각 3과 4 이면, $f(x)g(x)$는 $R(x)$에서 8차 일 수 있다.

(d) R이 환이면, x는 $R[x]$에 결코 영인수가 아니다.

►풀이◄ (a) T (b) T (c) F (d) T ■

유제 4.1.5 다음 각 명제가 참인지 아닌지를 말하라.

(1) D가 정역이면, $D[x]$ 역시 정역이다.

(2) R이 영인수를 포함하는 환이면, $R[x]$ 역시 영인수를 갖는다.

(3) R이 임의의 환이고 $f(x)$, $g(x) \in R[x]$의 차수가 각각 3

과 4이면, $f(x)g(x)$의 차수는 언제나 7이다.

(4) F가 체이면, $F[x]$에 단원은 정확히 F에서 단원이다.

(5) R이 환이면, $R[x]$에서 영인수는 정확히 R에서 영인수이다.

4.2 $F[x]$에서 나누어 떨어짐

F는 언제나 체를 나타낸다.

정의 4.2.1

F는 체, $f(x)$, $g(x) \in F[x]$이고 $f(x) \neq 0_F$라 하자. 적당한 다항식 $h(x) \in F[x]$가 존재하여 $g(x) = f(x)h(x)$이면 $f(x)$가 $g(x)$를 나눈다[또는 $f(x)$는 $g(x)$의 인수(factor)다]라고 한다.
이 경우에, 기호 $f(x) \mid g(x)$로 쓴다.

▌보기 4.2.1▐ $\mathbb{Q}[x]$에서 $(2x+1)|(6x^2-x-2)$. 왜냐면, $6x^2-x-2=(2x+1)(3x-2)$이기 때문이다. 더욱이, $2x+1$의 모든 상수배수는 역시 $6x^2-x-2$를 나눈다. 예컨대, $5(2x+1)=10x+5$는 $6x^2-x-2$를 나눈다. 왜냐면, $6x^2-x-2=5(2x+1)[\frac{1}{5}(3x-2)]$이기 때문이다. 일반적인 경우에, 비슷한 주장에 의하여, 다음이 성립한다 :

$$f(x)|g(x)\text{면 } cf(x)|g(x) \quad \forall 0_F \neq c \in F \qquad \blacksquare$$

보기 4.2.1은 영이 아닌 다항식은 무한히 많은 약수를 가질 수 있음을 보여준다. 대조적으로, 영이 아닌 정수는 유한개의 약수만을 갖는다. 이 보기는 역시 다음의 사실을 설명한다 : $g(x)\neq 0_F$면, $g(x)$의 모든 약수는 $\deg g(x)$보다 작거나 같은 차수를 갖는다. 이것을 증명하기 위하여, $f(x)|g(x)$라 가정하자. 그러면 적당한 다항식 $h(x)\in F[x]$가 존재하여 $g(x)=f(x)h(x)$를 만족한다. 그래서, 정리 4.1.2에 의하여,

$$\deg g(x)=\deg f(x)+\deg h(x).$$

따라서 $0\leq \deg f(x)\leq \deg g(x)$이다.

두 다항식 $f(x)$, $g(x)\in F[x]$의 최대공약수는 이 두 다항식을

모두 나누는 최고차수의 다항식이어야만 한다.
그러나 이와 같은 최대공약수는 유일하지 않을 것이다.
왜냐면 이 최대공약수의 각 상수배수는 같은 차수를 갖고 역시 $f(x)$와 $g(x)$를 모두 나누게 될 것이기 때문이다.

꼭 하나의 gcd를 보장하기 위하여, 우리는 새로운 개념을 소개함으로써 이 정의를 약간 변경한다. $F[x]$에서 다항식이 모닉(monic)이다 라는 뜻은 이 다항식의 최고차계수가 1_F임을 의미한다. 예컨대, x^3+x+2는 $\mathbb{Q}[x]$에서 모닉이지만 $2x+1$은 모닉이 아니다. 또한 상수다항식이 모닉이라는 뜻은 1_F라는 뜻이다.

정의 4.2.2

F는 체, $f(x)$, $g(x)\in F[x]$이고 $f(x)\neq 0_F$, $g(x)\neq 0_F$ 라 하자. 다항식 $d(x)$는 $f(x)$와 $g(x)$를 동시에 나누는 최고차의 모닉다항식이면 $d(x)$를 $f(x)$와 $g(x)$의 최대공약수(gcd)(the greatest common divisor)라고 한다. 다른말로 하면, $d(x)$가 $f(x)$와 $g(x)$의 gcd일 필요충분조건은 $d(x)$가 모닉이고

(i) $d(x)|f(x)$ 이고 $d(x)|g(x)$,

(ii) $c(x)|f(x)$ 이고 $c(x)|g(x)$면, $\deg c(x)\leq \deg d(x)$를 만족하는 것이다.

▌보기 4.2.2▐ $\mathbb{Q}[x]$에서 $3x^2+x+6$과 0의 gcd를 구하기 위하여, 우리는 최고차수의 공약수들이 바로 차수 2인 $3x^2+x+6$의 공약수들임에 주목한다. 이 공약수들은 $3x^2+x+6$ 자신과 이 다항식의 모든 영이 아닌 상수배수들 - 특히, 모닉다항식 $\frac{1}{3}(3x^2+x+6) = x^2+\frac{1}{3}x+2$를 포함한다. 따라서 $x^2+\frac{1}{3}x+2$가 $3x^2+x+6$과 0의 gcd다. ■

▌보기 4.2.3▐ 여러분은 쉽게 $\mathbb{Q}[x]$에서 다음의 인수분해를 확인할 수 있다:

$$f(x) = 2x^4+5x^3-5x-2 = (2x+1)(x+2)(x+1)(x-1),$$
$$g(x) = 2x^3-3x^2-2x = (2x+1)(x-2)x.$$

$2x+1$이 $f(x)$와 $g(x)$의 최고차수의 공약수인 듯하다. 이 경우에, 상수배수 $\frac{1}{2}(2x+1) = x+\frac{1}{2}$는 최고차수의 모닉공약수다. 실제로 $x+\frac{1}{2}$이 최대공약수라는 증명은 이 절의 끝에서 주어진다. 정수에서와 같이 이 gcd가 $f(x)u(x)+g(x)v(x)$꼴로 쓰여질

수 있음을 알 수있다.

$$x+\frac{1}{2} = (2x^4+5x^3-5x-2)\left(\frac{7}{48}x-\frac{1}{4}\right)$$
$$+(2x^3-3x^2-2x)\left(-\frac{7}{48}x^2-\frac{1}{3}x-\frac{1}{48}\right).$$ ■

정리 4.2.3

F는 체, $f(x),\ g(x)\in F[x]$이고 $f(x)\neq 0_F,\ g(x)\neq 0_F$라 하자. 그러면 $f(x)$와 $g(x)$의 유일한 최대공약수 $d(x)$가 존재한다. 더욱이, (꼭 하나일 필요가 없는)다항식 $u(x)$와 $v(x)$가 존재하여

$$d(x) = f(x)u(x)+g(x)v(x)$$

을 만족한다.

따름정리 4.2.4

F는 체, $f(x),\ g(x)\in F[x]$이고 $f(x)\neq 0_F,\ g(x)\neq 0_F$라 하자. 모닉 다항식 $d(x)\in F[x]$가 $f(x)$와 $g(x)$의 최대공약수일 필요충분조건은 $d(x)$가 다음의 조건을 만족하는 것이다:

(i) $d(x)|f(x)$ 이고 $d(x)|g(x)$,

(ii) $c(x)|f(x)$ 이고 $c(x)|g(x)$이면 $c(x)|d(x)$이다.

▸증명◂ 숙제 ■

▌보기 4.2.4▐ $\mathbb{Q}[x]$에서 $f(x)=2x^4+5x^3-5x-2$와 $g(x)=2x^3-3x^2-2x$의 gcd를 구하기 위하여, 나머지가 영이 될 때 까지 나눗셈 알고리즘을 반복하여 사용한다. 각 단계에서 나눗식과 나머지는 다음 단계에서 나뉨식과 나눗식이 된다 :

$$2x^4+5x^3-5x-2=(2x^3-3x^2-2x)(x+4)+(14x^2+3x-2),$$

$$2x^3-3x^2-2x=(14x^2+3x-2)\left(\frac{1}{7}x-\frac{12}{49}\right)+\left(-\frac{48}{49}x-\frac{24}{49}\right),$$

$$14x^2+3x-2=\left(-\frac{48}{49}x-\frac{24}{49}\right)\left(-\frac{343}{24}x+\frac{49}{12}\right)+0.$$

그래서 마지막 영이 아닌 나머지, $-\frac{48}{49}x-\frac{24}{49}$,는 최고차수의 공약수다. 따라서 gcd는 모닉다항식

$$\left(-\frac{49}{48}\right)\left(-\frac{48}{49}x-\frac{24}{49}\right)=x+\frac{1}{2}.$$ ■

정의 4.2.5

다항식 $f(x)$와 $g(x)$가 서로소(relatively prime)라는 말은 $f(x)$와 $g(x)$의 최대공약수가 1_F인 것이다.

모든 상수는 모든 다항식의 약수이다(예제 4.2.1). 따라서 두 다항식은 모든 상수 다항식을 공약수로 갖는 다. 그 공약수중 최대 공약수는 모닉다항식이어야 하므로 1_F라는 뜻이다.

정리 4.2.6

F는 체라 하고 $f(x),\ g(x),\ h(x)\in F[x]$라 하자. $f(x)|g(x)h(x)$이고 $f(x)$와 $g(x)$가 서로소이면 $f(x)|h(x)$이다.

►증명◄ $f(x)$와 $g(x)$가 서로소이면 정리 4.2.3에 의해 다항식 $u(x)$와 $v(x)$가 존재하여 $1_F=f(x)u(x)+g(x)v(x)$을 만족한다. 양변에 $h(x)$를 곱하면 $f(x)u(x)h(x)+g(x)v(x)h(x)=h(x)$이다.

$f(x)|g(x)h(x)$이므로 좌변을 나누므로 우변도 나누어야 하므로 $f(x)|h(x)$이다. ■

예제 | 4.2.1 $f(x)\in F[x]$면, 모든 영이 아닌 상수다항식은 $f(x)$의 인수임을 증명하라.

►풀이◄ $0_F\neq c\in F$를 임의로 택한다. F는 체이므로 $c^{-1}\in F$이 존재하여 $cc^{-1}=1_F$를 만족한다. 따라서 $f(x)=c(c^{-1}f(x))$가 되므로 $c|f(x)$이다. ■

예제 | 4.2.2 (a) 상수다항식 $f(x)=6\in F[x]$과 $g(x)=8\in F[x]$의 최대공약수를 구하라.

(b) $f(x)=x-1\in F[x]$ $g(x)=x-2\in F[x]$의 최대공약수를 구하라.

▸풀이◂ (a) F가 체이므로 예제 4,2,1에 의해 모든 상수다항식은 $f(x)$와 $g(x)$의 공약수이다. 하지만 그중 모닉은 1_F이므로 $f(x)$와 $g(x)$의 최대공약수는 1_F이다.

(b) 마찬가지로 $f(x)=x-1\in F[x]$ $g(x)=x-2\in F[x]$의 최대공약수는 1_F이다. ■

유제 | 4.2.1 $f(x)=c_nx^n+\cdots+c_0\in F[x]$이고 $c_n\neq 0_F$라 하자. 그러면 $f(x)$와 0_F의 gcd는 무엇인가?

예제 | 4.2.3 유클리드 알고리즘을 사용하여 다음 다항식의 gcd를 구하라 : $\mathbb{Q}[x]$에서 $x^4-x^3-x^2+1$과 x^3-1

▸풀이◂ $x-1$ ■

유제 | 4.2.2 유클리드 알고리즘을 사용하여 다음 다항식의 gcd를 구하라.

(1) $\mathbb{Z}_5[x]$에서 x^4+3x^3+2x+4와 x^2-1

(2) $\mathbb{C}[x]$에서 $x^3-ix^2+4x-4i$와 x^2+1

예제 | 4.2.4 $f(x)$, $g(x)$, $h(x)\in F[x]$이고 $f(x)$와 $g(x)$는 서로소라 하자. $h(x)|f(x)$면, $h(x)$와 $g(x)$는 서로소다. 이를 증명하라.

▸풀이◂ $h(x)$와 $g(x)$가 서로소가 아니라 가정한다. 그러면 모닉 다항식 $k(x)\in F[x]$, $\deg k(x)\geq 1$가 존재하여 $k(x)|h(x)$이고 $k(x)|g(x)$이다. 가정에 의해 $h(x)|f(x)$이므로, $k(x)|f(x)$이다. 그래서 $k(x)$는 $f(x)$와 $g(x)$의 공약수이다.

이것은 $f(x)$와 $g(x)$가 서로소라는 사실에 모순이다. 따라서 $h(x)$와 $g(x)$는 서로소이다. ■

유 제 | $f(x)$, $g(x)$, $h(x)\in F[x]$이고 $f(x)$와 $g(x)$는 서로소라 하자. $f(x)|h(x)$이고 $g(x)|h(x)$이면, $f(x)g(x)|h(x)$이다. 이를 증명하라.

유 제 | $f(x)$, $g(x)$, $h(x)\in F[x]$이고 $f(x)$와 $g(x)$는 서로소라 하자. 그러면 $f(x)h(x)$와 $g(x)$의 gcd는 $h(x)$와 $g(x)$의 gcd와 같다. 이를 증명하라.

4.3 기약다항식과 유일인수분해

정리 4.3.1 F는 체라 하자. 그러면

$f(x)$가 $F[x]$의 단원일 필요충분조건은 $f(x)$가 영이 아닌 상수 다항식인 것이다.

►증명◄ $(\Rightarrow)$: $f(x)$는 $F[x]$의 단원이라 가정하자. 그러면

$\exists g(x) \in F[x] \;\; s.t. f(x)g(x) = 1_F$.

정리 4.1.2에 의하여

$\deg f(x) + \deg g(x) = \deg[f(x)g(x)] = \deg[1_F] = 0.$

모든 차수는 음아닌 정수 이므로, $\deg f(x) = 0$이고 $\deg g(x) = 0$. 그러므로 $f(x)$와 $g(x)$는 영이 아닌 상수다항식이다.

$(\Leftarrow)$: $f(x)$는 영이 아닌 상수다항식이라 가정하자. 그러면 $\exists 0_F \neq b \in F \; s.t. \; f(x) = b$.

그런데 b는 F의 단원이므로 $b^{-1} \in F$이다.

$g(x) = b^{-1}$라 하면 $F[x]$에서 상수다항식이고 $f(x)g(x) = 1_F$이다. 따라서 $f(x)$는 $F[x]$의 단원이다. ■

정리 4.3.1은 $\mathbb{Q}[x]$, $\mathbb{R}[x]$와 $\mathbb{C}[x]$의 각각이 무한히 많은 단원을 가짐을 보여준다. F가 체가 아니면, 이 정리는 거짓일 수 있다. 예로써, 상수다항식 $f(x) = 2$는 $\mathbb{Z}[x]$의 단원이 아니다.

왜냐면, $f(x)$의 역 , $\frac{1}{2}$, 은 $\mathbb{Z}$에 속하지 않기 때문이다. 다항식 $3x+1$은 $\mathbb{Z}_9[x]$의 단원이다. 왜냐면, $(3x+1)(6x+1) = 1$이기 때문이다.

다항식 $f(x) \in F[x]$가 $g(x) \in F[x]$의 동반(associate)이다라는 뜻은 어떤 $0_F \neq c \in F$에 대하여 $f(x) = cg(x)$임을 의미한다. 예로

써, $\mathbb{Q}[x]$에서 x^2+1의 몇 개의 동반원은 $5(x^2+1)$과 $\frac{1}{7}(x^2+1)$이다. 정리 4.3.1에 의하여, $g(x)$의 동반원은 바로 $g(x)$와 $F[x]$의 단원의 곱이다.

$f(x)$가, $g(x)$의 동반원, 즉, $f(x) = cg(x)$면,

$c^{-1}f(x) = c^{-1}(cg(x)) = g(x)$. 따라서

$f(x)$가 $g(x)$의 동반원이다 $\Leftrightarrow$ $g(x)$가 $f(x)$의 동반원이다.

정의 4.3.2

F는 체라 하자. $p(x)\in F[x]$가 상수가 아닌(또는, 단원이 아닌) 다항식이라 하자. $p(x)$의 약수들이 $p(x)$의 동반원과 영이 아닌 상수 다항식(단원)들뿐이면 $p(x)$을 기약 다항식(irreducible polynomial)이라고 한다. 기약이 아닌 비상수 다항식을 가약(reducible)이라 한다.

즉, $p(x)\in F[x]$가 기약이라는 것은 $p(x)$가 F의 원소가 아니고 즉, 상수(단원)이 아니고 $p(x)=f(x)g(x)$이면 $f(x)$, $g(x)$ 둘 중 하나는 상수(단원)이라는 뜻이다. 그러나 F가 체가 아니면 $p(x)$가 ± 1이 아니고 $p(x)=f(x)g(x)$이면 $f(x)$, $g(x)$ 둘 중 하

나는 ± 1라는 뜻이다.

▌보기 4.3.1▐ 다항식 $x+2$는 $\mathbb{Q}[x]$에서 기약이다. 왜냐면 정리 4.1.2에 의하여, 이 다항식의 모든 약수는 차수 0 또는 1을 가져야만 한다. 차수 0의 약수는 영이 아닌 상수다. $f(x)|(x+2)$라 가정하자. 그러면 $g(x)\in\mathbb{Q}[x]$이 존재하여 $x+2=f(x)g(x)$을 만족한다. $\deg f(x)=1$이면, $\deg g(x)=0$ 그래서 $g(x)=c$, $c\in\mathbb{Q}$라 할 수 있다. 그러므로 $f(x)=c^{-1}(x+2)$이고 $f(x)$는 $x+2$의 동반원이다. 일반적인 경우에 비슷한 주장에 의하여, 다음의 결과가 얻어진다 :

$F[x]$에서 차수 1인 모든 다항식은 $F[x]$에서 기약이다. ■

기약성의 개념이 절대적인 개념이 아님에 주목한다.

예컨대, x^2+1은 $\mathbb{C}[x]$에서 가약이다. 왜냐면, $\mathbb{C}[x]$에서

$$x^2+1=(x+i)(x-i)$$

이고, 어떤 인수도 상수가 아니고 x^2+1의 동반원도 아니기 때문이다. 그러나 x^2+1은 $\mathbb{Q}[x]$에서 기약이다(예제 4.3.5).

다음의 결과는 $F[x]$에서 기약다항식이 본질적으로 $\mathbb{Z}$에서 소수가 갖는 것과 같은 나누어 떨어짐 성질을 가짐을 보여준다. 이

결과에 있는 조건 (3)은 종종 다항식이 기약임을 증명하기 위하여 사용되고, 많은 책에서 (3)은 "기약"의 정의로 주어진다.

정리 4.3.3 F는 체이고 $p(x)\in F[x]$는 비상수 다항식이라 하자. 그러면 다음의 조건들은 논리적으로 같다 :

(1) $p(x)$는 기약이다.
(2) $b(x)$와 $c(x)$가 $p(x)|b(x)c(x)$인 임의의 다항식이면, $p(x)|b(x)$ 또는 $p(x)|c(x)$.
(3) $r(x)$와 $s(x)$가 $p(x)=r(x)s(x)$인 임의의 다항식이면, $r(x)$ 또는 $s(x)$는 영이 아닌 상수다항식이다(둘중하나).

►증명◄ (1)⇒(2) : $b(x)$와 $c(x)$가 $p(x)|b(x)c(x)$인 임의의 다항식이라 하자. $p(x)\nmid b(x)$라 가정하자. 그러면 $p(x)$와 $b(x)$가 서로소이고 정리 4.2.6에 의하면 $p(x)|c(x)$이다.

(2)⇒(3) : 조건 (2)가 성립하고 $p(x)=r(x)s(x)$라 가정하자. 그러면, 조건 (2)에 대하여, $p(x)|r(x)$ 또는 $p(x)|s(x)$(둘중하나, 아니면 $p(x)=r(x)s(x)$에 모순).

경우 1 : $p(x)|r(x)$라 가정하자. 그러면 $v(x)\in F[x]$가 존재하여 $r(x)=p(x)v(x)$를 만족한다. 따라서

$p(x)=r(x)s(x)=p(x)v(x)s(x)$이 된다. $F[x]$는 정역이므로, 정리 3.2.7에 의하여, $1_F=v(x)s(x)$이므로 $s(x)$는 단원이다. 그러

므로 정리 4.3.1에 의하여, $s(x)$는 영이 아닌 상수다.

경우 2 : $p(x)|s(x)$라 가정하자. 경우 1과 비슷한 주장에 의하여, $r(x)$는 영이 아닌 상수다.

(3)⇒(1) : 조건 (3)이 성립한다고 가정하고 $c(x)$는 $p(x)$의 임의의 약수라 하자. 그러면 $d(x)\in F[x]$가 존재하여 $p(x)=c(x)d(x)$을 만족한다. (3)에 의하여, $c(x)$ 또는 $d(x)$는 영이 아닌 상수이다. $d(x)=d\neq 0_F$라 가정하자. 그러면 $p(x)=c(x)d(x)=dc(x)$이고 양변에 d^{-1}을 곱하면 $c(x)=d^{-1}p(x)$가 된다. 따라서 $c(x)$는 $p(x)$의 동반원이다. 그러므로 $p(x)$의 약수는 동반원이고 영이 아닌 상수뿐이다. 따라서 $p(x)$는 기약이다. ■

따름정리 4.3.4

F는 체이고 $p(x)$는 $F[x]$에서 기약다항식이라 하자.

$p(x)|a_1(x)a_2(x)\ldots a_n(x)$면, $p(x)$는 $a_i(x)$들 중에서 적어도 하나의 약수이다.

►증명◄ 따름정리 1.2.3의 증명을 $F[x]$에 각색한다. ■

정리 4.3.5

F는 체라 하자. $F[x]$의 모든 비상수다항식은 $F[x]$에서 기약 다항식들의 곱이다. 이 인수분해는 다음의 의미에서 유일하다 :

$f(x)=p_1(x)p_2(x)\ldots p_r(x)$이고,

$f(x)=q_1(x)q_2(x)\ldots q_s(x)$

이고 각 $p_i(x)$와 $q_j(x)$가 기약이면, $r=s$(즉, 기약인수들의 개수는 같다). 필요하다면, $q_j(x)$의 순서를 다시 정하고 새롭게 표시한 후에, $p_i(x)$는 $q_j(x)$의 동반원이다.$(i=1,\ 2,\ 3,\ \ldots,\ r)$.

예제 | 4.3.1 다음 모닉 동반원을 구하라. :

$\mathbb{Q}[x]$에서 $3x^3+2x^2+x+5$

▸풀이◂ $x^3+\frac{2}{3}x^2+\frac{1}{3}x+\frac{5}{3}$. ■

유제 | 4.3.1 다음 모닉 동반원을 구하라. $\mathbb{C}[x]$에서 ix^3+x-1이다.

예제 | 4.3.2 다음의 모든 동반원을 열거하라. :

$\mathbb{Z}_5[x]$에서 x^2+x+1

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

▸풀이◂ 따라서 $x^2+x+1\in\mathbb{Z}_5[x]$의 동반원은 x^2+x+1,

$2x^2+2x+2$, $3x^2+3x+3$, $4x^2+4x+4$.

■

유제 | 4.3.2 다음의 모든 동반원을 열거하라. $\mathbb{Z}_7[x]$에서 $3x+2$이다.

예제 | 4.3.3 $f(x)$와 $g(x)$가 $F[x]$에서 동반원일 필요충분조건은 $f(x)|g(x)$이고 $g(x)|f(x)$인 것이다. 이를 증명하라.

▸풀이◂ ⇒] $f(x)$와 $g(x)$가 $F[x]$에서 동반원이라 가정하자. 그러면, $0_F\neq c\in F$가 존재하여 $f(x)=cg(x)$를 만족한다. 그래서 $g(x)|f(x)$이다. 한편, F는 체이고 $c\neq 0_F$이므로, $c^{-1}\in F$가 존재하여 $cc^{-1}=1_F$이다. 그러므로 $g(x)=c^{-1}f(x)$,
즉, $f(x)|g(x)$이다.

(⇐) $f(x)|g(x)$이고 $g(x)|f(x)$라 가정하자. 그러면
$k_1(x)$, $k_2(x)\in F[x]$가 존재하여 $g(x)=f(x)k_1(x)$이고
$f(x)=g(x)k_2(x)$이다. 그래서 $g(x)=g(x)k_1(x)k_2(x)$가 된다. $F[x]$는 정역이므로, $k_1(x)k_2(x)=1_F$ 이고
$\deg k_1(x)k_2(x)=0$ 이다. 따라서

$$\deg\,[k_1(x)k_2(x)]=\deg\,k_1(x)+\deg\,k_2(x)=0$$

이다. 그러므로 $\deg\,k_1(x)=\deg\,k_2(x)=0$이고
$k_1(x)$와 $k_2(x)$는 영이 아닌 상수다항식이다.
따라서 $f(x)$와 $g(x)$는 동반원이다. ■

유제 4.3.3 $f(x)$가 $F[x]$에서 기약이다 $\Leftrightarrow$ $f(x)$의 각 동반원이 기약이다. 이를 증명하라.

예제 4.3.4 $\mathbb{Z}_2[x]$에서 2차의 모든 기약다항식을 구하라.

►풀이◄ x^2+x+1. ■

유제 4.3.4 $\mathbb{Z}_3[x]$에서 2차의 모든 기약다항식을 구하라.

예제 4.3.5 x^2+1은 $\mathbb{Q}[x]$에서 기약임을 보여라. [힌트 : 가약

이라 가정한다. 그러면 $x^2+1=(ax+b)(cx+d),\ a,\ b,c,\ d\in\mathbb{Q}$. 이것이 불가능함을 보인다.]

유 제 (1) 각 $a\in\mathbb{Z}_3$에 대하여 x^3+a는 $\mathbb{Z}_3[x]$에서 가약임을 보여라.

(2) 각 $a\in\mathbb{Z}_5$에 대하여 x^5+a는 $\mathbb{Z}_5[x]$에서 가약임을 보여라.

유 제 (1) x^2+2는 $\mathbb{Z}_5[x]$에서 기약임을 보여라.

(2) x^4-4를 $\mathbb{Z}_5[x]$에서 기약 다항식들의 곱으로 인수분해하라.

4.4 다항함수, 근과 가약성

R은 가환환이다. $R[x]$의 각 다항식 $a_nx^n+\ldots+a_2x^2+a_1x+a_0$과 결합되는 함수 $f:R\to R$는 다음의 규칙이다 :

$$\forall r\in R,\ f(r)=a_nr^n+\ldots+a_2r^2+a_1r+a_0.$$

이와 같은 방법으로 어떤 다항식에 의하여 만들어지는 함수 f를 다항함수(polynomial function)라 한다.

▌보기 4.4.1▐ 다항식 $x^2+5x+3\in\mathbb{R}[x]$는 다음의 규칙으로 주어지는 함수 $f:\mathbb{R}\to\mathbb{R}$을 만든다 :

$$f(r)=r^2+5r+3\quad\forall r\in\mathbb{R}.$$ ■

▌보기 4.4.2▐ 다항식 $x^4+x+1\in\mathbb{Z}_3[x]$는 규칙이 $f(r)=r^4+r+1$인 함수 $f:\mathbb{Z}_3\to\mathbb{Z}_3$를 만든다. 그러면

$$f(0)=0^4+0+1=1,\quad f(1)=1^4+1+1=0.$$
$$f(2)=2^4+2+1=1.$$

다항식 $x^3+x^2+1\in\mathbb{Z}_3[x]$는 아래와 같이 주어지는 함수 $g:\mathbb{Z}_3\to\mathbb{Z}_3$을 만든다:

$$g(0)=0^3+0^2+1=1,\quad g(1)=1^3+1^2+1=0,$$
$$g(2)=2^3+2^2+1=1.$$

그러므로 비록 f와 g가 $\mathbb{Z}_3[x]$에 속하는 다른 다항식에 의해서 만들어졌을 지라도, f와 g는 $\mathbb{Z}_3$에서 같은 함수다. ■

비록 다항식과 이 다항식이 만드는 다항함수 사이에 차이가 분명할 지라도, 관습상의 표시법은 아주 분명하지 않다.

$f(x)=x^2-3x+2$

- $f(x)$는 다항식 $x^2-3x+2\in\mathbb{R}[x]$
- 다항식 x^2-3x+2가 만드는 함수 $f:\mathbb{R}\to\mathbb{R}$의 규칙.

기호 x는 두가지 다른 방법으로 사용되고 있다.

- 다항식 x^2-3x+2에서, x는 환$\mathbb{R}[x]$의 부정원 (초월원)이다.
- 다항함수 $f:\mathbb{R}\to\mathbb{R}$에서, 기호 x는 이 함수의 규칙을 설명하기 위한 변수로 사용된다.

어떤 명제의 참 또는 거짓은 x가 부정원 또는 변수로 취급되는지 아닌지에 달려있다.

- x가 부정원(이환의 특별한 원)인 환 $R[x]$에서 명제
  $x^2-3x+2=0$은 거짓이다.
  왜냐하면 다항식이 영이다 $\Leftrightarrow$ 이 다항식의 모든 계수가 0이기 때문이다.
- 다항함수 $f(x)=x^2-3x+2$
  변수 x의 어느 값이 $x^2-3x+2=0$을 참이 되게 하는 가를 묻는 것은 더할 나위 없이 당연하다.

- 변수 x에 관한 명제가 환 R에서 생기는 것을 기억하는 것이 도움이 될 수 있다.
- 부정원 x에 관한 명제는 다항식 환 $R[x]$에서 생긴다.

다항식의 가약성에 대한 질문은 때때로 이 다항식이 만드는 다항함수를 생각함으로 답이 얻어질 수 있다. 이 분석에 대한 열쇠(key)는 근의 개념이다.

정의 4.4.1

R은 가환환이고 $f(x)\in R[x]$라 하자. $a\in R$가 $f(a)=0_R$를 만족하면 $a\in R$를 다항식 $f(x)$의 근(root)이라 한다 즉, 다항식 $f(x)$가 만드는 함수 $f:R\to R$가 a를 0_R에 대응시킨다.

▌보기 4.4.3▐ 다항식 $f(x)=x^2-3x+2\in\mathbb{R}[x]$의 근들은 $f(x)=0$인 변수 x의 값들, 즉, 방정식 $x^2-3x+2=0$의 해(solution)들이다. 근들이 1과 2임을 아는 것은 쉽다. ■

▌보기 4.4.4▐ 다항식 $x^2+1\in\mathbb{R}[x]$는 $\mathbb{R}$에서 근을 갖지 않는다. 왜냐면, 방정식 $x^2+1=0$의 실수해가 존재하지 않기 때문이다. 그러나 x^2+1을 $\mathbb{C}[x]$에서 다항식으로 생각하면, x^2+1은 근으로 i와 $-i$를 갖는다. 왜냐면, 이 두 값은 $\mathbb{C}$에서 $x^2+1=0$의 해들이기 때문이다. ■

$F[x]$에서 가약성에 관련된 문제들에 집중한다. 여기서 F는 체다.

정리 4.4.2 나머지정리(The Remainder Theorem)

F는 체, $f(x)\in F[x]$이고 $a\in F$라 하자. 그러면 $f(a)$는 $f(x)$를 다항식 $x-a$로 나눌 때 나머지다.

▸증명◂ 나눗셈 알고리즘에 의하여, $q(x)$, $r(x)\in F[x]$가 존재하여 $f(x)=(x-a)q(x)+r(x)$, $r(x)=0_F$ 또는 $\deg r(x)<\deg(x-a)$를 만족한다. $\deg(x-a)=1$이므로, $\deg r(x)=0$ 또는 $r(x)=0_F$이므로, 어느 경우에나 적당한 상수 $c\in F$가 존재하여 $r(x)=c$를 만족한다. 그러므로 $f(x)=(x-a)q(x)+c$이다. 따라서

$$f(a)=(a-a)q(c)+c=0_F+c=c.$$ ■

정리 4.4.3 **인수정리(The Factor Theorem)**

F는 체, $f(x)\in F[x]$이고 $a\in F$라 하자. 그러면 a가 다항식 $f(x)$의 근일 필요충분조건은 $x-a$가 $F[x]$에서 $f(x)$의 인수인 것이다.

▌보기 4.4.5▐ $x^7-x^5+2x^4-3x^2-x+2$가 $\mathbb{Q}[x]$에서 가약임을 보이기 위하여, 1은 이 다항식의 근임에 주목하라. 그러므로 $x-1$은 인수다. ■

따름정리 4.4.4

F는 체고 $f(x)$는 $F[x]$에서 영이 아닌 차수 n인 다항식이라 하자. 그러면 $f(x)$는 F에서 많아야 n개 근을 갖는다.

따름정리 4.4.5

F는 체, $f(x)\in F[x]$이고 $\deg f(x)\geq 2$라 하자. $f(x)$가 $F[x]$에서 기약이면, $f(x)$는 F에서 근을 갖지않는다.

▸증명◂ $f(x)$는 $F[x]$에서 기약이라 가정하자.
$f(x)$는 $F[x]$에서 $x-a$꼴의 인수를 갖지 않는다.
인수정리에 의하여 $f(x)$는 F에서 근을 갖지 않는다.

따름정리 4.4.6

F는 체, $f(x)\in F[x]$이고 $f(x)$가 차수 2 또는 3을 갖는 다고 하자. $f(x)$가 $F[x]$에서 기약일 필요충분조건은 $f(x)$가 F에서 근을 갖지 않는 것이다.

▸증명◂ $\Rightarrow$] 따름정리 4.4.5에 의해 성립한다.
$\Leftarrow$] $\deg f(x)=2$ 또는 3이고 F에서 근을 갖지 않는다고 가정하자. $F[x]$에서 모든 1차 다항식 $cx+d$는 F에서 근 $-c^{-1}d$를 갖기 때문에 $f(x)$는 $F[x]$에서 어떠한 1차 인수도 갖지 않는다. $f(x)=r(x)s(x)$라고 가정하면 $r(x)$와 $s(x)$는 1차가 아니다. 정리 4.1.2에 의해 $\deg f(x)=2$ 또는 3이므로 $\deg r(x)=0$이거

나 $\deg s(x)=0$이어야만 한다.

정리 4.1.2
R은 정역이고 $f(x)$와 $g(x)$는 $R[x]$의 영이 아닌 다항식이라 하자. 그러면 $\deg[f(x)g(x)]=\deg f(x)+\deg g(x)$.

즉, $r(x)$ 또는 $s(x)$는 영이 아닌 상수이다. 따라서, 정리 4.3.3에

정리 4.3.3 F는 체이고 $p(x)\in F[x]$는 비상수 다항식이라 하자. 그러면 다음의 조건들은 논리적으로 같다 :

(1) $p(x)$는 기약이다.
(2) $b(x)$와 $c(x)$가 $p(x)|b(x)c(x)$인 임의의 다항식이면, $p(x)|b(x)$ 또는 $p(x)|c(x)$.
(3) $r(x)$와 $s(x)$가 $p(x)=r(x)s(x)$인 임의의 다항식이면, $r(x)$ 또는 $s(x)$는 영이 아닌 상수다항식이다.

의하여, $f(x)$는 기약이다. ■

이 따름정리는 차수≥ 4에 대하여 거짓이다. 예로써, $x^4+2x^2+1=(x^2+1)(x^2+1)$은 $\mathbb{Q}[x]$에서 가약이지만 $\mathbb{Q}$에서 근을 갖지 않는다.

▌보기 4.4.6 ▐ x^3+x+1이 $\mathbb{Z}_5[x]$에서 기약임을 보이기 위하여, 여러분은 $0,\ 1,\ 2,\ 3,\ 4, \in \mathbb{Z}_5$중의 어느 것도 근이 아님을 확인할 필요가 있다. ■

우리는 출발점인 다항함수로 돌아감으로써 이 절을 끝낸다. 보기 4.4.2는 $F[x]$에서 두 다른 다항식이 F에서 F로의 같은 함수를 만든다는 것을 보여준다. F가 무한하면 이러한 일이 생길 수 없다는 것을 우리는 이제 보여 준다.

따름정리 4.4.7

F는 무한체이고 $f(x), g(x) \in F[x]$라 하자. $f(x)$와 $g(x)$가 F에서 F로의 같은 함수를 만들 필요충분조건은 $F[x]$에서 $f(x)=g(x)$인 것이다.

►증명◄ $(\Rightarrow)$: $f(x)$와 $g(x)$가 F에서 F로의 같은 함수를 만든다고 가정하자. 그러면 $a \in F$에 대하여 $f(a)=g(a)$이다.
그러므로 $a \in F$에 대하여 $f(a)-g(a)=0_F$이다.

이것은 F의 모든 원이 다항식 $f(x)-g(x)$의 근임을 의미한다. F는 무한하므로, 따름정리 4.4.3-1에 의하여, 이것은 불가능하다. 따라서 $f(x)-g(x)$는 영다항식, 즉 $f(x)=g(x)$이다.

$(\Leftarrow)$: 이 증명은 분명하다. ■

예제 | 4.4.1 $h(x)$가 $f(x)$의 인수인지를 결정하라:

$\mathbb{R}[x]$에서 $h(x)=x+2$와 $f(x)=x^3-3x^2-4x-12$

►풀이◄ $f(-2)=(-2)^3-3(-2)^2-4(-2)-12$
$=-24 \neq 0.$
따라서 $h(x)$는 $f(x)$의 인수가 아니다. ■

유제 | 4.4.1 $h(x)$가 $f(x)$의 인수인지를 결정하라.

$\mathbb{Z}_5[x]$에서 $h(x)=x+2$와 $f(x)=3x^5+4x^4+2x^3-x^2+2x+1$

예제 | 4.4.2 다음 각 명제가 참인지 거짓인지를 말하라.

(a) $x-2$는 $\mathbb{Q}$위에서 기약이다.

(b) x^2-3은 $\mathbb{Q}$위에서 기약이다.

(c) F가 체이면, $F[x]$의 단원들은 정확히 F의 영 아닌 원들이다.

(d) 체 F의 계수를 갖는 n차 다항식은 기껏해야 F에서 n개의 영을 가질 수 있다.

(e) $F[x]$에서 모든 1차 다항식은 체 F에서 적어도 하나의 영을 갖는다.

►풀이◄ (a)T (b)T (c)T (d)T (e)T. ■

유제 | 4.4.2 다음의 각 명제가 참인지 거짓인지를 말하라.

(1) $3x-6$은 $\mathbb{Q}$ 위에서 기약이다.

(2) x^2+3은 $\mathbb{Z}_7$ 위에서 기약이다.

(3) $F[x]$에서 각 다항식은 체 F에서 기껏해야 유한 개의 영들을 가질 수 있다.

예제 | 4.4.3 $a\in F$가 $f(x)\in F[x]$의 중근(multiple root)이다라는 뜻은 어떤 $k\geq 2$에 대하여 $(x-a)^k$이 $f(x)$의 인수임을 의미한다. $a\in\mathbb{R}$가 $f(x)\in\mathbb{R}[x]$의 중근일 필요충분조건은 a가 $f(x)$와 $f'(x)$의 근인 것이다. 여기서 $f'(x)$는 $f(x)$의 도함수이다. 이를 증명하라.

▸풀이◂ ($\Rightarrow$) $a\in\mathbb{R}$가 $f(x)\in\mathbb{R}[x]$의 중복근이라 가정하자. 그러면 적당한 $k\geq 2$가 존재하여 $(x-a)^k$가 $f(x)$의 인수가 된다. 그래서 $g(x)\in\mathbb{R}[x]$가 존재하여 $f(x)=(x-a)^k g(x)$, $g(a)\neq 0$을 만족한다. 그러므로 $f(a)=0$이다. 한편

$$f'(x)=k(x-a)^{k-1}g(x)+(x-a)^k g'(x)$$

이므로 $f'(a)=k(a-a)^{k-1}g(a)+(a-a)^k g'(a)=0$이다.

따라서 a는 $f(x)$와 $f'(x)$의 근이다.

($\Leftarrow$) a가 $f(x)$와 $f'(x)$의 근이라 가정하자. 그러면 $f(a)=0$이고 $f'(a)=0$이다. 그래서 $(x-a)\mid f(x)$이고 $(x-a)\mid f'(x)$이다. 따라서 적당한 다항식 $g(x)\in F[x]$가 존재하여 $f(x)=(x-a)g(x)$이다. 이를 미분하면 $f'(x)=g(x)+(x-a)g'(x)$가 된다. $(x-a)\mid f'(x)$이므로 오른편 항을 모두 나누어야 하므로 $(x-a)|g(x)$이게 된다. 즉, 적당한 다항식 $h(x)\in F[x]$가 존재하여 $g(x)=(x-a)h(x)$가 된다. 따

라서 $f(x)=(x-a)g(x)=(x-a)^2h(x)$가 된다. 그러므로 적당한 $k\geq 2$가 존재하여 $(x-a)^k\mid f(x)$이다. 따라서 증명이 완료된다. ■

유제 | 4.4.3 $f(x)\in\mathbb{R}[x]$이고 $f(x)$가 $f'(x)$와 서로소이면, $f(x)$는 $\mathbb{R}$에서 중복근을 갖지 않음을 증명하라.

예제 | 4.4.4 T는 체 F에서 체 F로의 모든 다항함수들의 집합이고 T에서 덧셈과 곱셈을 다음과 같이 정의한다. 각 $r\in F$에 대하여, $(f+g)(r)=f(r)+g(r)$이고

Tip 환의 정의와 다항함수의 정의를 확인한다.

$(fg)(r)=f(r)g(r)$이다. 그러면 T는 항등원이 있는 교환환이다. 이를 증명하라.

[풀이] 임의의 다항함수 $f(r)=a_n r^n+\cdots+a_2r^2+a_1r+a_0$와 $g(r)=b_m r^m+\cdots+b_2r^2+b_1r+b_0$, $m<n$가 주어졌을 때 다항함수의 덧셈은 다음과 같다

$$(a_0+a_1r+a_2r^2+\cdots+a_nr^n)+(b_0+b_1r+b_2r^2+\cdots+b_mr^m)$$

$$=(a_0+b_0)+(a_1+b_1)r+(a_2+b_2)r^2+\cdots+(a_n+b_n)r^n\in F,$$

여기서 $b_i=0$, $m<i$.

다항함수의 곱셈은

$$(a_0+a_1r+a_2r^2+\cdots+a_nr^n)(b_0+b_1r+b_2r^2+\cdots+b_mr^m)$$
$$=a_0b_0+(a_0b_1+a_1b_0)r+(a_0b_2+a_1b_1+a_2b_0)r^2+\cdots+a_nb_mr^{n+m}\in F$$

여기서 각 $k\geq 0$에 대하여, 이 곱에서 x^k의 계수는

$$a_0b_k+a_1b_{k-1}+a_2b_{k-2}+\cdots+a_{k-2}b_2+a_{k-1}b_1+a_kb_0=\sum_{i=0}^{k}a_ib_{k-i}.$$

여기서 $i>n$이면 $a_i=0_R$이고 $j>m$이면 $b_j=0_R$이다. 따라서 임의의 $f,\ g\in T$에 대하여 $f+g\in T$이고 $fg\in T$이다. "+"에 대한 교환성질과 결합성질과 "$\cdot$"에 대한 결합성질과 결합성질 및 분배성질은 $(F,\ +,\ \cdot)$의 성질에 의하여 분명하다. $0_F\in T$와

$1_F\in T$는 각각 다음과 같이 되는 다항함수라 하자. 임의의 $f\in T$에 대하여 $(-f)(r)=-f(r),\ r\in F$이라 하자. 그러면 분명히 $-f$는 $f+x=0_F$의 T에서의 해이다. 모든 $r\in F$에 대하여 $0_F(r)=0_F$이고 $1_F(r)=1_F$이다. 그러면 모든 $f\in F$에 대하여 $0_F+f=f$이고 $1_F\cdot f=f$이다. 그러므로 0_F와 1_F는 각각 "+"와 "$\cdot$"에 관한 항등원이다. 따라서 $(T,\ +,\ \cdot)$은 항등원이 있는 환이다. 또한 각 $k\geq 0$에 대하여, $f(x)g(x)$에서 x^k의 계수는 $a_0b_k+a_1b_{k-1}+\ \cdots\ +a_{k-1}b_1+a_kb_0$이고 F가 체이므로 $\sum_{i=0}^{k}a_ib_{k-i}$

$=\sum_{i=0}^{k}b_{k-i}a_i$이다. 즉 $g(x)f(x)$에서 x^k의 계수와 같다. T는 가환환이다. ■

유제 4.4.4 F는 무한체이고 T는 F에서 F로의 모든 다항함수들의 환(예제 4.4.4)이라 하자. 그러면 $F[x]\cong T$이다. 이를 증명하라. [도움말: 함수 $\varphi\colon F[x]\to T$를 각 다항식 $f(x)\in F(x)$에 $f(x)$가 만드는 T에서 함수로 대응시킴으로써 정의한다. 그러면 따름정리 4.4.3-3에 의하여 φ은 단사이다.]

4.5 $\mathbb{Q}[x]$에서 기약성

이 절의 중심적인 주제는 $\mathbb{Q}[x]$에서 인수분해가 $\mathbb{Z}[x]$에서 인수분해로 바꾸는 것이다.

$f(x)\in\mathbb{Q}[x]$면, $0\neq c\in\mathbb{Z}$가 존재하여 $cf(x)\in\mathbb{Z}[x]$을 만족한다.

예로써, $\mathbb{Q}[x]$에서 다항식

$$f(x)=x^5+\frac{2}{3}x^4+\frac{3}{4}x^3-\frac{1}{6}$$

을 생각하자. 그러면 $f(x)$의 계수의 최소의 공통분모(the least common denominator)는 12다. 그래서 $12f(x)$는 정수계수를 갖는 다항식이다:

$$12f(x)=12[x^5+\frac{2}{3}x^4+\frac{3}{4}x^3-\frac{1}{6}]=12x^5+8x^4+9x^3-2.$$

인수정리에 따라서, 다항식 $g(x)\in\mathbb{Q}[x]$의 1차 인수를 구하는 것은 $\mathbb{Q}$에서 $g(x)$의 근을 구하는 것과 논리적으로 같다.
또한 $a\in\mathbb{Q}$에 대하여 $g(a)=0$이면 $cg(a)=0, c\neq 0$이므로(역도 성립), $g(x)$는 임의의 영이 아닌 상수 c에 대하여 $cg(x)$와 같은 근을 갖는다.
$g(x)\in\mathbb{Q}[x]$에 대하여 $cg(x)\in\mathbb{Z}[x]$의 근을 다음 정리에서와 같이 구하므로 $g(x)$의 근을 찾을 수 있다.

정리 4.5.1 유리근판정법(Rational Root Test)

$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0\in\mathbb{Z}[x]$라 하자. $r\neq 0$이고 $(r,s)=1$인 유리수 $\frac{r}{s}$가 $f(x)$의 근이면, $r|a_0$이고 $s|a_n$.

►증명◄ r/s가 $f(x)$의 근이면

$$a_n\frac{r^n}{s^n}+a_{n-1}\frac{r^{n-1}}{s^{n-1}}+\cdots+a_1\frac{r}{s}+a_0=0$$

이다. 양변에 s^n을 곱하고 공통인수를 정리하면

$$a_nr^n+a_{n-1}sr^{n-1}+\cdots+a_1s^{n-1}r+a_0s^n=0$$
$$a_0s^n=-a_nr^n-a_{n-1}sr^{n-1}-\cdots-a_1s^{n-1}r$$
$$a_0s^n=r[-a_nr^{n-1}-a_{n-1}sr^{n-2}-\cdots-a_1s^{n-1}]$$

따라서 $r|a_0s^n$이다. 그러나 $(r,s)=1$이므로 $(r,s^n)=1$이다

따라서 $r|a_0$이다. 또한

$$a_nr^n=-a_{n-1}sr^{n-1}-a_{n-2}s^2r^{n-2}-\cdots-a_0s^n$$
$$a_nr^n=s[-a_{n-1}r^{n-1}-a_{n-1}sr^{n-2}-\cdots-a_0s^{n-1}]$$

이므로 비슷하게 $s|a_n$임을 보일수 있다. ■

▌보기 4.5.1▐ $f(x)=2x^4+x^3-21x^2-14x+12\in\mathbb{Z}[x]$의 $\mathbb{Q}$에서 가능한 해는 r/s꼴이다. 여기서 r은 $\pm1,\ \pm2,\ \pm3,\ \pm4,\ \pm6\pm12$ (상수항 12의 약수들)중의 하나고, s는 ±1또는 ±2(최고차 계수 2의 약수들)중의 하나다. 그래서 유리근판정법에 의하여, $f(x)$의 근이 될 수 있는 가능한 값들은 다음과 같다 :

$$1,\ -1,\ 2,-2,\ 3,\ -3,\ 4,\ -4,\ 6,\ -6,$$
$$12,\ -12,\ \frac{1}{2},\ -\frac{1}{2},\ \frac{3}{2},\ -\frac{3}{2}.$$

-3과 $1/2$이 $\mathbb{Q}$에서 $f(x)$의 유일한 근임을 구하기 위하여 $f(x)$에 이 값들을 대입하는 것은 지루하지만 수월하다. 인수정리에

의하여, $x-(-3)=x+3$과 $x-\frac{1}{2}$은 $f(x)$의 인수다. 긴 나눗셈에 의하여, $f(x)=(x+3)(x-\frac{1}{2})(2x^2-4x-8)$이다.

한편, 2차방정식의 근의공식에 의하여, $2x^2-4x-8$의 근은 $1\pm\sqrt{5}$. 이 근중 어느 것도 $\mathbb{Q}$에 속하지 않는다. 그러므로, 따름정리 4.4.3-2에 의하여, $2x^2-4x-8$은 $\mathbb{Q}[x]$에서 기약이다. 따라서 우리는 $f(x)$를 $\mathbb{Q}[x]$에서 기약다항식들의 곱으로 인수분해하였다. ■

▌보기 4.5.2▐ 유리근판정법에 의해 $\mathbb{Q}$에서 $g(x)=x^3+4x^2+x-1$의 가능한 근은 1과 -1뿐이다. 1도 -1도 $g(x)$의 근이 아님을 확인할 수있다. 따라서, 따름정리 4.4.6에 의하여, $g(x)$는 $\mathbb{Q}[x]$에서 기약이다.

따름정리 4.4.6

F는 체, $f(x)\in F[x]$이고 $f(x)$가 차수 2 또는 3을 갖는 다고 하자. $f(x)$가 $F[x]$에서 기약일 필요충분조건은 $f(x)$가 F에서 근을 갖지 않는 것이다.

■

$\mathbb{Q}[x]$에서 인수분해가 $\mathbb{Z}[x]$에서 인수분해로 바꾸는 것이 목표이다. 이유는 정수론을 써서 정수계수 다항식의 가약성 문제를 쉽게 풀 수 있기 때문이다.

(1) 정수계수 = (정수계수)(정수계수) in $\mathbb{Z}[x]$ so in $\mathbb{Q}[x]$

(2) 정수계수 = (유리계수)(유리계수) $\Rightarrow$ 정수계수로 바꾸기를 원함

(3) 유리계수 = (유리계수)(유리계수)

(4) 유리계수 = (정수계수)(정수계수)

(3)과 (4)의 경우 즉, $f(x)\in\mathbb{Q}[x]$면, 어떤 영이 아닌 정수 c에 대하여 $cf(x)$는 정수계수를 갖는다. $\mathbb{Z}[x]$에서 $cf(x)$의 임의의 인수분해는 $\mathbb{Q}[x]$에서 $f(x)$의 인수분해가 된다. $\mathbb{Q}[x]$에서 기약성에 대한 판정법은 정수계수를 갖는 다항식으로 제한될 수 있을 듯하다. 정수계수를 갖는 다항식이 $\mathbb{Q}[x]$에서 인수분해가

되면 $\mathbb{Z}[x]$에서도 인수분해 되어야 함을 보여야 한다.

보조정리 4.5.2

$f(x), g(x), h(x)\in\mathbb{Z}[x]$이고 $f(x)=g(x)h(x)$라 하자. p가 $f(x)$의 모든 계수를 나누는 소수면, p는 $g(x)$의 모든 계수를 나누거나 또는 $h(x)$의 모든 계수를 나눈다.

►증명◄ $f(x)=a_0+a_1x+\cdots+a_kx^k$, $g(x)=b_0+b_1x+\cdots+b_mx^m$이고 $h(x)=c_0+c_1x+...+c_nx^n$하 하자.

이 결론이 거짓이라 가정하자.

그러면 p는 $g(x)$의 어떤 계수와 $h(x)$의 어떤 계수를 나누지 못한다.

b_r은 p로 나누어질 수 없는 $g(x)$의 ***최초의*** 계수고

c_t도 p로 나누어질 수 없는 $h(x)$의 *최초의* 계수라 하자.

그래서 $i<r$에 대하여 $p|b_i$이고 $j<t$에 대하여 $p|c_j$이다. $f(x)$의 계수 a_{r+t}를 생각한다. $f(x)=g(x)h(x)$이므로,

$$a_{r+t}=b_0c_{r+t}+...+b_{r-1}c_{t+1}+b_rc_t+b_{r+1}c_{t-1}+...+b_{r+t}c_0.$$

그러므로,

$$b_rc_t=a_{r+t}-[b_0c_{r+t}+...+b_{r-1}c_{t+1}]-[b_{r+1}c_{t-1}+...+b_{r+t}c_0]. \quad (4.5.4)$$

가정에 의하여, $p|a_{r+t}$. 한편, 각 $i<r$에 대하여 $p|b_i$이고 각 $j<t$에 대하여 $p|c_j$이므로, 방정식(4.5.4)의 각 대괄호에 있는

각 항들은 p로 나누어진다. 그래서 p는 방정식 (4.5.4)의 오른쪽 변의 약수다.

그러므로 $p|b_rc_t$. 정리 1.3.2에 의하여, $p|b_r$ 또는 $p|c_t$. 이것은 $p\nmid b_r$이고 $r\nmid c_t$라는 사실에 모순이다. 따라서 보조정리는 성립한다. ■

정리 4.5.3

$f(x)\in\mathbb{Z}[x]$라 하자. 그러면 다음은 동치이다.

(1) $f(x)$가 $\mathbb{Q}[x]$에서 차수 m과 n인 다항식들의 곱으로 인수분해 된다

(2) $f(x)$가 $\mathbb{Z}[x]$에서 차수 m과 n인 다항식들의 곱으로 인수분해 된다.

►증명◄ 분명히, $f(x)$가 $\mathbb{Z}[x]$에서 인수분해가 되면 같은 다항식으로 $\mathbb{Q}[x]$에서 인수분해 된다.

반대로, $f(x)\in\mathbb{Z}[x]$에 대하여 $\mathbb{Q}[x]$에서

$$f(x)=g(x)h(x)$$

이라 하자.

c, d를 $cg(x)$와 $dh(x)$가 정수 계수를 갖게 하는 영이 아닌 정수라고 하자.

그러면 $\mathbb{Z}[x]$에서

$$\deg cg(x) = \deg g(x) \text{와} \quad \deg dh(x) = \deg h(x)$$

를 만족하며

$$cdf(x) = [cg(x)][dh(x)].$$

p를 cd의 소수인 약수라고 하자.

즉, $cd = pt$라고 하면 p는 다항식 $cdf(x)$의 모든 계수들을 나눈다.

그러면 p는 $cg(x)$의 모든 계수를 나누거나 $dh(x)$의 모

든 계수를 나누게 된다.

$cg(x)$의 모든 계수를 나눈다 하자. 그러면

$$cg(x) = pk(x),\ k(x) \in \mathbb{Z}[x]$$

이고

$$\deg\ k(x) = \deg g(x).$$

그러므로

$$ptf(x) = cdf(x) = [cg(x)][dh(x)] = [pk(x)][dh(x)]$$

이고 p를 양변에서 소거하면 $\mathbb{Z}[x]$에서

$$tf(x) = k(x)[dh(x)]$$

이다. 이런 방식으로 계속 cd의 모든 소인수를 양변에서 제거

하면 오른쪽 항에는 $\pm f(x)$가 남고 왼쪽에는 $g(x)$와 같은 차수의 다항식하나와 $h(x)$와 같은 차수의 다항식 하나가 남을 것이다. ■

▌보기 4.5.3▐ $f(x) = 9x^4 + 6x^3 + 39x^2 + 2x + 12 \in \mathbb{Z}[x]$이고 $\mathbb{Q}[x]$에서 $f(x) = 9(x^2 + \frac{2}{3}x + 4)(x^2 + \frac{1}{3})$와 같이 인수분해된다.

양변에 9를 곱하면

$$9f(x) = 9(3x^2 + 2x + 12)(3x^2 + 1)$$

이고 양변에서 9를 소거하면

$$f(x) = (3x^2 + 2x + 12)(3x^2 + 1)$$

$\mathbb{Z}[x]$에서의 인수분해를 얻는다.

▌보기 4.5.4▐ $f(x) = x^4 - 5x^2 + 1$은 $\mathbb{Q}[x]$에서 기약임을 증명하라.

▸풀이◂ 이 증명은 모순법에 의한다.

$f(x)$가 가약이라 가정하자.

그러면 $f(x)$는 $\mathbb{Q}[x]$에서 두 개의 비 상수 다항식의 곱으로 인수분해 된다.

이 인수들 중에서 어느 하나가 차수 1을 가지면, $f(x)$는 $\mathbb{Q}$에서

근을 갖는다.

유리근판정법에 의하여, $f(x)$는 $\mathbb{Q}$에서 근을 갖지 않는다(가능성은 ± 1뿐이고 어느 것도 근이 아니다).

그래서 $f(x)$가 가약이므로, 정리 4.1.2에 의하여, 유일하게 가능한 인수분해는 두 2차식의 곱이다.

이 경우에 정리 4.5.3은 $\mathbb{Z}[x]$에서 이와 같은 인수분해가 존재한다는 것을 보여준다.

또한 $f(x)$가 모닉이므로 $\mathbb{Z}[x]$에서 모닉 2차식의 곱으로 인수분해된다. 그래서

$$(x^2+ax+b)(x^2+cx+d)=x^4-5x^2+1 \qquad (4.5.5)$$

라 하자. 여기서 $a,\ b,\ c,\ d\in\mathbb{Z}$라 하자. 방정식 (4.5.5)의 왼쪽 변을 전개하면,

$$x^4+(a+c)x^3+(ac+b+d)x^2+(bc+ad)x+bd$$
$$=x^4+0x^3-5x^2+0x+1$$

이다. 같은 다항식은 같은 계수를 가지므로

$$a+c=0,\ ac+b+d=-5\ \ bc+ad=0\ \ bd=1.$$

$a+c=0$이므로 $a=-c$.

그러므로

$$-5=ac+b+d=-c^2+b+d,$$

또는

$$5=c^2-b-d. \qquad (4.5.6)$$

한편, $bd=1\in\mathbb{Z}$ 이므로, $b=d=1$ 또는 $b=d=-1$. 그래서, 방정식 (4.5.6)으로부터,

$$5=c^2-1-1 \quad \text{또는} \quad 5=c^2+1+1$$
$$7=c^2 \quad \text{또는} \quad 3=c^2$$

그런데 제곱이 3또는 7이 되는 정수는 존재하지 않는다. 그러므로 $\mathbb{Z}(x)$에서 2차식의 곱으로 $f(x)$를 인수분해 할 수 없다. 따라서 $\mathbb{Q}(x)$에서 $f(x)$는 기약이다. ■

정리 4.5.4 아이젠스타인의 판정법(Eisenstein's Criterion)

$f(x)=a_nx^n+\ldots+a_1x+a_0$는 정수계수를 갖는 비상수 다항식이라 하자. 만약 소수 p가 존재하여 $p|a_0, p|a_1, \ldots p|a_{n-1}, p\nmid a_n$이고 $p^2\nmid a_0$을 만족하면 $f(x)$는 $\mathbb{Q}[x]$에서 기약이다.

▌보기 4.5.5 ▐ $p=3$인 아이젠스타인의 판정법에 의하면, 다항식 $x^{17}+6x^{13}-15x^4+3x^2-9x+12$는 $\mathbb{Q}[x]$에서 기약이다. ■

▌보기 4.5.6 ▐ $p=5$인 아이젠스타인의 판정법에 의하면, 다항식 x^9+5는$\mathbb{Q}[x]$에서 기약이다. 비슷하게, 각 $n\geq 1$에 대하여 x^n+5는 $\mathbb{Q}[x]$에서 기약이다. 그러므로 $\mathbb{Q}[x]$에서 모든 차수의 기약 다항식이 존재한다. ■

비록 아이젠스타인의 판정법이 매우 효과적일지라도, 이것이 적용될 수 없는 많은 다항식이 있다. 이와 같은 경우에 다른 기술이 필요하다. 이와 같은 한 가지 방법은, 다음의 의미에서, p를 법으로 변형시키는 것을 포함한다. p는 양의 소수고, 각 정수 a에 대하여, $[a]$는 $\mathbb{Z}_p$에 속하는 a의 합동류를 나타낸다고 하자. $f(x)=a_hx^h+\ldots+a_1x+a_0\in\mathbb{Z}[x]$

일 때,

$$\overline{f}(x)=[a_h]x^h+\ldots+[a_1]x+[a_0]\in\mathbb{Z}_p[x]$$

를 나타낸다고 하자. 예로써, $f(x)=2x^4-3x^2+5x+7\in\mathbb{Z}[x]$면,

$\mathbb{Z}_3[x]$에서,

$$\begin{aligned}\overline{f}(x)&=[2]x^4-[3]x^2+[5]x+[7]\\&=[2]x^4-[0]x^2+[2]x+[1]=[2]x^4+[2]x+[1].\end{aligned}$$

$f(x)$와 $\overline{f}(x)$는 같은 차수를 가짐에 주목하라. 이것은 언제나 $f(x)$의 최고차계수가 p로 나누어 질수 없는 경우(그러므로 $\overline{f}(x)$의 최고차 계수는 $\mathbb{Z}_p[x]$에 속하는 영류가 되지 못할 것이다)가 될 것이다.

정리 4.5.5

$f(x)=a_kx^k+\cdots+a_1x+a_0\in\mathbb{Z}[x]$이고 p는 $p\nmid a_k$인 양의 소수라 하자. $\overline{f}(x)$가 $\mathbb{Z}_p[x]$에서 기약이면, $f(x)$는 $\mathbb{Q}[x]$에서 기약이다.

►증명◄ $f(x)$가 $\mathbb{Q}[x]$에서 가약이라 가정하자. 그러면, 정리 4.5.3에 의하여, 비상수 다항식 $g(x),h(x)\in\mathbb{Z}[x]$가 존재하여 $f(x)=g(x)h(x)$이다. $p\nmid a_k$ 이므로, p는 (곱이 a_k인) $g(x)$또는 $h(x)$의 최고차계수를 나눌 수 없다. 그래서 $\deg\overline{g}(x)=\deg g(x)$ 이고 $\deg\overline{h}(x)=\deg h(x)$. 특히, $\overline{g}(x)$도 $\overline{h}(x)$도 $\mathbb{Z}_p[x]$에서 상수다항식이

아니다. 더욱이, $\mathbb{Z}_p[x]$에서 $\overline{f}(x)=\overline{g}(x)\,\overline{h}(x)$이다(연습문제 21번). 이것은 $\mathbb{Z}_p[x]$에서 $f(x)$의 기약성에 모순이다. 따라서 $f(x)$는 $\mathbb{Q}[x]$에서 기약이어야만 한다. ■

정리 4.5.5의 유용성은 다음 사실에 달려 있다: 각 음아닌 정수 k에 대하여, $\mathbb{Z}_p[x]$에서 $f(x)$ 차수 k인 다항식이 유한개만 있다($\mathbb{Z}_n[x]$에는 차수가 k인 다항식이 $n^{k+1}-n^k$개 존재한다:과제). 그러므로,

이론적으로, $\mathbb{Z}_p[x]$에 속하는 주어진 다항식이 기약인가를 결정하는 것은 유한개의 가능한 인수를 확인함으로써 언제나 가능하다. p의 크기와 $f(x)$의 차수에 따라서, 이 확인하는 일은 종종 적당한 양의 횟수로 이루어 질수 있다.

▌보기 4.5.7 ▐ $f(x)=x^5+8x^4+3x^2+4x+7$이 $\mathbb{Q}[x]$에서 기약임을 보여라.

►풀이◄ 우리는 $f(x)$를 법으로 변형시킨다. $\mathbb{Z}_2[x]$에서,

$\overline{f}(x)=x^5+x^2+1.$

$\overline{f}(x)$가 $\mathbb{Z}_2$에서 근을 갖지 않음을 보이기는 쉽다. 그래서 $\overline{f}(x)$는 $\mathbb{Z}_2[x]$에서 1차인수를 갖지 않는다.

$\mathbb{Z}_2[x]$에서 2차 인수는 x^2, x^2+x, x^2+1과 x^2+x+1뿐이다. 여러분은 긴 나눗셈을 사용하여 이들 중 어느 것도 $\overline{f}(x)$의 인수가 아님을 보여줄 수 있다.

더욱이, $\overline{f}(x)$는 차수 3 또는 4인 인수를 가질 수 없다(가진다면, 다른 인수는 차수 2 또는 1을 갖는다. 이것은 불가능하다). 그러므로 $\overline{f}(x)$는 $\mathbb{Z}_2[x]$에서 기약이다. 따라서 $f(x)$는 $\mathbb{Q}[x]$에서 기약이다. ■

주목 $\mathbb{Z}[x]$에서 다항식이 $\mathbb{Z}_p[x]$에서 가약인 다항식으로 p를 법으로 변형되면, 정리 4.5.5로부터, 어떤 결론도 끌어내질 수 없다. 불행하게도, $f(x)$가 실제로 $\mathbb{Q}[x]$에서 기약일 때 조차도, $f(x)$의 변형이 $\mathbb{Z}_p[x]$에서 가약이 되는 많은 p가 존재 할 수 있다. 그러므로, 정리 4.5.5를 적용하기위하여, 외견상 보다 더 많

은 횟수의 시도가 필요 할 수 있다.

예제 | 4.5.1 다음을 기약다항식의 곱으로 써라.

(a) $2x^3+x^2+2\in\mathbb{Z}_3[x]$

(b) $x^3+3x^2+x+4\in\mathbb{Z}_5[x]$

►풀이◄ (a) $0,1,2$를 각각 대입한다. 그러면

$$f(0)\neq 0,\ f(1)\neq 0,\ f(2)\neq 0.$$

$\therefore\ 2x^3+x^2+2\in\mathbb{Z}_3[x]$는 기약이다.

(b) $f(1),f(2),f(3)\neq 0,\ \ f(-1)=f(4)=0.$

$\therefore\ (x^3+3x^2+x+4)=(x+1)(x^2+2x-1)\in\mathbb{Z}_5[x].$ ■

유제 | 4.5.1 다음을 기약다항식의 곱으로 써라.

(1) $x^2+5\in\mathbb{Z}_7[x]$

(2) $x^4+x^3+2x^2+x+2\in\mathbb{Z}_3[x]$

(3) $x^5+x^2+x-1\in\mathbb{Z}_2[x]$

(4) $x^4+4\in\mathbb{Z}_5[x]$

예제 | 4.5.2 유리근 판정법을 사용하여 $-x^4+x^3+x^2+x+2$를

$\mathbb{Q}[x]$에서 기약다항식들의 곱으로 써라.

►풀이◄ $-(x+1)(x-2)(x^2+1).$ ■

유제 | 4.5.2 유리근 판정법을 사용하여 각 다항식을 $\mathbb{Q}[x]$에서 기약다항식들의 곱으로 써라.

(1) $3x^5+2x^4-7x^3+2x^2$

(2) $2x^4+7x^3+5x^2+7x+3$

예제 | 4.5.3 아이젠스타인의 판정법을 사용하여 $x^5-4x+22$이 $\mathbb{Q}[x]$에서 기약임을 보여라:

►풀이◄ $p=2$라 하자. 그러면 $p\mid 22,\ p\mid(-4)$이지만 $p\nmid 1$이고

$p^2\nmid 22$. 따라서 $x^5-4x+22$는 $\mathbb{Q}[x]$에서 기약이다. ■

유제 | 4.5.3 아이젠스타인의 판정법을 사용하여 $5x^{11}-6x^4+12x^3+36x-6$이 $\mathbb{Q}[x]$에서 기약임을 보여라.

예제 | 4.5.4 $f(x)$가 $\mathbb{Z}_p[x]$에서 기약이 되는 소수 p를 구함으로써 $7x^3+6x^2+4x+6$가 $\mathbb{Q}[x]$에서 기약임을 보여라:

►풀이◄ $p=5$ 라 하자. 그러면 $\mathbb{Z}_5[x]$에서

$\overline{f}(x)=2x^3+x^2+4x+1.$

그래서 $\overline{f}(0)=1\neq 0, \overline{f}(1)=3\neq 0, \overline{f}(2)=4\neq 0,$ $\overline{f}(3)=1\neq 0, \overline{f}(4)=1\neq 0.$ 그러므로 $\overline{f}(x)$는 $\mathbb{Z}_5$에서 해를 갖지 않는다. 따름정리 4.4.3-2에 의해서 $\overline{f}(x)$는 $\mathbb{Z}_5[x]$에서 기약이다. 그런데 $p=5$는 소수이고 $p\nmid 7$. 따라서, 정리 4.5.5에 의하여, $f(x)$는 $\mathbb{Q}[x]$에서 기약이다.

■

유제 | 4.5.4 $f(x)$가 $\mathbb{Z}_p[x]$에서 기약이 되는 소수 p를 구함으로써

$9x^4+4x^3-3x+77x^3+6x^2+4x+6$가 $\mathbb{Q}[x]$에서 기약임을 보여라.

예제 | 4.5.5 F는 체이고 $f(x)\in F[x]$라 하자. $c\in F$이고 $f(x+c)$가 $F(x)$에서 기약이면, $f(x)$는 $F[x]$에서 기약이다. 이를 증명하라. [힌트: 모순법을 사용하라.]

▸풀이◂ $f(x)=g(x)h(x)$라 가정하자. 그러면 $f(x+c)=g(x+c)h(x+c)$. 가정에서 $f(x+c)$가 $F[x]$에서 기약이므로, $g(x+c)$ 또는 $h(x+c)$는 영 아닌 상수 다항식이다. 그래서 $g(x)$ 또는 $h(x)$는 영이 아닌 상수다항식이다.

따라서 $f(x)$는 기약이다. ■

유제 | 4.5.5 $f(x+1)$이 기약임을 보이기 위하여 아이젠스타인의 판정법을 사용하고 예제 4.5.5를 적용함으로써 $f(x)=x^4+4x+1$이 $\mathbb{Q}[x]$에서 기약임을 증명하라.

4.6 $\mathbb{R}[x]$와 $\mathbb{C}[x]$에서 기약성

$\mathbb{Q}[x]$에서의 경우와는 달리 $\mathbb{R}[x]$와 $\mathbb{C}[x]$에서 모든 기약다항식에 대하여 명백하게 설명 할 수 있다. 그러므로 유리근 판정법이나 아이젠스타인의 판정법이 없이 $\mathbb{R}[x]$ 또는 $\mathbb{C}[x]$에서 다항식이 기약인지 아닌지를 곧바로 말할 수 있다. 이러한 사실들은 1799년에 가우스(Gauss)가 처음에 증명했던 다음의 정리의 결과다.

정리 4.6.1 대수학의 기본정리
(The Fundamental Theorem of Algebra)

$\mathbb{C}[x]$의 모든 비상수 다항식은 $\mathbb{C}$에서 근을 갖는다.

이 정리는 때때로 체$\mathbb{C}$가 대수적으로 닫힌다(algebraically closed)고 말함으로써 다른 용어로 표시된다. 이 정리에 대하여 알려진 모든 증명은 해석학(analysis) 및 (또는) 복소변수(complex variable)함수론으로 부터의 사실들에 상당히 의존한다. 이 이유 때문에, 우리는 $\mathbb{C}[x]$와 $\mathbb{R}[x]$에서 기약성에 대한 기본정리와 밀접한 몇 가지 관계만을 생각할 것이다. 증명에 대

하여, 맥코이(Mccoy)와 베르거(Berger)[6] 또는 헝거포드(Hungerford)[7]를 보라.

따름정리 4.6.1-1

다항식이 $\mathbb{C}[x]$에서 기약일 필요충분조건은 이 다항식의 차수 1인 것이다.

따름정리 4.6.1-2

$\mathbb{C}[x]$에서 차수 n인 모든 비상수 다항식 $f(x)$는 어떤 $c, a_1, a_2 \ldots a_n \in \mathbb{C}$에 대하여 $c(x-a_1)(x-a_2)\ldots(x-a_n)$꼴로 써질 수 있다. 이 인수분해는 인수의 순서를 제외하고 유일하다.

$\mathbb{R}[x]$에서 모든 기약 다항식의 설명을 얻기 위하여, 우리는 다음의 결과가 필요하다.

보조정리 4.6.2

$f(x) \in \mathbb{R}[x]$이고 $a+bi$가 $\mathbb{C}$에서 $f(x)$의 근이면 $a-bi$ 역시 $f(x)$의 근이다.

정리 4.6.3

다항식 $f(x)$가 $\mathbb{R}[x]$에서 기약일 필요충분조건은 $f(x)$가 1차 다항식이거나 또는 $b^2-4ac<0$ 인 $f(x)=ax^2+bx+c$이다.

►증명◄ ($\Leftarrow$): 분명히 성립한다.

($\Rightarrow$): 다항식 $f(x)$가 $\mathbb{R}[x]$에서 기약이고 $\deg f(x) \geq 2$라 가정하

자. 즉, $\mathbb{R}$에서 근을 갖지 않는다. 그러면 정리 4.6.1에 의하여, $f(x)$는 $\mathbb{C}$에서 근 w을 갖는다. 보조정리 4.6.2에 의하여, $\overline{w}$역시 $f(x)$의 근이다. 더욱이 $w \neq \overline{w}$($w=\overline{w}$가 가정하면 w는 $f(x)$의 실근이다. 그러면 이것은 $f(x)$의 기약성에 모순이다)이다. 그래서 인수정리에 의하여, $x-w$와 $x-\overline{w}$는 $\mathbb{C}[x]$에서 $f(x)$의 인수다. 그러므로 $h(x) \in \mathbb{C}[x]$가 존재하여

$$f(x) = (x-w)(x-\overline{w})h(x)$$

이다. $g(x) = (x-w)(x-\overline{w})$라 하자. 그러면

$$f(x) = g(x)h(x) \in \mathbb{C}[x]$$

이다. 더욱이 $w = r+si$ $(r, s \in \mathbb{R})$면,

$$g(x) = (x-w)(x-\overline{w}) = (x-(r+si))(x-(r-si))$$
$$= x^2 - 2rx + (r^2+s^2).$$

그러면 $g(x)$의 계수는 실수다.

이제 우리는 $h(x)$ 역시 실수계수를 가짐을 보이고자 한다. $\mathbb{R}[x]$에서 나눗셈 알고리즘에 의하여, 다항식 $q(x)$, $r(x) \in \mathbb{R}[x]$가 존재하여

$$f(x) = g(x)q(x) + r(x)$$

존재한다. 여기서 $r(x) = 0$ 또는 $\deg r(x) < \deg g(x)$이다. 그러나 $\mathbb{C}[x]$에서, $f(x) = g(x)q(x) + 0$이다. $q(x)$와 $r(x)$는 $\mathbb{C}[x]$에서 다항식으로 생각 될 수 있으므로 $\mathbb{C}[x]$에서 나눗셈 알고리

즘의 유일성에 의하여, $q(x) = h(x)$이고 $r(x) = 0$이다. 따라서 $h(x) = q(x) \in \mathbb{R}[x]$이다.

$f(x) = g(x)h(x)$, $f(x)$는 $\mathbb{R}[x]$에서 기약이고 $\deg g(x) = 2$이므로, $h(x)$는 상수 $d \in \mathbb{R}$이어야만 한다. 그러므로 $f(x) = dg(x)$는 $\mathbb{R}[x]$에서 2차 다항식이다. 즉, $f(x) = ax^2 + bx + c$꼴이다. 여기서 $a, b, c \in \mathbb{R}$. $f(x)$는 $\mathbb{R}$에서 근을 갖지 않으므로, $b^2 - 4ac < 0$ ■

따름정리 4.6.3

$\mathbb{R}[x]$에서 홀수차수의 모든 다항식은 $\mathbb{R}$에서 근을 갖는다.

►증명◄ 정리4.3.4에 의하여, $f(x) = p_1(x)p_2(x) \ldots p_k(x)$이고 각 $p_i(x)$는 $\mathbb{R}[x]$에서 기약이다. 그러면, 정리 4.6.3에 의하여, 각 $p_i(x)$는 차수1 또는 2를 갖는다. 그래서 정리 4.1.2에 의하여,

$$\deg f(x) = \deg p_1(x) + \deg p_2(x) + \ldots \deg p_k(x).$$

$f(x)$는 홀수차수를 가지므로, $p_i(x)$들 중의 적어도 하나는 차수 1을 가져야만 한다. 그러므로 $f(x)$는 $\mathbb{R}[x]$에서 1차인수를 갖는다. 따라서 $f(x)$는 $\mathbb{R}$에서 근을 갖는다. ■

예제 | 4.6.1 다항식 $x^4-3x^3+x^2+7x-30$의 $\mathbb{C}$에서 모든 근을 구하라.(하나의 근 $1-2i$)

►풀이◄ $1-2i, 1+2i, 3, -2$. ■

유제 | 4.6.1 다항식 $x^4-4x^3+3x^2+14x+26$의 $\mathbb{C}$에서 모든 근을 구하라(하나의 근은 $3+2i$).

예제 | 4.6.2 다항식 x^4-2를 $\mathbb{Q}[x]$, $\mathbb{R}[x]$와 $\mathbb{C}[x]$에서 기약다항식들의 곱으로 인수분해하라:

►풀이◄ $\mathbb{Q}[x]$에서, x^4-2.

$\mathbb{R}[x]$에서, $(x^2+\sqrt{2})(x+\sqrt[4]{2})(x-\sqrt[4]{2})$.

$\mathbb{C}[x]$에서, $(x-\sqrt[4]{2}\,i)(x+\sqrt[4]{2}\,i)(x+\sqrt[4]{2})(x-\sqrt[4]{2})$.

■

유제 | 4.6.2 다항식 x^3-x^2-5x+5를 $\mathbb{Q}[x]$, $\mathbb{R}[x]$와 $\mathbb{C}[x]$에서 기약다항식들의 곱으로 인수분해하라.

예제 | 4.6.3 $f(x)=ax^2+bx+c\in\mathbb{R}[x]$이고 $a\neq 0$라 하자. $\mathbb{C}$에서 $f(x)$의 근이 $(-b+\sqrt{b^2-4ac})/2a$와 $(-b-\sqrt{b^2-4ac})/2a$임을 증명하라.

[힌트:$a^2+bx+c=0\Leftrightarrow x^2+(b/c)x=-c/a$ 임을 보이고 왼쪽 변을 완전 제곱하여 x를 구하라.]

►풀이◄ $ax^2+bx+c \Leftrightarrow x^2+\dfrac{b}{a}x=-\dfrac{c}{a}$

$$\Leftrightarrow (x+\frac{b}{2a})^2=\frac{b^2}{4a^2}-\frac{c}{a}=\frac{b^2-4ac}{4a^2}$$

$$\Leftrightarrow x+\frac{b}{2a}=\pm\sqrt{\frac{b^2-4ac}{4a^2}}=\pm\frac{\sqrt{b^2-4ac}}{2a}.$$

따라서 $\mathbb{C}$에서 $f(x)$의 근은

$$\frac{-b+\sqrt{b^2-4ac}}{2a}\text{와}\quad\frac{-b-\sqrt{b^2-4ac}}{2a}.$$

■

유제 | 4.6.3 $b^2-4ac<0$인 모든 $ax^2+bx+c\in\mathbb{R}[x]$는 $\mathbb{R}[x]$에서 기약임을 증명하라. [도움말: 예제 4.6.3을 보라.]

4장 연습문제

1. $c \in R$가 교환환 R의 영인수면, c는 역시 $R[x]$의 영인수인가?

2. R은 교환환이라 하자. $a_n \neq 0_R$이고 $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$이 $R[x]$의 영인수이면, a_n은 R의 영인수임을 보여라.

3. R은 정역이라 하자. 나눗셈 알고리즘이 $R[x]$에서 언제나 성립한다고 가정한다. R은 체임을 증명하라.

4. $\overline{h}(a_0 + a_1x + \cdots + a_nx^n) = h(a_0) + h(a_1)x + h(a_2)x^2 + \cdots + h(a_n)x^n$

다음의 각각을 증명하라.
(1) $\overline{h}$는 환들의 준동형사상이다.
(2) $\overline{h}$가 단사다 $\Leftrightarrow$ h가 단사다.
(3) $\overline{h}$가 전사다 $\Leftrightarrow$ h가 전사다.
(4) $R \cong S$이면, $R[x] \cong S[x]$.

5. $a, b \in F$이고 $a \neq b$라 하자. $x+a$와 $x+b$는 $F[x]$에서 서로소(relatively prime)임을 보여라.

6. $f(x) \in F[x]$라 하고 모든 상수가 아닌 $g(x) \in F[x]$에 대하여 $f(x) | g(x)$라 가정하자. $f(x)$는 상수다항식임을 증명하라.

7. $f(x)$가 0_F와 서로소이면, $f(x)$에 대하여 무엇을 말할 수 있는가?

(2) $f(x), g(x) \in F[x]$가 F에서 같은 근을 가지면, 이들은 $F[x]$에서 동반원인가?

16. x^2+1가 $\mathbb{Z}_p[x]$에서 가약이다 $\Leftrightarrow$ $\exists\, a, b \in \mathbb{Z}$ $s.t.$ $p = a+b$이고 $ab \equiv 1 \pmod{p}$. 이를 증명하라.

17. a는 F의 고정된 원이고 함수 $\varphi_a : F[x] \to F$는 $\varphi[f(x)] = f(a)$로 정의된다고 하자. 그러면 φ_a는 환들의 전사 준동형사상이다. 이를 증명하라. 함수 φ_a를 **수값 준동형사상(evaluation homomorphism)**이라 한다.

18. 정수 계수를 갖는 모닉 다항식이 $\mathbb{Z}[x]$에서 차수 m과 n인 다항식들의 곱으로 인수분해 되면, 이 다항식은 $\mathbb{Z}[x]$에서 차수 m과 n인 모닉 다항식들의 곱으로 인수분해 될 수 있음을 증명하라.

19. $30x^n - 91$는 $\mathbb{Q}$에서 근을 갖지 않음을 증명하라. 여기서 $n \in \mathbb{Z}$이고 $n > 1$이다.

20. $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1(x) + a_0 \in \mathbb{Z}[x]$라 하자. p가 $p \mid a_1, \cdots, p \mid a_n$, $p \nmid a_0$이고 $p^2 \nmid a_n$인 소수가 존재하면, $f(x)$는 $\mathbb{Q}[x]$에서 기약이다. 이를 증명하라.
[도움말 $y = 1/x$라 놓는다. 그러면 이 결과는 정리 4.5.4에 의하여 기약이다.]

21. $f(x) = a_nx^n + \cdots + a_1x + a_0$, $g(x) = b_rx^r + \cdots + b_1x + b_0$와 $h(x) = c_sx^s + \cdots + c_1x + c_0$는 $f(x) = g(x)h(x)$인 $\mathbb{Z}[x]$에서 다항식이면, $\mathbb{Z}_n[x]$에서, $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ 이다. 이를 증명하라.

22. 중복근이 없는 $\mathbb{R}[x]$에서 홀수 차수의 다항식은 홀수 개의 실근을 가짐을 증명하라.

8. $x^3 - 3$은 $\mathbb{Z}_7[x]$에서 기약임을 보여라.

9. 유일인수분해를 사용하여 $\mathbb{C}[x]$에서 다음의 gcd를 구하라.

$$(x-3)^3(x-4)^4(x-i)^2 \text{과 } (x-1)(x-3)(x-4)^3$$

10. R은 정역이라 하자. 그러면

$$f(x) \text{가 } R[x] \text{의 단원이다} \Leftrightarrow f(x) = c \text{이고 } c \text{는 } R \text{의 단원이다.}$$

이를 증명하라.

11. $F[x]$에서 $x - 1_F$가 $a_nx^n + \cdots + a_2x^2 + a_1x + a_0$의 약수이다. $\Leftrightarrow$ $a_0 + a_1 + a_2 + \cdots + a_n = 0_F$.
이를 증명하라.

12. 인수정리를 사용하여 $\mathbb{Z}_7[x]$에서 $x^7 - x$가 $x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)$으로 인수분해 됨을 보여라. 단 어떠한 다항식의 곱셈도 하지 않는다.

13. $\mathbb{Z}_3[x]$에서 차수 2인 모든 모닉 기약다항식을 열거하라. 역시 $\mathbb{Z}_5[x]$에서 같은 일을 하라.

14. $\mathbb{Z}_p[x]$에서 $x-2$가 $x^4 + x^3 + 3x^2 + x + 1$의 약수가 되는 홀수 소수 p를 구하라.

15. (1) $f(x)$와 $g(x)$가 $F[x]$에서 동반원이면, 이들은 F에서 같은 근을 가짐을 보여라.