한국수학사학회지 제18권 제2호(2005년 5월), 117-126

유한체상의 치환다항식에 관한 역사적 고찰*

한양대학교 수학과 박홍구
hpark@hanyang.ac.kr

본 논문에서는 유한체의 치환다항식 이론의 기본 개념 및 역사적 배경을 주요 치환다항식들을 중심으로 분석해본다. 아울러 유한체의 원소로 이루어진 순환들의 다항식 표현법을 구현한다.

주제어 : 유한체, 치환다항식 .

0. 서론

소수 p와 양의 정수 n에 대해, p^n개의 원소로 이루어진 유한체(finite field 혹은 Galois field) $GF(p^n)$에서 자기 자신으로 보내는 치환(permutation)을 다항식 함수 $f(x)$로 표현할 수 있을 때, $f(x)$를 $GF(p^n)$의 치환다항식(permutation polynomial)이라 말한다. 오늘날 치환다항식 이론은 많은 학문 분야에 폭넓게 응용되고 있으며, 특히 데이터 전송을 안전하게 전송할 수 있는 암호체계를 구성하는 데도 매우 중요한 역할을 하고 있다.

치환다항식을 처음 연구한 수학자는 에르미트(Hermite)로 1863년 그의 논문[11]을 통해 유한소수체(finite prime field) $GF(p)$에서의 일반적인 치환다항식에 관한 결과를 발표하였다. 이후 임의의 유한체에서 치환다항식의 구체적인 표현 방법 및 성질들이 1897년 딕슨(Dickson)[10]에 의해 본격적으로 연구되었다. 이후 수많은 수학자들에 의해 치환다항식에 관한 연구가 활발히 진행되었지만 현재까지 알려진 유한체의 치환다항식들은 그리 많지가 않은 실정이다. 가장 큰 문제는 유한체의 원소를 계수로 갖는 다항식의 치환성(permutation property)을 판단할 수 있는 유용한 알고리즘을 찾기가 매우 어렵다는 데 있다. 이와 아울러 유한체의 원소로 표현된 치환을 유한체의 원소인 영이 아닌 계수와 유한 차수로 이루어진 치환다항식으로 표현할 수 있는 알고리즘 역시 전무하다. 이와 더불어 일반적으로 주어진 치환다항식의 순환구조(cycle structure)를 밝히는 유용한 방법 또한 알려져 있지 않다. 이러한 문제들이 치환다항

* 본 논문은 2002학년도 한양대학교 교내연구비 지원에 의한 결과물임.

식 이론에 있어 아직까지 풀어야할 난제로 남아있다.

본 논문에서는 우선 유한체의 치환다항식의 기본 개념을 다루며, 시대별로 주요 논문들에 나타난 치환다항식들을 분석해본다. 이를 바탕으로 유한체상에서 치환의 기본 단위인 순환(cycle)을 치환다항식으로 표현할 수 있는 방법을 구현해 보기로 한다.

1. 치환다항식의 기본 개념

치환다항식을 유도해 내기 위해선 먼저 주어진 유한체에서 자기 자신으로 가는 함수 f를 다항식 함수로 유일하게 표현할 수 있어야 한다. 라그랑주의 보간법 공식(Lagrange interpolation formula)을 적용하면 위의 함수는 $q=p^n$일 때, x^q-x를 법으로 다음 다항식에 의해 유일하게 표현됨을 보일 수 있다[12, p. 348].

$$f(x)=\sum_{i=0}^{n} a_i x^i \qquad (n<q,\ a_i \in GF(q))$$

따라서 위의 함수가 전단사함수일 경우 차수가 q보다 작은 유일한 치환다항식 $f(x)$가 존재하게 되며, 이와 같이 표현할 수 있는 치환다항식들의 집합은 함수결합과 x^q-x를 법으로 하는 연산에 관해 군을 이룬다. 이 군은 $GF(p^n)$에서의 대칭군과 동형이 되고 위수(order)는 $q!$이 된다. 다음 문제는 당연히 위의 다항식 $f(x)$가 치환다항식임을 밝힐 수 있는 필요충분조건 혹은 유용한 알고리즘을 찾는 것이다. 우선 위 다항식 $f(x)$가 치환다항식이라 가정할 경우 만일 q의 값이 비교적 작다면 주어진 유한체의 모든 원소 c에 대해 q개의 $f(c)$의 값들이 다른지를 비교하면 된다. 허나 차수가 n인 다항식의 연산 회수는 $O(qn)GF(q)$이므로 q의 값이 크면 클수록 계산은 더 이상 불가능하게 된다.

현재 가장 많이 알려진, 경우에 따라서 한 가지 매우 유용한 판단 방법이 에르미트[11]와 딕슨[10]에 의해 밝혀졌다. 에르미트는 $q=p$, 딕슨은 $q=p^n$에 대해 다음과 같은 결과를 유도해 냈다. 즉, $f(x)$가 $GF(q)$의 치환다항식이기 위한 필요충분조건은,

(ㄱ) $f(x)=0$을 만족시키는 $GF(q)$의 원소는 오로지 하나만 존재하며,

(ㄴ) $1\le t\le q-2,\ t\not\equiv 0 \pmod p$를 만족시키는 모든 t의 값에 대해 x^q-x를 법으로 $[f(x)]^t$를 정제한 후 나타난 다항식의 차수는 $q-1$보다 항시 작아야 한다.

이 방법 또한 일정한 다항식에만 유용할 뿐 일반적인 경우 조건 (ㄴ)을 계산하는 데에는 엄청난 복잡성이 있는 관계로 치환성을 판단하기가 불가능해진다. 이 이외 $f(x)$의 계수들을 이용한 방법들([6], [14], [15], [18])이 알려져 있으나 위와 마찬가지로 일반적인 경우에 적용하기엔 계산상 많은 어려움이 있다. 결국 이 분야에 있어 가장 핵심이 되는 쟁점은 새로운 형태의 치환다항식들을 찾아내는 데에 있으며 이를 위해선 조건 (ㄱ)과 (ㄴ)에서 나타난 다항식 계산의 복잡성을 최대한으로 줄일 수 있는 보다 효율적인 알고리즘 및 이론을 유도해내야 한다.

2. 치환다항식의 역사적 배경

일반적으로 주어진 유한체 $GF(q)$의 치환다항식에 관한 본격적인 연구결과는 1897년 딕슨에 의해 <Annals of Mathematics>에 발표되었으며, 그의 박사학위논문이기도 한 이 논문[10]에서 주목할 만한 많은 새로운 치환다항식이 발견되었다. 이 논문을 통해 딕슨은 유한체에서 차수가 5보다 작거나 같은 모든 정규치환다항식(normalized permutation polynomial)을 정확하게 찾았다. 유한체의 정규치환다항식이라 함은 만일 다항식 $f(x)$가 $GF(q)$의 치환다항식이고 $a\neq 0, b, c\in GF(q)$이면 $g(x)=af(x+b)+c$ 역시 치환다항식이 된다. 이때 $g(x)$의 최고차수의 계수가 1, x^{n-1}의 계수가 0, 상수항이 0, 그리고 p가 n의 약수가 아닐 때 $g(x)$를 정규치환다항식이라 말한다. 차수 5까지 차수별로 모든 $GF(q)$의 정규치환다항식들을 정리해보면 다음과 같다.

(1) 차수 1

x: 모든 q에 대해

(2) 차수 2

x^2: $q\equiv 0 \pmod 2$

(3) 차수 3

x^3: $q\not\equiv 1 \pmod 3$, x^3-ax: a가 제곱이 아닐 때

(4) 차수 4

$x^4\pm 3x$: $q=7$, x^4+ax^2+bx: 0이 유일한 해이고 $q\equiv 0 \pmod 2$

(5) 차수 5

x^5: $q\not\equiv 1 \pmod 5$, x^5-ax: a가 네제곱이 아니고 $q\equiv 0 \pmod 5$

x^5+ax: $a^2=2$이고 $q=9$, $x^5\pm 2x^2$: $q=7$

$x^5+ax^3\pm x^2+3a^2x$: a는 제곱이 아니고 $q=7$

$x^5+ax^3+5^{-1}a^2x$: 임의의 a 그리고 $q\equiv\pm 2 \pmod 5$

$x^5+ax^3+3a^2x$: a가 제곱이 아니고 $q=13$

$x^5-2ax^3+a^2x$: a가 제곱이 아니고 $q\equiv 0 \pmod 5$

이외 동일 논문에서 딕슨은 q가 홀수일 때 차수가 6인 다항식을 특성화하였으며 차수가 7과 8인 경우에 대한 부분적인 결과도 발표하였다. 또한 $GF(q)$의 치환다항식의 차수는 $q-1$보다 작음을 보였다. 이후 많은 수학자들에 의해 차수가 5보다 큰 다항식의 치환성이 연구되어 왔으며, 특히 항의 수가 두 개인 이항다항식의 치환성 연구에 많은 영향을 주었다([8], [9]).

잘 알려진 간단한 형태의 치환다항식은, $a, b\in GF(q)$이고 a가 0이 아닐 때, 다음과 같다.

$$x^k,\ ax+b$$

순환군 내의 부분순환군의 위수 계산 방법을 적용할 경우 x^k가 치환다항식일 필요충분조건은 $\gcd(k, q-1)=1$이 됨을 쉽게 보일 수 있다. $ax+b$는 위 조건 하에 치환다항식이 되며 a가 1이고 b가 0이 아닌 경우 함수결합의 기본 개념을 적용하면 p^{n-1}개의 길이가 p인 서로 다른 순환들(disjoint cycles)의 곱으로 구성되어 있다. 만일 $a\neq 1$일 경우 $ax+b$의 순환구조 역시 유사한 방법을 통해 어렵지 않게 구할 수 있다. 즉, 곱에 관해 a의 위수가 r일 때, $(q-1)/r$개의 길이가 r인 서로 다른 순환들의 곱과 원소 $b/(1-a)$로 이루어진 길이 1인 순환과의 곱으로 구성되어 있음을 알 수 있다.

현재에도 연구가 활발히 진행되고 있으며 1897년 딕슨의 논문[10]에 소개된 유한체의 다항식으로 1968년 뇌바우엘(Noebauer)[17]에 의해 치환성의 필요충분조건이 완성되었으며 후에 딕슨다항식으로 명명된 다음 다항식을 들 수 있다.

$$g_k(x, a)=\sum_{j=0}^{[k/2]}\frac{k}{k-j}\binom{k-j}{j}(-a)^j x^{k-2j} \qquad (a\in GF(q))$$

딕슨은 위 다항식의 치환성에 대한 부분적인 조건만을 구하는 데 그쳤으며, 1968년 뇌바우엘은 위에 언급된 x^k의 치환성 조건과 왜링(Waring)의 공식을 $g_k(x, a)$에 적

용한 결과 치환다항식이 되기 위한 필요충분조건은 $\gcd(k, q^2-1)=1$이 됨을 유도해냈다. 특히 이 다항식은 쉬(Shur)[20]의 추론과 밀접한 관계가 있음이 그 후 많은 수학자들에 의해 밝혀졌다.

p-다항식으로 불리는 특별한 형태의 다항식으로 다음과 같은 것이 있다.

$$L(x)=\sum_{j=0}^{n-1} a_j x^{p^j} \qquad (a_j \in GF(q))$$

이는 주어진 유한체에서 일차변환의 성질을 지니고 있다. 베티(Betti)[1]에 의해 1852년 처음으로 소개가 되었고, 이에 대한 치환성은 그 후 딕슨[10]에 의해 규명되었다. 즉, $L(x)$가 치환다항식이기 위한 필요충분조건은 $\det(a_i^{p^j})\neq 0,\ 0\leq i, j\leq n-1$이다. 모든 가능한 치환다항식 $L(x)$들의 집합은 군이 됨을 알 수 있으며, 베티·매튜군(Betti-Mathieu group)으로 불린다. 또한 [10]에서 딕슨은 베티·매튜군의 다항식들과 일반선형군(general linear group) $GL(n, GF(q))$의 원소와 1:1 대응 관계가 있음을 보였다. 1930년 보테마(Bottema)[2]는 위의 두 군이 동형이 된다는 사실을 처음으로 증명하였다.

또 다른 형태의 치환다항식으로는 다음과 같은 다항식을 들 수 있다.

$$x^r(f(x^s))^{(q-1)/s}$$

다음 두 조건들을 만족시킬 경우 위 다항식이 치환다항식이 됨을 알 수 있다.

(1) $r>1$, $\gcd(r, q-1)=1$이고 양의 정수 k가 $q-1$의 약수

(2) 임의로 주어진 $GF(q)$의 다항식 $f(x)$에 대해 $f(x^s)$가 0이 아닌 근을 갖지 않음

이에 대한 증명은 $q=p$일 때 로저스(Rogers)[19] 그리고 일반적인 경우 딕슨[10]에 의해 이루어졌다.

마지막으로 잘 알려진 주요 치환다항식으론 다음과 같은 두 가지 이항다항식을 들 수 있다.

$$f(x)=x^{(q+m-1)/m}+ax, \quad g(x)=x^r(x^d-a)^{(q-1)/d}$$

이 경우 $f(x)$는 m이 $q-1$의 약수일 때, 그리고 $g(x)$는 d가 $q-1$의 약수일 때

각각 치환다항식이 됨을 알 수 있다([4], [5], [7], [12], [16]).

이 이외 관련된 많은 치환다항식들이 있지만 이상이 1897년 딕슨 이후 발견된 새로운 형태의 주요 치환다항식들이다. 하지만 $p^n!$개의 치환다항식 중에 위에 기술된 치환다항식의 수가 극히 적음을 알 수 있다.

3. 유한체에서 순환의 치환다항식

유한체의 다항식에 관한 치환성을 판정하려면 보다 효율적 알고리즘의 개발이 필요함을 1절과 2절을 통해 알 수 있었다. 이 절에서는 다른 각도에서 이러한 치환성을 분석해 보려한다. 유한체의 원소로 구성된 치환들은 각 각 유한 개의 서로 다른 순환들의 곱(함수결합)으로 유일하게 표현할 수 있으며 또한 길이가 2인 유한 개의 순환들(즉, transpositions)의 곱으로 표현이 가능하다. 따라서 우선 순환들의 다항식 표현 방법을 구현함으로서 치환성을 판정할 수 있는 새로운 형태의 방법을 살펴보기로 하자.

한 가지 예로 $a\neq 0$, $a\in GF(q)$일 때 간단한 형태의 순환 $(0, a)$를 차수가 $q-1$보다 작은 유한체의 치환다항식으로 유일하게 표현할 수 있음을 2절을 통해 알 수 있었다. 문제는 어떤 방법으로 위의 $(0, a)$ 함수를 다항식으로 변환시키는가에 있다. 1953년 칼리츠(Carlitz)[4]는 최초로 $(0, a)$가 다음과 같은 치환다항식 $g(x)$로 표현됨을 유도 과정 없이 간략히 기술하였다.

(1) $$g(x)=-a^2\left(\left((x-a)^{q-2}+\frac{1}{a}\right)^{q-2}-a\right)^{q-2}$$

위의 다항식은 $\alpha, \beta\in GF(q)$, $\alpha\neq 0$일 때 $\alpha x+\beta$, x^{q-2} 두 치환다항식의 함수결합으로 표현되어 있으며, 또한 $GF(q)$의 모든 치환다항식이 이 두 치환다항식에 의해 생성이 가능함을 알 수 있다. 그렇다면 $g(x) \bmod (x^q-x)=?$ 따라서 임의의 다항식에 대한 치환성을 판단할 수 있는 알고리즘을 찾는 일이 결코 쉽지 않음을 알 수 있다.

다음으로 유한체의 원소들로 만들어진 순환의 치환다항식을 찾아보자. 임의의 원소 $c\in GF(q)$에 대해 $c^q=c$의 성질을 이용하면 다음 다항식의 값은 $x=c$일 때 1이 되며, $x\neq c$일 경우 0이 됨을 알 수 있다.

(2) $$f(x)=1-\sum_{i=0}^{q-1} c^{q-1-i}x^i$$

이러한 사실로부터 어렵지 않게 다음과 같은 결과를 얻을 수 있다. 즉, $0 \le i \le q-1$을 만족하는 모든 i에 대해 $GF(q)$의 원소 c_i들이 서로 다른 원소가 될 필요충분조건은 원소 c_i들이 다음을 만족시키는 경우이다.

(3) $$\sum_{i=0}^{q-1} c_i^k = \begin{cases} 0, & \text{if } k=0,1,\cdots,q-2 \\ -1, & \text{if } k=q-1 \end{cases}$$

$GF(q)$의 원소로 만들어진 순환 $\pi = (c_1 \ldots\ldots c_t)$에 대해 $q-1$보다 작은 차수를 갖는 치환다항식 $f(x)$가 유일하게 존재하므로, $f(x) = \sum_{i=0}^{q-2} a_i x^i$라 가정할 수 있으며, 또한 각각의 계수 a_i는 다음과 같이 된다[10, p. 69-70].

$$a_i = - \sum_{c \in GF(q)} \pi(c)\, c^{q-1-i}$$

따라서 $A = \{ c_0, c_1, \ldots, c_t \}$이고 $GF(q)$ 내에서 A를 제외한 원소를 B라 할 때, 다음과 같이 된다.

$$a_i = - \sum_{c \in A} \pi(c)\, c^{q-1-i} = - \sum_{c \in B} \pi(c)\, c^{q-1-i}$$

$$= \delta_i - \sum_{c \in GF(q)} c^{q-i}$$

여기서 $\delta_i = \sum_{j=1}^{t} (c_j - \pi(c_j)) c_j^{q-1-i}$이다. (3)에 의해 $a_1 = 1 + \delta_1$이 되고, $i \neq 1$일 때 $a_i = \delta_i$이다. 그러므로 순환 π는 다음 다항식으로 표현된다.

(4) $$f(x) = x + \sum_{i=0}^{q-2} \delta_i x^i$$

그리고 (2)에 의해 위의 다항식이 치환이 됨을 어렵지 않게 보일 수 있다. 또한 유사한 방법으로 $\sigma_i = \sum_{j=1}^{t} (\pi(c_j) - c_j) c_j^{q-1-i}$일 때 다음을 구할 수 있다.

$$f^{-1}(x)=x+\sum_{i=0}^{q-2}\sigma_i x^i$$

예를 들어 $\pi=(0\ a)$일 때 (4)에 의해 $\delta_i=(a-0)a^{q-1-i}=a^{q-i}$이므로 π의 치환다항식은 다음과 같이 된다.

$$f(x)=x+\sum_{i=0}^{q-2}a^{q-i}x^i$$

그리고 (1)에 의해 다음이 성립함을 유도해 낼 수 있다.

$$-a^2\left(\left((x-a)^{q-2}+\frac{1}{a}\right)^{q-2}-a\right)^{q-2}\equiv x+\sum_{i=0}^{q-2}a^{q-i}x^i\pmod{x^q-x}$$

4. 결론

이제까지 치환다항식의 기본 개념과 역사적 배경 그리고 잘 알려진 주요 치환다항식의 몇 가지 성질을 적용하여 유한체에서 주어진 순환의 치환다항식에 대해 살펴보았다. 이러한 과정의 주요 목적은 임의 유한체에서 새로운 형태의 치환다항식들의 계(class)를 찾기 위한 한 가지 방법이었다. 보다 일반적으로 $GF(q)$에서 임의의 치환 θ에 대한 치환다항식은 3절에서 적용한 방법을 $\theta=\pi_1\cdot\cdot\cdot\pi_m$의 각각 서로 다른 순환 $\pi_j,\ 1\le j\le m$에 반복 적용할 경우 θ는 다음과 같은 치환 성질을 지니는 다항식으로 표현할 수 있음을 보일 수 있다. 즉, (4)에 의해 표현된 π_j의 치환다항식을 $f_j(x)$라 할 때, 다음과 같은 흥미로운 결과를 얻을 수 있다.

(5) $$f(x)=(1-m)x+\sum_{j=1}^{m}f_j(x)$$

한 가지 남아있는 연구과제는 (4)와 (5)에서 주어진 다항식들에서 0이 되는 항들을 어떻게 특성화하느냐에 있다. 즉, 유한체의 원소로 이루어진 다항식의 해를 구체적으로 찾아야하는 매우 어려운 문제인 것이다.

참고 문헌

1. Betti, E., "Sulla risoluzione delle equazioni algebriche," *Ann. Sci. Mat. Fis.* 3 (1852), 49-115.
2. Bottema, O., "On the Betti-Mathieu Group (Dutch)," *Nieuw Arch. Wisk.*(2) 16, no. 4(1930), 46-50.
3. Carlitz, L., "Permutations in a Finite Field," *Proc. Amer. Math. Soc.* 4(1953), 538.
4. _____, "Some Theorems on permutation Polynomials," *Bull. Amer. Math. Soc.* 68(1962), 120-122.
5. _____, "Permutations in Finite Fields," *Acta Sci. Math. Szeged* 24(1963), 196-203.
6. Carlitz, L. · Lutz, "A Characterization of Permutation polynomials over a finite field," *Amer. math. Monthly* 85(1978), 746-748.
7. Carlitz, L., and Well, C., "The Number of Solutions of a Special System of Equations in a Finite Field." *Acta Arith* 12(1966), 77-84.
8. Chowla, S., "On Substitution Polynomials (mod p)," *Norske Vid. Selsk. Forh.* (Trondheim) 41(1968), 4-6.
9. Cavior, S.R., "A Note on Octic Permutation polynomials," *Math. Comp.* 17 (1963), 450-452.
10. Dickson, L.E., "The Analytic representation of substitutions on a Power of a rime Number of letters with a discussion of the Linear group," *Ann. of Math.* 11(1897), 65-120, 161-183.
11. Hermite, C., "Sur les Fonctions de Sept Lettres," *C. R. Acad. Sci. Paris* 7 (1863), 750-757.
12. Lidl, R. · Niederreiter H., *Finite Fields, Encyclopedia Math. Appl. 20*, Addison-Wesley, Reading, Mass., 1983.
13. London, D. · Ziegler, Z., "Functions over the Residue Field Modulo a Prime," *J. Austral. Math. Soc.* Ser. A 7(1967), 410-416.
14. Lausch, R.R. · Noebauer, W., *Algebra of Polynomials*, North-Holland, Amsterdam, 1973.
15. Mollin, R.A. · Small, C., "On Permutation Polynomials over Finite Fields," *Internat. J. Math. Sci.* 10(1987), 535-544.
16. Niederreiter, H. · Robinson, K.H., "Complete Mappings of Finite Fields," *J. Austral. Math. Soc.* Ser. A 33(1982), 197-212.
17. Noebauer. W., "Uber eine Klasse von Permutationspolynomen und die dadurch

dargestellten Gruppen," *J. reine angew. Math.* 231(1968), 215-219.
18. Raussnitz, G., "Math. Naturw," *Ber. Ungarn* 1(1882/83), 266-278.
19. Rogers, L. J., "On the Analytic Representation of Heptagrams," *Proc. London Math. Soc.* 22(1890), 37-52.
20. Shur, I., "Uber den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz uber algebraische Funktionen," *Sitzungsber. Preu β. Akad. Wiss. Berlin Math.-Naturwiss.* Kl.(1923), 123-134.

A Historical Note on Permutation Polynomials over Finite Fields

Department of Mathematics, Hanyang University **Hong Goo Park**

In this paper, we analyze the basic concepts of permutation polynomials over finite fields, and the historical background through the use of the major classes of permutation polynomials over the fields. And also, we find a method of the polynomial representation with respect to cycles on the fields.

Key words: finite fields, permutation polynomials

2000 Mathematics Subject Classification: 12F10, ZDM Subject Classification: H20

논문 접수: 2005년 4월 20일 심사 완료: 2005년 5월