Number Theoretic Algorithms

다항식과 다항식 환의 성질

May 29, 2019

1 다시 시작

더 멀리 나아가기 위해서는 기초부터 튼튼히 하는 것이 중요합니다.

우리가 아는 것으로부터 새로운 개념을 도입해나갑니다. 새로운 개념으로부터 필요해지게 되는 새로운 알고리즘과 전혀 새롭지 않은 논리 전개를 위해 계속해서 나아가 봅시다.

2 다항식

체 F 에 대해 마지막 항이 0이 아닌 유한 수열을 모은 집합과 $\{(0)\}$ 의 합집합을 $F[x]$ 로 씁니다. 즉,

$$F[x] = \{(a_0, \dots, a_n) : a_n \neq 0, n \in \mathbb{N}\} \cup \{(0)\}$$

입니다. $F[x]$ 의 원소 $f = (a_0, \dots, a_n)$ 을, 중학교 때부터 언제나 그래 왔듯,

$$f(x) = a_0 + a_1x + \dots + a_nx^n = \sum_{i=0}^n a_ix^i$$

으로 씁니다. $F[x]$ 의 원소 $f \neq 0$ 에 대해, n 을 f 의 차수라고 정의하고, $\deg f$ 로 씁니다. 계수, 차수 등의 표현은 잘 알고 있다고 생각합니다.

F 의 원소들로 구성된 무한수열 전체의 집합을 $\text{Seq}(F)$ 라 할 때, $\Psi : F[x] \rightarrow \text{Seq}(F)$ 를 $\Psi(a_0, \dots, a_n) = (a_0, \dots, a_n, 0, 0, \dots)$ 으로 주면, Ψ 는 injection이 됩니다. 이제 $\text{Seq}(F)$ 의 원소 $f = (a_0, a_1, \dots)$, $g = (b_0, b_1, \dots)$ 에 대해 $+$: $\text{Seq}(F) \times \text{Seq}(F) \rightarrow \text{Seq}(F)$ 와 $\cdot$: $\text{Seq}(F) \times \text{Seq}(F) \rightarrow \text{Seq}(F)$ 를 각각 다음과 같이 정의하면, $f + g$ 와 $f \cdot g$ 는 $\Psi(F[x])$ 의 원소임을 쉽게 확인할 수 있습니다.

$$f + g = (c_0, c_1, \dots) \text{ where } c_i = a_i + b_i$$

$$f \cdot g = (d_0, d_1, \dots) \text{ where } d_i = \sum_{j=0}^i a_j b_{i-j}$$

따라서, $F[x]$ 와 $\Psi(F[x]) \subseteq \text{Seq}(F)$ 를 **identify**하여 $+$ 와 $\cdot$ 을 정의합니다.¹ 우리는 계속해서

¹같은 것은 정말로 같다.

이 identification을 지켜 나갑니다.

다항식과 정수와의 가장 큰 차이점은 평가 여부에 달려 있습니다. 다항식 $(a_0, a_1, \dots) = f \in F[x]$ 에 대해 $\Phi : F[x] \rightarrow (F \rightarrow F)$ 를

$$\Phi(f)(c) = \sum_{i=0}^{\infty} a_i c^i$$

로 정의합니다. 이때 다항식 f 의 c 에서의 평가를 $\Phi(f)(c)$ 로 정의하고, $f(c)$ 로 씁니다.

우리는 다항식 f 를 g 로 나누면 몫으로 다항식 q 와 나머지로 다항식 r 이 나오고, $f(x) = g(x)q(x) + r(x)$ 을 만족함을 잘 알고 있습니다. 이는 증명 없이 사용합니다. 만일 $r = 0$ 이면 $f(x)$ 가 $g(x)$ 로 나누어떨어진다고 하고, $g(x)$ 는 $f(x)$ 를 나눈다고 합니다.

3 환

체 F 에 대해 $F[x]$ 는 더 이상 체가 아닙니다: $f(x) = x$ 와 곱해서 1이 되는 다항식 g 는 없습니다. 이러한 불만을 해소하기 위해 환을 정의합니다. 환 R 은 체의 공리에서 다음 두 가지를 제거한 대수적 구조입니다.

- 곱셈에 대한 교환 법칙. 즉, 더 이상 $a, b \in R$ 이 $ab \neq ba$ 일 수 있습니다.
- 각 $f \in R$ 에 대해, f^{-1} 의 존재. 즉, 더 이상 곱셈에 대한 역원이 없을 수 있습니다.

$F[x]$ 는 명백히 환입니다.² $F[x]$ 는 첫 번째 성질이 제거되지 않는데, 그러한 환은 가환환이라고 부릅니다. 이후의 논의에서는 다항식 환을 주로 다룰 것이며, 가환환이 아닌 환을 다루는 일은 없을 것입니다.

만일 두 환 R 과 R' 사이에, 임의의 $a, b \in R$ 에 대해 다음

$$\begin{aligned} \varphi(a) + \varphi(b) &= \varphi(a + b) \\ \varphi(a)\varphi(b) &= \varphi(ab) \end{aligned}$$

및 $\varphi(1) = 1$ 을 만족하는 $\varphi : R \rightarrow R'$ 이 있으면, φ 를 (환) homomorphism이라고 부릅니다. 이외에 monomorphism, epimorphism, isomorphism, endomorphism 등의 단어도 모두 사용합니다.

다항식 환 $F[x]$ 에서의 덧셈과 곱셈의 경우, 우리가 알고 있는 덧셈 및 곱셈이 $\text{Seq}(F)$ 와 잘 조화되도록, 즉 Ψ 가 homomorphism을 이루도록 $\text{Seq}(F)$ 에 덧셈 및 곱셈을 정의한 것입니다.³ $F \rightarrow F$ 에 함수 덧셈 및 곱셈을 componentwise 정의하면, 사실 Φ 도 homomorphism임을 보일 수 있습니다.⁴

²이제 곱셈에 대한 역원이 제거되었으므로, 더 이상 보일 것이 없습니다.

³ $\text{Seq}(F)$ 에 정의된 곱셈은 sequence convolution이라고 합니다.

⁴Theorem 1에서 이 사실을 사용하므로, 반드시 증명해 보시기 바랍니다. 이런 걸 증명하고 있다 보면 같은 게 같은 건가 싶은 생각이 드는 건 사실입니다...

4 $\mathbb{Z}_p$ 위에서의 다항식 환

체 $\mathbb{Z}_p$ 위에서 정의된 다항식 환 $\mathbb{Z}_p[x]$ 에는 정수와 비슷한 많은 좋은 성질이 있습니다.

우선, 임의의 체 F 에서 성립하는 다음 정리를 생각합니다.

Theorem 1. 체 F 와 다항식 $f \in F[x]$ 에 대해 $f(c) = 0$ 이면, f 는 $(x - c)$ 로 나누어떨어진다.

Proof. $f(x) = (x - c)q(x) + r(x)$ 로 쓰면, $\deg(x - c) = 1$ 이기 때문에 $\deg r = 0$ 이거나 $r = 0$ 이어야 합니다. 어느 쪽이든 $r = c_0$ 로 쓸 수 있습니다. 양 변을 c 에서 평가하면,

$$0 = \Phi(f)(c) = (c - c)\Phi(q)(c) + \Phi(r)(c) = \Phi(r)(c) = c_0$$

이므로, $r = c_0 = 0$ 입니다. □

따라서, 유한 체의 경우 1주차 보강 자료에서 증명해 두었던 지식을 활용하여 재미있는 얘기를 해 볼 수 있습니다.

Theorem 2. 유한 체 F 에 대해 $|F| = n$ 이라 두면, 다음이 성립한다.

$$x^n - x = \prod_{x_0 \in F} (x - x_0)$$

Proof. Theorem 1에 의해, 다음을 만족하는 다항식 $q(x)$ 가 존재합니다.

$$x^n - x = q(x) \prod_{x_0 \in F} (x - x_0)$$

degree를 이용해 $\deg q = 0$ 혹은 $q = 0$ 을 얻으며, 양쪽 수열의 n 차 항 계수를 비교해 $q = 1$ 을 얻습니다. 이로부터 원하는 등식이 얻어집니다. □

Theorem 2에서 양 변의 계수를 비교하여 모든 $k = 1, \dots, n - 2$ 에 대해

$$\sum_{S \subseteq F, |S|=k} \left(\prod_{s \in S} s \right) = 0$$

와 $k = n - 1$ 일 때 $\prod_{x \in F \setminus \{0\}} x = (-1)^n$, 혹은 더욱 구체적으로 $F = \mathbb{Z}_p$ 일 때 $(p - 1)! = -1$ 을 얻습니다. (Wilson)

이제, 다음을 얻습니다.

Corollary 3. 유한 체 F 위에서 정의된 임의의 다항식 $f, g \in F[x]$ 에 대해,

$$\prod_{x_0 \in F} (f(x) \pm x_0 g(x)) = (f(x))^{|F|} - f(x) (g(x))^{|F|-1}$$

이 성립한다.

다음은 유한 체 전반이 아닌 $\mathbb{Z}_p$ 의 성질입니다. 증명은 p 가 소수임에서 곧바로 나옵니다.

Theorem 4 (Freshman's dream comes true). 다항식 $f_1, \dots, f_k \in \mathbb{Z}_p[x]$ 에 대해 다음이 성립한다.

$$\left(\sum_{i=1}^k f_i \right)^p = \sum_{i=1}^k f_i^p$$

Corollary 3과 **Theorem 4**의 사실들은 후반부에서 쓰이게 됩니다. 지금 이런 예제들을 통해 우리가 거침없이 계산을 진행해 나갈 수 있었던 것은 우리가 체 위에서의 다항식 환이라는, 상대적으로 **행복한** 세계에서 논의를 진행하고 있기 때문입니다.

5 $\mathbb{Z}_p[x]$ 에서의 최대공약수

체 F 위의 다항식 환 $F[x]$ 에서, f 와 g 를 통해 생성된 $F[x]$ 의 부분환⁵

$$R = \{uf + vg : u, v \in F[x]\}$$

의 0 아닌 원소 중 차수가 가장 작은 것을 f 와 g 의 최대공약수라고 하고, $\gcd(f, g)$ 로 씁니다.⁶ 이 최대공약수가 정말 f 와 g 를 나누는 다항식 중 최대임을 보입니다.

$h := \gcd(f, g)$ 로 놓습니다.

- (나눈다) $h = uf + vg$ 가 되게 하는 $u, v \in F[x]$ 이 존재합니다. $f = hq + r$ 이 되는 다항식 q 와 $r \neq 0$ 이라면 $\deg r < \deg h$ 인 r 이 존재합니다. 이제

$$r = f - hq = f - (uf + vg)q = (1 - uq)f + (-vq)g \in R$$

이고, $\deg h$ 의 최소성에 모순되지 않으려면 $r = 0$ 일 수밖에 없습니다.⁷

- (최대이다) h' 이 f 와 g 를 모두 나눈다고 합시다. $f = ph', g = qh'$ 로 놓으면,

$$h = uf + vg = uph' + vqh' = (up + vq)h'$$

이므로, h' 은 h 를 나눕니다. 즉, $\deg h' \leq \deg h$ 입니다.

이로써 나눗셈을 알 때의 정의와 나눗셈을 모르고서 정의한 것이 일치한다고 생각할 수 있습니다.

위에서 다항식을 다룰 때 정수의 많은 성질 – 덧셈, 곱셈, 순서 등 – 을 모두 사용했습니다. 우리가 맨 처음 했던 가정에 이 모든 내용이 숨어 있다고 생각할 수 있습니다.

⁵1이 없을 수도 있는데, 그냥 환이라고 부릅니다. 책에 따라서는 1이 있는 환을 단위 있는 환이라고 부르기도 하고 1이 있는 환을 환, 없는 환을 rng이라고 부르기도 합니다.

⁶정수의 경우에도 이렇게 정의했으면, 논의할 내용이 조금 많아졌을 것입니다. 이 방식의 정의는 다항식 나눗셈을 몰라도 할 수 있습니다.

⁷이 논증을 제대로 이해하면 학부 대수학의 반을 이해한 것이나 다름없다고 합니다.

6 문제

1. $+$ 와 $\cdot$ 은 정말 잘 정의되었을까요?

(a) 무한 수열 f 와 g 에 대해, $f + g$ 와 $f \cdot g$ 는 모두 다음 성질을 만족함을 보이세요.

$n > N$ 일 때마다 $a_n = 0$ 인 자연수 N 이 존재한다.

따라서 $f + g$ 와 $f \cdot g$ 는 $\Psi(F[x])$ 의 원소라고 할 수 있습니다.

(b) $\deg(f + g) \leq \deg f$ 를 증명하세요. 덧셈이 교환법칙을 만족하므로, $\deg(f + g) \leq \deg g$ 역시 성립합니다.

(c) $\deg(f \cdot g) = \deg f + \deg g$ 를 증명하세요.

2. 다항식의 나눗셈은 정수의 순서 구조를 본질적으로 담고 있기 때문에, 정수의 순서 구조를 알고 있다고 생각하면 이로부터 다항식의 나눗셈을 유도해낼 수 있습니다.

Claim. 다항식 f 와 g 에 대해, $f = gq + r$ 인 [$r \neq 0$ 이면 $\deg r < \deg g$]인 다항식 q 와 r 이 (유일하게) 존재합니다.

(a) $\deg f < \deg g$ 일 때, **Claim**의 존재성을 증명하세요.

(b) $\deg f$ 에 대한 수학적 귀납법으로, $\deg f \geq \deg g$ 일 때 **Claim**의 존재성을 증명하세요.

(c) 차수의 크기 비교를 통해 **Claim**의 유일성을 증명하세요.

3. (키파컵 F번 풀이) 분자와 분모의 약수가 모두 L 이하인 유리수들의 집합을 $\mathbb{Q}_L^\times$ 이라 하고, 연산 구조에는 평범한 유리수 구조를 줍니다. $p > L^2$ 인 소수 p 에 대해, $\varphi : \mathbb{Q}_L^\times \rightarrow \mathbb{Z}_p$ 를 $\varphi(a/b) = ab^{-1} \pmod p$ 로 정의합니다.

(a) φ 가 잘 정의되어 있음을 보이세요.

(b) φ 가 homomorphism임을 보이고, 특히 φ 의 정의역을 기약분수의 분자 및 분모가 모두 L 이하인 유리수로 제한할 경우 φ 는 monomorphism임을 보이세요.

(c) φ 가 homomorphism이기 때문에, v 가 주어졌을 때 $\varphi(a/b) = v$ 인 a, b 를 찾아내는 시간 $\mathcal{O}(\sqrt{L})$ 의 방법이 있습니다. 이를 찾아내어, 백준 16645번 문제를 푸세요.

4. 다항식 환은 환 위에서 정의할 수 있습니다. 환은 얼마나 안 좋은 공간일까요?

(a) $\mathbb{Z}$ 에 $\sqrt{5}i$ 를 추가해서 확장한 환을 생각합니다. 이 환은 $\mathbb{Z}[\sqrt{-5}]$ 와 같이 씁니다. 즉,

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$$

입니다. 이때, $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ 임을 확인하세요.

(b) $\mathbb{Z}_{10001}$ 에서 $x^2 - 1 = (x - 2191)(x - 7810)$ 임을 계산을 통해 확인하세요. 또 평범하게, $x^2 - 1 = (x - 1)(x - 10000)$ 임을 확인하세요.

즉, 1주차에서 최대공약수를 설명하기 위해 정수가 **유일 인수 분해 정역**이라는 사실을 아무 생각 없이 썼다는 것을 알 수 있습니다. 정수는 대단히 좋은 공간이고, 이를 확장한 것은 **아이디얼**이라고 부릅니다.⁸

5. $F = \mathbb{Z}_p$ 에서, 다음을 확인하세요.

(a)

$$\prod_{a,b \in F} (x^2 + ax + b) = (x^p - x)^p (x^{p^2} - x).$$

(b)

$$\prod_{a,b,c \in F} (x^3 + ax^2 + bx + c) = (x^p - x)^{p^2} (x^{p^2} - x)^p (x^{p^3} - x).$$

6. 1주차 자료의 최대공약수 부분을 자세히 읽고, 최대공약수를 구하는 유클리드 알고리즘은 나눗셈**에만** 의존함을 납득하세요. 따라서 다항식의 최대공약수를 구할 때도 마찬가지로 방법을 사용할 수 있습니다.

7. 다항식의 해를 구할 때나 약수를 구할 때, 한 약수가 반복되지 않도록 차수를 낮추는 것은 대단히 중요합니다. 예를 들어, Newton's method를 시행할 때 다항식의 한 약수가 반복된다면, 그 주변에서 값이 거의 변하지 않아 해 근처에 도달한 경우 크게 요동칠 것입니다. 차수를 낮추기 위해, $(a_0, a_1, \dots) = f \in F[x]$ 에 대해 연산자 $D : \text{Seq}(F) \rightarrow \text{Seq}(F)$ 를

$$Df = (b_0, b_1, \dots) \text{ where } b_i = (i+1)a_{i+1}$$

가 되도록 정의합니다.

(a) $D : F[x] \rightarrow F[x]$ 가 well-defined임을 보이고, 만일 $Df \neq 0$ 이라면 $\deg(Df) \leq \deg f$ 임을 보이세요.

(b) D 는 덧셈을 보존하지만 homomorphism은 아닙니다. 하지만, 곱셈에 대해 다음과 같은 “그나마 나은” 성질이 성립함을 보이세요.

$$D(fg) = (Df)g + f(Dg)$$

(c) (b)를 바탕으로, $D(f^n) = n(Df)f^{n-1}$ 임을 보이세요.

(d) $g, h \in F[x]$ 에 대해 (g 와 h 는 서로소이고) 다항식 $f = g^c h$ 로 정의되었다면, $Df = g^{c-1} h'$ 을 만족하는 [$h' \neq 0$ 이라면 $\gcd(g, h') = 1$ 인] $h' \in F[x]$ 가 존재함을 보이세요. 따라서, 만일 c 가 F 의 characteristic의 배수가 아니라면, $f / \gcd(f, Df)$ 는 g 의 차수가 1입니다.

⁸아이디얼은 원래 정수론에서 유래했다고 합니다. “정수는 이렇게 힘든데, 이상적이고 행복한 공간이 있으면 어떨까?”라는 물음에서 출발한 것이 아이디얼입니다. 그 유래답게, 주 아이디얼 정역은 모두 유일 인수 분해 정역입니다.