$F[x]$에서 합동과 합동류 계산

추상대수학(abstract algebra)

5.1 $F[x]$에서 합동과 합동류

정수의 합동개념은 나뉘어 떨어짐에 대한 어떤 기초적인 사실에만 의존한다. F가 체면, 다항식 환 $F[x]$는 본질5.1적으로 $\mathbb{Z}$가 갖는 것과 같은 나뉘어 떨어짐의 성질을 갖는다. 그래서 $\mathbb{Z}$에서 합동개념과 이 개념의 기초적인 성질(2.1절)이 거의 말대로 $F[x]$로 옮겨지게 될 수 있음은 놀라운 일이 아니다.

정의 5.1.1

F는 체, $f(x), g(x), p(x) \in F[x]$이고, $p(x) \neq 0_F$라 하자. 만약 $p(x) \mid [f(x)-g(x)]$이면 $f(x)$가 $p(x)$를 법으로 $g(x)$와 합동 ($f(x)$ is congruent to $g(x)$ modulo $p(x)$)이라 하고

$f(x) \equiv g(x) \pmod{p(x)}$라 쓴다.

보기 5.1.1 $\mathbb{Q}[x]$에서 $x^2+x+1 \equiv x+2 \pmod{x+1}$이다. 왜냐하면,

$$(x^2+x+1)-(x+2) = x^2-1 = (x+1)(x-1). \quad \blacksquare$$

보기 5.1.2 $\mathbb{R}[x]$에서

$$3x^4+4x^2+2x+2 \equiv x^3+3x^2+3x+4 \pmod{x^2+1}.$$

왜냐하면, 긴 나눗셈에 의하여,

$$\begin{aligned}&(3x^4+4x^2+2x+2)-(x^3+3x^2+3x+4)\\ &= 3x^4-x^3+x^2-x-2\\ &= (x^2+1)(3x^2-x-2). \quad \blacksquare\end{aligned}$$

정리 5.1.2

F는 체이고 $p(x)$는 $F[x]$에서 영이 아닌 다항식이라 하자. 그러면 $p(x)$를 법으로 하는 합동의 관계는 같은꼴관계다. 즉

(1) 반사율: 모든 $f(x)\in F[x]$에 대하여 $f(x)\equiv f(x) \pmod{p(x)}$.

(2) 대칭율: $f(x)\equiv g(x) \pmod{p(x)}$이면,

$$g(x)\equiv f(x) \pmod{p(x)}.$$

(3) 추이율: $f(x)\equiv g(x)\pmod{p(x)}$이고 $g(x)\equiv h(x)\pmod{p(x)}$이면, $f(x)\equiv h(x) \pmod{p(x)}$.

[증명](1) $f(x)-f(x)=0$이고 $p(x)|0$이므로

$f(x)\equiv f(x) \pmod{p(x)}$이다.

(2) $f(x)\equiv g(x) \pmod{p(x)}$라 가정하자. 그러면

$p(x)|[f(x)-g(x)]$이다. $k(x)\in F[x]$가 존재하여

$f(x)-g(x)=p(x)k(x)$이다. 그러므로

$g(x)-f(x)=-(f(x)-g(x))=-p(x)k(x)=p(x)(-k(x))$이고

$-k(x)\in F[x]$이다. 그래서 $p(x)|(g(x)-f(x))$이므로

$g(x)\equiv f(x) \pmod{p(x)}$이다.

(3) $f(x)\equiv g(x) \pmod{p(x)}$이고 $g(x)\equiv h(x) \pmod{p(x)}$이라 가정하자. 그러면 $k(x), t(x)\in F[x]$가 존재하여

$f(x)-g(x)=p(x)k(x)$이고 $g(x)-h(x)=p(x)t(x)$이다.

그래서
$$\begin{aligned} f(x)-h(x)&=(f(x)-g(x))+(g(x)-h(x))\\ &=p(x)k(x)+p(x)t(x)\\ &=p(x)(k(x)+t(x)) \end{aligned}$$

$k(x)+t(x)\in F[x]$이므로, $p(x)|(f(x)-h(x))$이다. 따라서 $f(x)\equiv h(x) \pmod{p(x)}$이다. ■

정리 5.1.3

F는 체이고 $p(x)$는 $F[x]$에서 영이 아닌 다항식이라 하자.

$f(x)\equiv g(x) \pmod{p(x)}$이고 $h(x)\equiv k(x) \pmod{p(x)}$이면,

(1) $f(x)+h(x)\equiv g(x)+k(x) \pmod{p(x)}$,

(2) $f(x)h(x)\equiv g(x)k(x) \pmod{p(x)}$.

[증명] (1) 합동의 정의에 의하여, $k(x), t(x)\in F[x]$가 존재하여

$f(x)-g(x)=p(x)k(x)$이고 $h(x)-k(x)=p(x)t(x)$이다.

그러면

$$f(x)+h(x)-(g(x)+k(x)) = (f(x)-g(x))+(h(x)-k(x))$$
$$= p(x)k(x)+p(x)t(x)$$
$$= p(x)(k(x)+t(x))$$

그래서 $p(x)\mid[(f(x)+h(x))-(g(x)+k(x))]$.

따라서 $f(x)+h(x)\equiv g(x)+k(x) \pmod{p(x)}$이다.

(2)

$$f(x)h(x)-g(x)k(x) = f(x)h(x)-g(x)h(x)+g(x)h(x)-g(x)k(x)$$
$$= h(x)(f(x)-g(x))+g(x)(h(x)-k(x))$$
$$= h(x)p(x)k(x)+g(x)p(x)t(x)$$
$$= p(x)(h(x)k(x)+g(x)t(x))$$

그러므로 $p(x)\mid(f(x)h(x)-g(x)k(x))$이고

$f(x)h(x)\equiv g(x)k(x) \pmod{p(x)}$이다. ■

정의 5.1.4

F는 체, $f(x),\ p(x)\in F[x]$이고 $p(x)\neq 0_F$라 하자. $p(x)$를 법으로 $f(x)$의 합동류(congruence class) 또는 나머지류(residue class)는 $p(x)$를 법으로 $f(x)$와 합동인 $F[x]$의 모든 다항식으로 이루어지고 이를 $[f(x)]$로 쓴다. 따라서

$$[f(x)] = \{g(x) : g(x)\in F[x]\text{이고}\quad g(x)\equiv f(x) \pmod{p(x)}\}.$$

$g(x)\equiv f(x) \pmod{p(x)}$는 어떤 $k(x)\in F[x]$에 대하여 $g(x)-f(x)=k(x)p(x)$ 또는 논리적으로 같게 $g(x)=f(x)+k(x)p(x)$를 의미하므로,

$$[f(x)] = \{g(x) : g(x)\equiv f(x) \pmod{p(x)}\}$$
$$= \{f(x)+k(x)p(x) \mid k(x)\in F[x]\}.$$

보기 5.1.3 $\mathbb{R}[x]$에서 x^2+1을 법으로 하는 합동을 생각하자. 그러면

$$[2x+1] = \{(2x+1)+k(x)(x^2+1) : k(x)\in\mathbb{R}[x]\}.$$

나눗셈 알고리즘에 의하여, 이 집합의 원들은 x^2+1로 나누어질 때 나머지가 $2x+1$인 $\mathbb{R}[x]$에 속하는 다항식들이다. ■

보기 5.1.4 $\mathbb{Z}_2[x]$에서 x^2+x+1을 법으로 하는 합동을 생각하자.

$x+1\in[x^2]$임을 보여라.

[증명] $x^2\equiv x+1 \pmod{x^2+x+1}$임에 주목하라. 왜냐하면,

$x^2-(x+1)=x^2-x-1=(x^2+x+1)1$($\mathbb{Z}_2[x]$에서 $1+1=0$. 그래서 $1=-1$임을 기억하라.)이기 때문이다. 그러므로 $x+1\in[x^2]$이다. 다음의 정리는 $[x+1]=[x^2]$임을 보여준다. ■

정리 5.1.5

$$f(x)\equiv g(x) \pmod{p(x)} \Leftrightarrow [f(x)]=[g(x)].$$

[증명] $\Rightarrow$] $a(x)\in[f(x)]$라 하자. 그러면 $k(x)\in F[x]$가 존재하여 $a(x)=f(x)+k(x)p(x)$이다. $f(x)\equiv g(x)\pmod{p(x)}$이므로 $t(x)\in F[x]$가 존재하여 $p(x)t(x)=f(x)-g(x)$이다. 따라서

$$\begin{aligned} a(x) &= p(x)t(x)+g(x)+k(x)p(x) \\ &= g(x)+(k(x)+t(x))p(x) \end{aligned}$$

이고 $k(x)+t(x)\in F[x]$이므로 $a(x)\in[g(x)]$이다. 따라서 $[f(x)]\subseteq[g(x)]$이다. 비슷하게 $[f(x)]\supseteq[g(x)]$ 임을 보일 수 있다.

$\Leftarrow$] $[f(x)]=[g(x)]$이므로 $f(x)\in[g(x)]$이다. $k(x)\in F[x]$가 존재하여 $f(x)=g(x)+k(x)p(x)$이다. $f(x)-g(x)=(-k(x))p(x)$

이고 $-k(x)\in F[x]$이므로 $f(x)\equiv g(x)\pmod{p(x)}$이다.

■

따름정리 5.1.6 (구 5.1.5-1)

$p(x)$를 법으로 두 합동류는 서로소이거나 또는 일치한다.

[증명] $[f(x)]\cap[g(x)]=\varnothing$이면 증명할 필요가 없으므로 $[f(x)]\cap[g(x)]\neq\varnothing$라 하자. 그러면 $k(x)\in F[x]$가 존재하여 $k(x)\in[f(x)]$이고 $k(x)\in[g(x)]$이다. 합동류의 정의에 의하여 $k(x)\equiv f(x)\pmod{p(x)}$이고 $k(x)\equiv g(x)\pmod{p(x)}$이므로 $f(x)\equiv g(x)\pmod{p(x)}$이므로 $[f(x)]=[g(x)]$이다. ■

$\mathbb{Z}$에서 n을 법으로 하는 합동에서, 꼭 n개의 다른 합동류가 존재한다(따름정리 2.1.5-2). 이러한 류들은 $[0]$, $[1]$, $\cdots$, $[n-1]$이다. n에 의한 나눗셈에서 각 가능한 나머지에 대한 류가 존재함에 주목하라. $F[x]$에서 차수 n인 다항식에 의한 나눗셈에서 가능한 나머지는 n보다 더 작은 (물론 0도 포함) 차수의 모든 다항식들이다. 그래서 우리는 따름정리 2.1.5-2와 비슷한 결과를 얻는다.

따름정리 5.1.7 (구 5.1.5-2)

F는 체, $p(x)$는 $F[x]$에서 차수 n인 다항식이고

$$S=\{0_F\}\cup\{g(x)\in F[x] : \deg g(x)<n\}$$

라 하자. 그러면 $p(x)$를 법으로 하는 모든 합동류는 S에 속하는 어떤 다항식의 류이고, S의 다른 다항식들의 합동류들은 다르다.

[증명] S에 속하는 다른 두 다항식은 $p(x)$를 법으로 합동일 수 없다. 왜냐하면, 이 두 다항식의 차는 n보다 더 작은 차수를 갖고, 그러므로 $p(x)$로 나누어질 수 없기 때문이다. 그래서 정리 5.1.5에 의하여, S에 속하는 다른 다항식은 다른 합동류에 속해야만

한다. 따름정리 2.1.5-2의 증명의 마지막 부분에서처럼, 나눗셈 알고리즘을 사용하여 $F[x]$에서 모든 다항식이 $p(x)$를 법으로 S에 속하는 한 다항식과 합동임을 보여준다. 따라서 정리 5.1.5에 의하여, 모든 합동류는 S에 속하는 어떤 다항식의 합동류와 같다. ■

$p(x)$를 법으로 하는 모든 합동류들의 집합을 $F[x]/p(x)$로 나타낸다. 이것은 $\mathbb{Z}_n$의 표시법과 비슷하다.

보기 5.1.5 $\mathbb{R}[x]$에서 x^2+1을 법으로 하는 합동을 생각하자. x^2+1에 의한 나눗셈에서 각 가능한 나머지에 대한 합동류들이 있다. 이제 가능한 각 나머지는 $rx+s(r,\ s\in\mathbb{R})$ 꼴의 다항식들이다. r, s 중의 하나 또는 둘 다 0일 수 있다. 그래서 $\mathbb{R}[x]/(x^2+1)$은

$$[0],\ [x],\ [x+1],\ [5x+3],\ \left[\frac{7}{9}x+2\right],\ [x-7],\ \cdots$$

을 포함하여 무한히 많은 다른 합동류들로 이루어진다. 따름정리 5.1.5-2에 의 하여,

$$[rx+s]=[cx+d]\Leftrightarrow rx+s=cx+d.$$

다항식의 같음의 정의에 의하여, $rx+s=cx+d\Leftrightarrow r=c$이고 $s=d$이다. 따라서$\mathbb{R}[x]/(x^2+1)$의 모든 원은 $[rx+s]$ 꼴로 유일하게 쓰일 수 있다. ■

보기 5.1.6 $\mathbb{Z}_2[x]$에서 x^2+x+1을 법으로 하는 합동을 생각하자. 그러면 x^2+x+1에 의한 나눗셈에서 가능한 나머지는

$ax+b(a,\ b\in\mathbb{Z}_2)$ 꼴의 다항식이다. 그래서 4가지 가능한 나머지들만 있다. 0, 1, x와 $x+1$이다. 따라서

$$\mathbb{Z}_2[x]/(x^2+x+1)=\{[0],\ [1],\ [x],\ [x+1]\}.$$ ■

보기 5.1.7 보기 5.1.6에서 패턴은 일반적인 경우에 도움이 된다. $p(x)\in\mathbb{Z}_n[x]$가 차수 k를 가지면 $p(x)$에 의한 나눗셈에서 가능한 나머지는 $a_0+a_1x+\cdots+a_{k-1}x^{k-1}$ 꼴이다. 여기서 $a_i\in\mathbb{Z}_n$이다. k개의 계수 $a_0,\ \cdots,\ a_{k-1}$의 각각에 대하여 n개의 가능성이 있고, 이와 같은 꼴의 n^k개의 다른 다항식이 있

다. 따라서 따름정리 5.1.5-2에 의하여, $\mathbb{Z}_n[x]/(p(x))$에 꼭 n^k 개의 다른 합동류가 존재한다. ■

예제 5.1.1 $f(x) \equiv g(x) \pmod{p(x)} \Leftrightarrow f(x)$와 $g(x)$가 $p(x)$로 나누어질 때 같은 나머지를 갖는다. 이를 증명하라.

[풀이] ($\Rightarrow$) : $f(x) \equiv g(x) \pmod{p(x)}$라 가정하자. 나눗셈 알고리즘에 의하여, 다항식 $q(x)$, $r(x) \in F[x]$가 존재하여

$f(x) = p(x)q(x) + r(x)$, $r(x) = 0_F$ 또는 $\deg r(x) < \deg p(x)$를 만족한다. 그리고 $q'(x), r'(x) \in F[x]$가 존재하여

$g(x) = p(x)q'(x) + r'(x)$, $r'(x) = 0_F$ 또는 $\deg r'(x) < \deg p'(x)$

를 만족한다. 그러면

$$r(x) - r'(x) = f(x) - g(x) + p(x)[q'(x) - q(x)] \qquad (5.1.1)$$

이다. $f(x) \equiv g(x) \pmod{p(x)}$이므로 다항식 $h(x) \in F[x]$가 존재하여 $f(x) - g(x) = p(x)h(x)$이다. (5.1.2)

식 (5.1.1)와 식 (5.1.2)에 의하여,

$r(x) - r'(x) = p(x)[h(x) + q'(x) - q(x)]$이다.

여기서 $h(x) + q'(x) - q(x) \in F[x]$이다.

그래서 $p(x) \mid [r(x) - r'(x)]$이다. 그런데 $\deg r(x) < \deg p(x)$이고

$\deg r'(x) < \deg p(x)$이므로 $\deg (r(x) - r'(x)) < \deg p(x)$이다.

따라서 $r(x) - r'(x) = 0_F$이다. 따라서 $r(x) = r'(x)$.

($\Leftarrow$) : 이것은 합동의 정의에 의하여 분명하다. ■

유제 5.1.1 $p(x)$가 $F[x]$에서 영이 아닌 상수다항식이면, $F[x]$에 속하는 임의의 두 다항식은 $p(x)$를 법으로 합동이다. 이를 증명하라.

예제 5.1.2 $p(x)$가 $k(x)$와 서로소이고

$f(x)k(x) \equiv g(x)k(x) \pmod{p(x)}$이면,

$f(x) \equiv g(x) \pmod{p(x)}$임을 증명하라.

[풀이] $f(x)k(x) \equiv g(x)k(x) \pmod{p(x)}$이므로

$$p(x) \mid (f(x) - g(x))k(x).$$

$p(x)$와 $k(x)$가 서로소이므로 정리 4.2.4에 의하여, $p(x) \mid (f(x) - g(x))$. 따라서 $f(x) \equiv g(x) \pmod{p(x)}$. ■

유제 5.1.2 $f(x)$가 $p(x)$와 서로소이면, 다항식 $g(x) \in F[x]$가 존재하여 $f(x)g(x) \equiv 1_F \pmod{p(x)}$을 만족한다.

이를 증명하라.

예제 5.1.3 $p(x)$는 $F[x]$에서 기약이고 $f(x)g(x) \equiv 0_F \pmod{p(x)}$이면 $f(x) \equiv 0_F \pmod{p(x)}$ 또는 $g(x) \equiv 0_F \pmod{p(x)}$임을 증명하라.

[풀이] $f(x)g(x) \equiv 0_F \pmod{p(x)}$이므로, $p(x) | f(x)g(x)$이다. $p(x)$는 기약다항식이므로 정리 4.3.3에 의하여, $p(x) | f(x)$ 또는 $p(x) | g(x)$. 따라서

$$f(x) \equiv 0_F \pmod{p(x)} \text{ 또는 } g(x) \equiv 0_F \pmod{p(x)}.$$

■

유제 5.1.3 $p(x)$가 $F[x]$에서 기약이 아니면, $f(x), g(x) \in F[x]$가 존재하여 $f(x) \not\equiv 0_F \pmod{p(x)}$이고, $g(x) \not\equiv 0_F \pmod{p(x)}$이다. 그러나 $f(x)g(x) \equiv 0_F \pmod{p(x)}$이다. 이를 증명하라.

예제 5.1.4 $\mathbb{Z}_3[x]$에서 $x^3 + 2x + 1$을 법으로 하는 합동에서 꼭 27개의 다른 합동류가 존재함을 보여라.

[풀이]

$\mathbb{Z}_3[x]/(x^3 + 2x + 1) = \{[ax^2 + bx + c] : a, b, c \in \mathbb{Z}_3\}$이 다 . 이때 a, b, c 각각이 취할 수 있는 값은 3가지이다. 따라서

$$|\mathbb{Z}_3[x]/(x^3 + 2x + 1)| = 3^3 = 27.$$

■

유제 5.1.4 $\mathbb{Z}_2[x]$에서 $x^3 + x + 1$을 법으로 하여 몇 개의 다른 합동류가 존재하는가? 이 합동류를 열거하라.

5.2 합동류 계산

정수들의 합동은 환 $\mathbb{Z}_n$이 된다. 비슷하게, $F[x]$에서 합동은 역시 새로운 환과 체를 만든다. 이들은 결국 환 $\mathbb{Z}_n$보다 구조에 있어서 훨씬 더 풍부함이 드러난다. 이 전개는 여기에서 2.2절과 밀접하게 비슷하다.

정리 5.2.1

F는 체이고, $p(x)$는 $F[x]$에서 비상수다항식이라 하자. $F[x]/p(x)$에서 $[f(x)]=[g(x)]$이고 $[h(x)]=[k(x)]$이면,
$[f(x)+h(x)]=[g(x)+k(x)]$이고 $[f(x)h(x)]=[g(x)k(x)]$이다.

[증명] $f(x)\equiv g(x)\pmod{p(x)}$이고 $h(x)\equiv k(x)\pmod{p(x)}$이므로 $f(x)+h(x)\equiv g(x)+k(x)\pmod{p(x)}$이고
$f(x)h(x)\equiv g(x)k(x)\pmod{p(x)}$이다. 따라서
$[f(x)+h(x)]=[g(x)+k(x)]$이고 $[f(x)h(x)]=[g(x)k(x)]$이다.
■

정리 5.2.1 때문에, 우리는 이제 정수에서처럼 합동류들의 덧셈과 곱셈을 정의할 수 있고, 이 연산들은 각 합동류에서 대표자들의 선택에 무관함이 분명하다.

정의 5.2.2

F는 체이고 $p(x)$는 $F[x]$에서 비상수다항식이라 하자. $F[x]/(p(x))$에서 덧셈과 곱셈을 다음과 같이 정의한다.

$$[f(x)]+[g(x)]=[f(x)+g(x)],\quad [f(x)][g(x)]\equiv[f(x)g(x)]$$

보기 5.2.1 $\mathbb{R}[x]$에서 x^2+1를 법으로 하는 합동을 생각하자. 그러면 합

동류 $[2x+1]$과 $[3x+5]$의 합과 곱은 각각 다음과 같다.

$$[2x+1][3x+5]=[(2x+1)(3x+5)]=[6x^2+13x+5],$$
$$[(2x+1)+(3x+5)]=[5x+6].$$

보기 5.1.5에서 주목하였듯이, $\mathbb{R}[x]/(x^2+1)$에 속하는 모든 합동류는 $[ax+b]$ 꼴로 쓰여질 수 있다. $[6x^2+13x+5]$를 이 꼴로 나타내기 위하여, $6x^2+13x+5$를 x^2+1로 나눈다. 그러면

$$6x^2+13x+5=6(x^2+1)+(13x-1).$$

그래서

$$6x^2+13x+5\equiv 13x-1\pmod{x^2+1}.$$

따라서 $[6x^2+13x+5]=[13x-1]$. ■

보기 5.2.2 보기 5.1.6에서, 우리는 $\mathbb{Z}_2[x]/(x^2+x+1)=\{[0],[1],[x],[x+1]\}$임을 알았다. 류들의 덧셈의 정의를 사용하여, 우리는 $[x+1]+[1]=[x+1+1]=[x]$($\mathbb{Z}_2$에서 $1+1=0$임을 기억하라.)임을 안다. 비슷한 계산에 의하여, 우리는 $\mathbb{Z}_2[x]/(x^2+x+1)$에 대한 다음의 덧셈표를 얻는다. $\mathbb{Z}_2[x]/(x^2+x+1)$에 대한 대부분의 곱셈표 역시 정의로부터

쉽게 얻어진다.

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$		
$[x+1]$	$[0]$	$[x+1]$		

이 표의 나머지를 채워 넣기 위한 예로써,

$$[x]\cdot[x+1]=[x(x+1)]=[x^2+x]$$

임에 주목하라. 이제 $\mathbb{Z}_2[x]$에서 긴 나눗셈 또는 간단한 덧셈은 $x^2+x=(x^2+x+1)+1$임을 보여준다. 그래서

$$x^2+x\equiv 1(\text{mod } x^2+x+1).$$

그러므로 $[x^2+x]=[1]$이다. 비슷한 계산에 의하여, $[x]\cdot[x]=[x^2]=[x+1]$ (왜냐면, $\mathbb{Z}_2[x]$에서 $x^2=(x^2+x+1)+(x+1)$이기 때문이다)이다. ■

여러분이 보기 5.2.2에 있는 표들을 검토하면, $\mathbb{Z}_2[x]/$

(x^2+x+1)은 항등원이 있는 가환환(실로, 체)임을 알게 될 것이다. $\mathbb{Z}$와 $\mathbb{Z}_n$에 대한 경험의 관점에서 이것도 그다지 놀라운 일이 아니다. 예기치 않은 것은 두 표의 위 왼쪽 모퉁이($[0]$과 $[1]$의 합과 곱)다. 부분집합 $F^*=\{[0],[1]\}$은 $\mathbb{Z}_2$와 동형이다(이 두 체계에 대한 표들은 F^*에 있는 대괄호들을 제외하고 일치한다). 이러한 사실들은 다음의 결과를 설명한다.

정리 5.2.3

F는 체이고 $p(x)$는 $F[x]$에서 비상수다항식이라 하자. 그러면 $F[x]/(p(x))$는 항등원이 있는 가환환이다. 더욱이, $F[x]/(p(x))$는 F와 동형인 부분환 F^*를 포함한다.

[증명] $F[x]/(p(x))$가 항등원이 있는 가환환임을 증명하기 위하여 정리 2.2.2의 증명을 각색한다.

$$F^*=\{[a]:a\in F\}$$

즉 F^*는 모든 상수다항식들의 합동류들로 이루어진 $F[x]/(p(x))$의 부분집합이라 하자. F^*는 $F[x]/(p(x))$의 부분

환임을 확인하라. 함수 $\varphi : F \to F^*$를 $\varphi(a) = [a]$로 정의한다. 그러면 분명히 φ는 전사함수이다. $F[x]/(p(x))$의 덧셈과 곱셈의 정의에 의하여,

$$\varphi(a+b) = [a+b] = [a] + [b] = \varphi(a) + \varphi(b),$$
$$\varphi(ab) = [ab] = [a] \cdot [b] = \varphi(a) \cdot \varphi(b).$$

그래서 φ는 준동형사상이다. 이제 φ가 단사함수임을 증명하자. 임의의 $a, b \in F$에 의하여 $\varphi(a) = \varphi(b)$라 가정하자. 그러면 $[a] = [b]$. 그래서 $a \equiv b \pmod{p(x)}$. 그러므로 $p(x) | (a-b)$. 그런데 $\deg p(x) \geq 1$이고 $a - b \in F$. 그래서 $a - b = 0$, 즉 $a = b$.

그러므로 φ는 단사함수이다. 따라서 $\varphi : F \to F^*$는 동형사상이다. ■

우리는 체 F와 $F[x]$의 다항식 $p(x)$에서 시작하였다. 지금 우리는 F의 동형의 복사를 포함하는 환 $F[x]/(p(x))$를 만들었다. 참으로 체 F 자신을 포함하는 환은 무엇과 같을까? 다음의 보기에서 설명되듯이, 이것을 완성하기 위한 두 가지 가능한 방법이 있다.

보기 5.2.3 보기 5.2.2에서, $\mathbb{Z}_2$와 동형인 부분집합 $F^* = \{[0], [1]\}$을 포

함하는 환 $\mathbb{Z}_2[x]/(x^2+x+1)$을 만들기 위하여 우리는 $\mathbb{Z}_2[x]$에서 다항식 x^2+x+1을 사용하였다. 우리는 $\mathbb{Z}_2$를 $\mathbb{Z}_2[x]/(x^2+x+1)$의 내부에 $\mathbb{Z}_2$의 동형의 복사 F^*와 일치시킨다고 가정하고 F^*의 원들이 마치 $\mathbb{Z}_2$의 원인 것처럼 F^*의 원들을 쓴다. 그러면 보기 5.2.2에 있는 표들은 다음과 같이 된다.

$+$	0	1	$[x]$	$[x+1]$
0	0	1	$[x]$	$[x+1]$
1	1	0	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	0	1
$[x+1]$	$[x+1]$	$[x]$	1	0

$\cdot$	0	1	$[x]$	$[x+1]$
0	0	0	0	0
1	0	1	$[x]$	$[x+1]$
$[x]$	0	$[x]$	$[x+1]$	1
$[x+1]$	0	$[x+1]$	1	$[x]$

이제 우리는 $\mathbb{Z}_2$를 부분집합으로 갖는 환을 갖는다. 이 과정이 여러분에게 약간 어려움을 줄지라도($\mathbb{Z}_2$는 부분집합인가?),

여러분은 같은 결과를 위하여 다음의 교체되는 길을 사용할 수 있다. E는 부분집합으로 $\mathbb{Z}_2$를 포함하는 임의의 4개 원의 집합, 즉 $E=\{0, 1, r, s\}$라 하자. E에서 덧셈과 곱셈은 다음과 같이 정의한다.

$+$	0	1	r	s
0	0	1	r	s
1	1	0	s	r
r	r	s	0	1
s	s	r	1	0

$\cdot$	0	1	r	s
0	0	0	0	0
1	0	1	r	s
r	0	r	s	1
s	0	s	1	r

$\mathbb{Z}_2[x]/(x^2+x+1)$에 대한 표들과 E에 대한 표들을 비교하

면, 이 두 환은 동형이다($[x]$를 r로 $[x+1]$을 s로 바꾸는 것은 표의 한 집합을 다른 집합으로 변화시킨다). 그러므로 E는 본질적으로 앞에서 얻었던 환과 같다. 그러나 E는, 어떠한 일치시킴도 없이, 진짜의 부분집합으로 $\mathbb{Z}_2$를 포함한다. ■

보기 5.2.3에서 처리되었던 것을 일반적인 경우에 적용할 수 있다. 체 F와 $F[x]$에서 다항식 $p(x)$가 주어지면, 우리는 부분집합으로 F를 포함하는 환을 만들 수 있다. 이렇게 하는 습관적인 방법은 F를 $F[x]/(p(x))$의 내부에 F의 동형의 복사 F^*와 일치시키고 F를 $F[x]/(p(x))$의 부분집합으로 생각

하는 것이다. 이렇게 하는 것이 여러분을 불편하게 할지라도, 보기 5.2.3에서처럼, 순수하게 부분집합으로 F를 포함하는 $F[x]/(p(x))$와 동형인 환을 언제나 만들 수 있음을 마음속에 간직하라. 이 후자의 접근은 귀찮게 되는 경향이 있기 때문에, 우리는 보통의 습관에 따르고 앞으로 F를 F^*와 일치시킨다. 그러므로 $a, b\in F$일 때 우리는 $b[x]$를 $[b][x]$ 대신에 $a+b[x]$를 $[a]+[b][x]=[a+bx]$ 대신에 쓸 것이다. 정리 5.2.3을 바꾸어 말할 수 있다.

정리 5.2.4

F는 체이고 $p(x)$는 $F[x]$에서 비상수다항식이라 하자. 그러면 $F[x]/(p(x))$는 F 자신을 포함하는 항등원이 있는 가환환이다.

예제 5.2.1 합동류 $F=\mathbb{Z}_2; p(x)=x^3+x+1$의 환 $F[x]/p(x)$에 대한 덧셈과 곱셈표 를 만들어라. $F[x]/p(x)$는 체인가?

[풀이]

+	$[0]$	$[1]$	$[x]$	$[x+1]$	$[x^2]$	$[x^2+1]$	$[x^2+x]$	$[x^2+x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$	$[x^2]$	$[x^2+1]$	$[x^2+x]$	$[x^2+x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$	$[x^2+1]$	$[x^2]$	$[x^2+x+1]$	$[x^2+x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$	$[x^2+x]$	$[x^2+x+1]$	$[x^2]$	$[x^2+1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$	$[x^2+x+1]$	$[x^2+x]$	$[x^2+1]$	$[x^2]$
$[x^2]$	$[x^2]$	$[x^2+1]$	$[x^2+x]$	$[x^2+x+1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x^2+1]$	$[x^2+1]$	$[x^2]$	$[x^2+x+1]$	$[x^2+x]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x^2+x]$	$[x^2+x]$	$[x^2+x+1]$	$[x^2]$	$[x^2+1]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x^2+x+1]$	$[x^2+x+1]$	$[x^2+x]$	$[x^2+1]$	$[x^2]$	$[x+1]$	$[x]$	$[1]$	$[0]$

·	$[0]$	$[1]$	$[x]$	$[x+1]$	$[x^2]$	$[x^2+1]$	$[x^2+x]$	$[x^2+x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$	$[x^2]$	$[x^2+1]$	$[x^2+x]$	$[x^2+x+1]$
$[x]$	$[0]$	$[x]$	$[x^2]$	$[x^2+x]$	$[x+1]$	$[1]$	$[x^2+x+1]$	$[x^2+1]$
$[x+1]$	$[0]$	$[x+1]$	$[x^2+x]$	$[x^2+1]$	$[x^2+x+1]$	$[x^2]$	$[1]$	$[x]$
$[x^2]$	$[0]$	$[x^2]$	$[x+1]$	$[x^2+x+1]$	$[x^2+x]$	$[x]$	$[x^2+1]$	$[1]$
$[x^2+1]$	$[0]$	$[x^2+1]$	$[1]$	$[x^2]$	$[x]$	$[x^2+x+1]$	$[x+1]$	$[x^2+x]$
$[x^2+x]$	$[0]$	$[x^2+x]$	$[x^2+x+1]$	$[1]$	$[x^2+1]$	$[x+1]$	$[x]$	$[x^2]$
$[x^2+x+1]$	$[0]$	$[x^2+x+1]$	$[x^2+1]$	$[x]$	$[1]$	$[x^2+x]$	$[x^2]$	$[x+1]$

더욱이 $p(x)\in\mathbb{Z}_2[x]$에서는 기약이다. 따라서 $\mathbb{Z}_2[x]/(p(x))$는 체이다. ■

유제 5.2.1 합동류

$$F=\mathbb{Z}_2;\ p(x)=x^2+1$$

$$F=\mathbb{Z}_2;\ p(x)=x^2+x+1$$

의 환 $F[x]/(p(x))$에 대한 덧셈과 곱셈표를 만들어라. $F[x]/(p(x))$는 체인가?

예제 5.2.2 $\mathbb{R}[x]/(x^2+1)$에서 덧셈과 곱셈에 대한 규칙을 결정하라.

[풀이] $\mathbb{R}[x]/(x^2+1)=\{[ax+b]:\ a,\ b\in R\}$이므로 임의로

$$[ax+b],\ [cx+d]\in\mathbb{R}[x]/(x^2+1)$$

을 택하자.

(i) $[ax+b]+[cx+d]=[(a+c)x+(b+d)]$

(ii) $[ax+b][cx+d]=[acx^2+(ad+bc)x+bd]$ (5.2.1)

$\mathbb{R}[x]/(x^2+1)$의 모든 원은 $rx+t$ $(r,\ t\in\mathbb{R})$이므로,

$acx^2+(ad+bc)x+bd$를 x^2+1로 나누어 그 나머지 $r(x)$를 구한다. 그러면

$$r(x)=(ad+bc)x+bd-ac.$$

그러므로 식 (5.2.1)에서

$$[ax+b][cx+d]=[(ad+bc)x+bd-ac]. \quad \blacksquare$$

유제 5.2.2 $\mathbb{Q}[x]/(x^2-3)$에서 덧셈과 곱셈에 대한 규칙을 결정하라.

5.3 $p(x)$가 기약일때 $F[x]/(p(x))$

p가 소수정수일 때, $\mathbb{Z}_p$는 체이다(물론 정역이다). 아마도 여러분은 $F[x]$에 대하여 비슷한 결과를 예측할 수 있다(정리 5.3.1). 그러나 $\mathbb{Z}$에서 일어났던 것의 비슷함보다 여기에서 훨씬 더 많은 일이 일어난다. 우리는 이미 $F[x]/(p(x))$가 체 F를 포함한다는 것을 알았다. 이렇게 우리는 $F[x]/(p(x))$ 역시 $p(x)$의 근을 포함한다는 것을 보여준다.

정리 5.3.1

F는 체이고 $p(x)$는 $F[x]$에서 비상수다항식이라 하자. 그러면 다음의 명제들은 논리적으로 같다.

(1) $p(x)$는 $F[x]$에서 기약이다.

(2) $F[x]/(p(x))$는 체이다.

(3) $F[x]/(p(x))$는 정역이다.

[증명] (1) $\Rightarrow$ (2) : $p(x)$가 $F[x]$에서 기약이라 가정하고 $F[x]/(p(x))$의 임의의 원 $[a(x)]\neq[0]$를 택하자. 그러면, 정리 5.1.5에 의하여

$$a(x)\not\equiv 0 \pmod{p(x)} \Leftrightarrow [a(x)]\neq 0$$

이므로 $F[x]$에서 $p(x)\nmid a(x)$이다.

그런데 $p(x)$가 $F[x]$에서 기약이므로 $a(x)$와 $p(x)$의 gcd는 1_F이거나 또는 $p(x)$의 모닉동반원이다. 하지만 $p(x)\nmid a(x)$이므로 $a(x)$는 $p(x)$의 임의의 동반원에 의하여 나누어질 수 없다. 그러므로 $p(x)\nmid a(x)$면, $a(x)$와 $p(x)$의 gcd는 1_F이어야만 한다. 정리 4.2.3에 의하여, $\exists$ 다항식 $u(x)$와 $v(x)$ $s.t.$ $1=p(x)u(x)+a(x)v(x)$.

그러면 $a(x)v(x)-1=p(x)(-u(x))$. 그래서

$a(x)v(x) \equiv 1 \pmod{p(x)}$. 정리 5.1.1에 의하여, $F[x]/(p(x))$에서 $[a(x)v(x)] = [1]$이고 $[a(x)]\,[v(x)] = [1]$이므로 $x = [v(x)]$는 $[a(x)]x = [1]$의 해이다.

(2) $\Rightarrow$ (3): $F[x]/(p(x))$가 체라 가정하자. 여기에서 정리 2.3.1을 결코 마음에 둘 필요는 없다. 이것은 따름정리 3.2.7의 직접적인 결과이다.

(3) $\Rightarrow$ (1) : $F[x]/p(x)$가 정역이라 가정하자. $p(x) = a(x)b(x)$이고 $a(x)b(x) \equiv 0 \pmod{p(x)}$이다. 정리5.1.5에 의하여 $[a(x)][b(x)] = 0$이다. $F[x]/p(x)$가 정역이므로 $[a(x)] = [0]$ 또는 $[b(x)] = 0$이다. $[a(x)] = 0$이라 가정하자.

$a(x) \equiv 0 \pmod{p(x)}$이므로 $p(x) | a(x)$이다. 적당한 다항식 $k(x) \in F[x]$가 존재하여

$$a(x) = k(x)p(x)$$

이다. $p(x) = a(x)b(x) = k(x)p(x)b(x)$이므로 $1 = k(x)b(x)$이다. 따라서 $b(x)$는 상수다항식이므로 $a(x)$는 $p(x)$의 동반원이다. ■

정리 5.3.1은 유한체를 만드는데 사용될 수 있다. p가 소수이고 $p(x)$가 차수 k인 $\mathbb{Z}_p[x]$에서 기약이면, 정리 5.3.1에 의하여, $\mathbb{Z}_p[x]/(p(x))$는 체이다. 보기 5.1.7은 이 체가 p^k개의

원을 가짐을 보여준다. 유한체는 9.6절에서 또 논의된다. 여기서 $\mathbb{Z}_p[x]$에서 모든 양의 차수의 기약 다항식이 있고 따라서 모든 가능한 소수거듭제곱 개수의 유한체가 존재함을 보여준다.

F는 체, $p(x)$는 $F[x]$에서 기약다항식이고 K는 합동류들의 체 $F[x]/(p(x))$를 나타낸다고 하자. 정리 5.2.4와 정리 5.3.1에 의하여, F는 체 K의 부분체이다. 우리는 역시 K를 F의 확대체(extension field)라 한다. $F[x]$에서 다항식들은 더 큰 체 K에서 계수들을 갖는다고 생각될 수 있고, 우리는 K에서 이와 같은 다항식들의 근에 관하여 질문할 수 있다. 특히,

우리가 출발한 다항식 $p(x)$의 근에 대하여 무엇을 말할 수 있는가? 비록 $p(x)$가 $F[x]$에서 기약일지라도, $p(x)$는 확대체 K에서 근을 가질 수 있다.

보기 5.3.1 다항식 $p(x) = x^2 + x + 1$은 $\mathbb{Z}_2$에서 근을 갖지 않는다. 그러면 따름정리 4.4.3-2에 의하여 $p(x)$는 $\mathbb{Z}_2[x]$에서 기약이다. 그래서 정리 5.3.1에 의하여, $K = \mathbb{Z}_2[x]/(x^2 + x + 1)$은 $\mathbb{Z}_2$의 확대체이다. ■

보기 5.2.3에 있는 K에 대한 표들을 사용하면,

$$[x^2]+[x]+1=[x+1]+[x]+1=[2x+1]+1=1+1=0.$$

우리가 다른 표시법을 사용하면 이 결과를 이해하는데 약간 더 쉬울 수 있다. $\alpha=[x]$라 하자. 그러면 위의 계산에 의하여, $\alpha^2+\alpha+1=0$, 즉 α는 $p(x)=x^2+x+1$의 K에서 근이다. 우리는 $x^2+x+1\equiv 0(\mathrm{mod}\ x^2+x+1)$임을 알기 때문에 α가 $p(x)$의 근임을 증명하기 위하여 여러분은 참으로 K에 대한 덧셈과 곱셈표를 여기에서 필요로 하지 않음에 주목하는 것이 중요하다. 왜냐하면, 우리는 $x^2+x+1\equiv 0(\mathrm{mod}\ x^2+x+1)$임을 알기 때문이다. 그러므로 $[x^2+x+1]=0\in K$이고 합동류 계산의 정의에 의하여,

$$\alpha^2+\alpha+1=[x]^2+[x]+1=[x^2+x+1]=0.$$

일반적인 경우에 대하여 우리는 다음의 결과를 갖는다.

정리 5.3.2

F는 체이고 $p(x)$는 $F[x]$에서 기약다항식이라 하자. 그러면 $F[x]/(p(x))$은 $p(x)$의 근을 포함하는 F의 확대체이다.

[증명] $K=F[x]/(p(x))$라 하자. 정리 5.2.4와 정리 5.3.1에 의하여, K는 F의 확대체다. $p(x)=a_nx^n+\cdots+a_1x+a_0\in F[x]$라 하자. 그러면 각 $a_i\in F$이다. 그래서 각 $a_i\in K$이다. $\alpha=[x]\in K$라 하자. 우리는 α가 $p(x)$의 근임을 보여줄 것이다. K에서 합동류

계산의 정의에 의하여,

$$\begin{aligned}a_nx^n+\cdots+a_1x+a_0&=a_n[x]^n+\cdots+a_1[x]+a_0\\&=[a_nx^n+\cdots+a_1x+a_0]\\&=[p(x)]=0_F.\quad [p(x)\equiv 0_F(\mathrm{mod}\ p(x))\text{이므로}]\end{aligned}$$

따라서 α는 $p(x)$의 근이다. ■

따름정리 5.3.2

F는 체이고 $f(x)$는 $F[x]$에서 비상수다항식이라 하자. 그러면 $f(x)$의 근을 포함하는 F의 확대체 K가 존재한다.

[증명] 정리 4.3.4에 의하여, $f(x)$는 $F[x]$에서 기약인수 $p(x)$를 갖는다. 정리 5.3.2에 의하여, $K=F[x]/(p(x))$는 $p(x)$의 근을 포함하는 F의 확대체이다. $p(x)$의 모든 근은 $f(x)$의 근이다. 따라서 K는 $f(x)$의 근을 포함한다. ■

제곱이 -1이 되는 수에 대하여 질문하는 대신에 우리는 "다항식 x^2+1이 근을 갖는 $\mathbb{R}$을 포함하는 체가 존재하는가?"라고 질문한다. x^2+1은 $\mathbb{R}[x]$에서 기약이므로, 정리 5.3.2에 의하여, 이 질문에 대한 답은 "그렇다"이다 :

$K=\mathbb{R}[x]/(x^2+1)$은 x^2+1의 근, $\alpha=[x]$를 포함하는 $\mathbb{R}$의 확대체이다. 체 K에서 α는 제곱이 -1이 되는 원이다. 그러나 이 체 K는 이 책에서 더 일찍이 소개된 복소수의 체와 어떻게 관련되는가?

보기 5.1.5에서 주목되었듯이, $K=\mathbb{R}[x]/(x^2+1)$의 모든 원은 $[ax+b](a, b\in\mathbb{R})$꼴로 유일하게 써 질 수 있다. 우리는 각 원 $r\in\mathbb{R}$을 K의 원 $[r]$과 일치 시키고 있으므로, K의 모든 원은

$$[a+bx]=[a]+[b][x]=a+b\alpha$$

꼴로 유일하게 써 질수 있음을 우리는 안다. K에서 덧셈은 규칙

$$(a+b\alpha)+(c+d\alpha)=[a+bx]+[c+dx]=[(a+bx)+(c+dx)]$$
$$=[(a+c)+(b+d)x]=[a+c]+[b+c][x]$$

로 주어진다. 그러므로

$$(a+b\alpha)+(c+d\alpha)=(a+c)+(b+d)\alpha.$$

K에서 곱은 다음의 규칙으로 주어진다:

$$(a+b\alpha)(c+d\alpha)=[a+bx][c+dx]=[(a+bx)(c+dx)]$$
$$=[ac+(ad+bc)x+bdx^2]$$
$$=ac+(ad+bc)\alpha+bd\alpha^2.$$

그런데 α는 x^2+1의 근이므로, $\alpha^2=-1$. 따라서 K에서 곱셈에 대한 규칙은 다음과 같이 된다:

$$(a+b\alpha)(c+d\alpha)=(ac-bd)+(ad+bc)\alpha.$$

기호 α를 기호 i로 바꾸게 되면, 이 두 덧셈과 곱셈의 규칙은 복소수를 더하고 곱하게 되는 보통의 규칙이 된다. 공식적인 표현을 빌면, 체 K는 $f(a+b\alpha)=a+bi$로 주어지는 동형사상 f와 함께, 체 $\mathbb{C}$와 동형이다.

5장 연습문제

1. $\mathbb{Q}[x]$에서 x^2-2를 법으로 무한히 많은 다른 합동류가 존재함을 보여라. 이 합동류들을 설명하라.

2. 환 $\mathbb{Q}[x]/(x^2)$은 체가 아님을 보여라.

3. 근들이 체 $\mathbb{Z}_2[x]/(x^2+x+1)$의 원들인 $\mathbb{Z}_2[x]$에서 4차 다항식을 구하라. 여기서 $\mathbb{Z}_2[x]/(x^2+x+1)$에 대한 덧셈과 곱셈표는 보기 5.2.3에 있다.
[도움말: 인수정리가 도움이 될 수 있다.]

4. $a\in F$일 때, 체 $F[x]/(x-a)$는 체인가? 자신의 주장을 설명하라.

5. (1) $\mathbb{Q}(\sqrt{3})=\{r+s\sqrt{3} : r, s\in\mathbb{Q}\}$는 $\mathbb{R}$의 부분체임을 증명하라.
(2) $\mathbb{Q}(\sqrt{3})$는 $\mathbb{Q}[x]/(x^2-3)$와 동형임을 보여라.

6. $f(x)\in F[x]$이 차수 n이라 하면 F의 확대체 E가 존재하여 서로 다를 필요가 없는 $c_i\in E$에 대하여

$$f(x)=c_0(x-c_1)(x-c_2)\cdots(x-c_n)$$

을 만족함을 보여라. 다른 말로 하면, E는 $f(x)$의 모든 근을 포함함을 증명하라.