김일성종합대학학보 JOURNAL OF KIM IL SUNG UNIVERSITY
(자연과학) (NATURAL SCIENCE)
주체106(2017)년 제63권 제2호 Vol. 63 No. 2 JUCHE106(2017).

유한체우에서 $k-$불변다항식의 존재성과 몇가지 성질

권일진, 김률

경애하는 최고령도자 **김정은**동지께서는 다음과 같이 말씀하시였다.

《이미 일정한 토대가 있고 전망이 확고한 연구대상들에 힘을 넣어 세계패권을 쥐며 그 성과를 확대하는 방법으로 과학기술을 빨리 발전시켜야 합니다.》(《조선로동당 제7차대회에서 한 중앙위원회사업총화보고》 단행본 39페지)

론문에서는 유한체리론의 중요한 연구대상인 기약다항식가운데서 k －불변다항식을 정의하고 그것의 몇가지 성질을 연구하였다.

선행연구[2]에서는 불변원소의 개념을 일반화하여 $k-$불변원소를 정의하고 행렬의 위수를 리용하여 유한체의 원소가 $k-$불변원소로 되기 위한 한가지 필요충분조건을 밝혔으며 그것의 개수의 한계에 관한 평가식을 비롯한 몇가지 성질을 연구하였다.

선행연구[1]에서는 선행연구[2]에서와는 달리 $k-$불변원소가 되기 위한 몇가지 조건을 다항식들의 최대공약수의 차수를 리용하여 밝히고 그로부터 이미 알고있는 불변원소나 $k-$불변원소를 리용하여 새로운 $k-$불변원소를 구성하는 방법을 제기하였다.

론문에서는 불변다항식의 개념을 일반화하여 $k-$불변다항식을 정의하고 그것의 개수를 비롯한 몇가지 성질과 낮은 차수의 $k-$불변다항식으로부터 보다 높은 차수의 $k-$불변다항식을 구성하는 방법을 연구하였다.

q를 씨수의 제곱, n을 자연수, $\alpha\in\mathbf{F}_{q^n}$이라고 하자.

α의 공액원소전부의 모임이 1차독립일 때 α의 공액원소들로 이루어진 토대 $\{\alpha,\ \alpha^q,\ \alpha^{q^2},\ \cdots,\ \alpha^{q^{n-1}}\}$을 $\mathbf{F}_q$에 관한 $\mathbf{F}_{q^n}$의 불변토대라고 부르고 이때 α를 $\mathbf{F}_q$에 관한 $\mathbf{F}_{q^n}$의 불변원소라고 부른다.

다항식 x^n-1과 $\sum_{i=0}^{n-1}\alpha^{q^i}x^i\in\mathbf{F}_{q^n}[x]$의 $\mathbf{F}_{q^n}$에 관한 최대공약수의 차수가 k일 때 α를 $\mathbf{F}_q$에 관한 $\mathbf{F}_{q^n}$의 $k-$불변원소라고 부른다.[2]

α가 불변원소이기 위하여서는 다항식 x^n-1과 $\sum_{i=0}^{n-1}\alpha^{q^i}x^i\in\mathbf{F}_{q^n}[x]$가 서로 소일것이 필요충분하다는 사실로부터 불변원소는 0－불변원소라고 말할수 있다.

다항식 $f(x)\in\mathbf{F}_q[x]$가 기약이고 그 뿌리들이 $\mathbf{F}_q$에 관하여 1차독립이면 $f(x)$를 불변다항식 또는 $N-$다항식이라고 부른다.

정의 기약다항식 $f(x)\in\mathbf{F}_q[x]$의 뿌리들전부로 이루어진 벡토르단의 $\mathbf{F}_q$에 관한 위수가 k일 때 $f(x)$를 $k-$불변다항식 또는 N_k-다항식이라고 부른다.

k가 다항식의 차수와 같을 때 n차k－불변다항식은 불변다항식으로 된다.

실례 1 $f(x)=x^3+x+1$ 은 $\mathbf{F}_2[x]$ 의 3차기약다항식이다. $f(x)$ 의 한 뿌리를 α 라고 하면 $\alpha, \alpha^2, \alpha^4$ 은 $f(x)$ 의 서로 다른 세 뿌리이며 $\alpha^4=\alpha^2+\alpha$ 이므로 $\alpha, \alpha^2, \alpha^4$ 의 위수는 2이다.

따라서 $f(x)$ 는 3차 N_2-다항식이다.

기약다항식이 어떤 때 $k-$불변다항식으로 되는가를 보자.

$f(x)$ 를 n 차기약다항식, α를 $f(x)$ 의 한 뿌리라고 하면 $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ 은 $\mathbf{F}_{q^n}$ 의 다항식토대를 이루며 $\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}$ 은 $f(x)$ 의 뿌리전부이다.

$f(x)$ 의 뿌리들의 다항식토대에 관한 표시식이 $\alpha^{q^i}=\sum_{j=0}^{n-1} b_{ij}\alpha^j,\ b_{ij}\in\mathbf{F}_q$ 라고 하자.

그러면 벡토르단 $\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}$ 의 위수는 행렬 $b=(b_{ij})$ 의 위수와 같다. 따라서 $b=(b_{ij})$ 의 위수가 k 일 때 그리고 그때에만 $f(x)$ 가 $k-$불변다항식으로 된다. n 차불변다항식의 임의의 뿌리는 $\mathbf{F}_q$ 에 관한 $\mathbf{F}_{q^n}$ 의 불변원소이며 불변토대 $\{\alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$ 의 원소들은 $N-$다항식의 뿌리로 된다.

$k-$불변다항식에 대하여 이와 같은 성질이 성립되는가를 보자.

보조정리[2] $\alpha\in\mathbf{F}_{q^n}$ 이 $k-$불변원소이기 위해서는 벡토르단 $\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}$ 의 $\mathbf{F}_q$ 에 관한 위수가 $n-k$ 일것이 필요충분하다.

명제 1 $\mathbf{F}_q$ 에 기초한 n차 $k-$불변다항식의 임의의 뿌리는 $\mathbf{F}_q$ 에 관한 $\mathbf{F}_{q^n}$ 의 $(n-k)-$불변원소이다.

명제 2 α 가 $\mathbf{F}_q$ 에 관한 $\mathbf{F}_{q^n}$ 의 $k-$불변원소이면 α 의 최소다항식 $\min(\mathbf{F}_q, \alpha)$ 는 $(n-k)-$불변다항식이고 그것의 차수는 n 의 약수이다.

사실 α 가 $\mathbf{F}_q$ 에 관한 $\mathbf{F}_{q^n}$ 의 $k-$불변원소이면 $m(x)=\prod_{i=0}^{n-1}(x-\alpha^{q^i})\in\mathbf{F}_q[x]$ 는 α 의 최소다항식의 제곱이며 최소다항식의 뿌리들로 이루어진 벡토르단의 $\mathbf{F}_q$ 에 관한 위수는 $n-k$ 이다.

정리 1 $\mathbf{F}_q$ 에 기초한 n 차 $k-$불변다항식이 존재하면 다항식 x^n-1 은 $\mathbf{F}_q$ 에서 차수가 k 인 인수를 가진다.

증명 $f(x)\in\mathbf{F}_q[x]$ 가 n 차 $k-$불변다항식이라고 하면 그것의 뿌리들은 $\mathbf{F}_q$ 에 관한 $\mathbf{F}_{q^n}$ 의 $(n-k)-$불변원소이다. $\mathbf{F}_q$ 에 관한 $\mathbf{F}_{q^n}$ 의 $k-$불변원소가 존재하기 위해서는 다항식 x^n-1 이 $\mathbf{F}_q$ 에서 차수가 k 인 인수를 가질것이 필요하고 충분하다.(증명끝)

주의 정리 1의 거꿀은 일반적으로 성립하지 않는다.

실례 2 $q=2,\ n=6$ 인 경우 $\mathbf{F}_2$ 에 기초한 6차기약다항식들은 다음과 같다.

$$f_1(x)=x^6+x^5+1,\quad f_2(x)=x^6+x^5+x^4+x^2+1,\quad f_3(x)=x^6+x^5+x^4+x+1$$
$$f_4(x)=x^6+x^5+x^2+x+1,\quad f_5(x)=x^6+x+1,\quad f_6(x)=x^6+x^4+x^3+x+1$$
$$f_7(x)=x^6+x^3+1,\quad f_8(x)=x^6+x^4+x^2+x+1,\quad f_9(x)=x^6+x^5+x^3+x^2+1$$

여기서 f_1, f_2, f_3, f_4 는 6－불변다항식, f_5, f_6 은 5－불변다항식, f_7, f_8, f_9 는 4－불변다항식이다.

한편 $x^6-1=(x+1)^2(x^2+x+1)^2$ 이므로 1차부터 6차까지의 임의의 차수의 인수는 모두 존재한다. 그러나 1－불변다항식과 2－불변다항식, 3－불변다항식은 존재하지 않는다.

$\mathbf{F}_q[x]$에서 n차 $k-$불변다항식의 개수를 $N(q,\ n\,;k)$, $\mathbf{F}_q$에 관한 $\mathbf{F}_{q^n}$의 $k-$불변원소의 개수를 $N_e(q,\ n\,;k)$로 표시하자.

$f\in\mathbf{F}_q[x]$가 모니크다항식일 때 차수가 f의 차수를 넘지 않으면서 f와 서로 소인 다항식의 개수를 $\Phi_q(f)$로 정의한다.[2]

정리 2[2] $\mathbf{F}_q$에 관한 $\mathbf{F}_{q^n}$의 $k-$불변원소의 개수는 $N_e(q,\ n\,;k)=\sum\limits_{\substack{h|x^n-1\\ \deg h=n-k}}\Phi_q(h)$로 주어진다. 여기서 $h(x)$는 모니크다항식이며 나누기는 $\mathbf{F}_q$에 관하여 진행한다.

정리 3 $\mathbf{F}_q[x]$에서 n차 $k-$불변다항식의 개수는 다음과 같다.

$$N(q,\ n\,;k)=\frac{N_e(q,\ n\,;n-k)-\sum\limits_{\substack{d|n\\ \neq}}N(q,\ d\,;k)\cdot d}{n}$$

증명 $f(x)\in\mathbf{F}_q[x]$가 n차 N_k-다항식이라고 하면 $f(x)$는 $\mathbf{F}_{q^n}$에서 n개의 서로 다른 뿌리를 가지며 그것들은 모두 $\mathbf{F}_q$에 관한 $\mathbf{F}_{q^n}$의 $(n-k)-$불변원소이다. 그런데 $(n-k)-$불변원소의 최소다항식이 언제나 n차인것은 아니므로 $N(q,\ n\,;k)$는 최소다항식이 n차로 되는 $(n-k)-$불변원소의 개수를 n으로 나눈 값과 같다.

α가 $\mathbf{F}_q$에 관한 $\mathbf{F}_{q^n}$의 $(n-k)-$불변원소이고 그것의 최소다항식을 $p(x)$라고 하자.

그러면 명제 2로부터 $p(x)$는 $k-$불변다항식이고 그것의 차수는 n의 약수이다. α가 n보다 작은 차수의 최소다항식을 가진다면 n의 정의약수 d가 있어서 α는 어떤 d차 $k-$불변다항식의 뿌리로 된다.

d차 $k-$불변다항식의 개수는 $N(q,\ d\,;k)$이므로 최소다항식의 차수가 n보다 작은 $(n-k)-$불변원소의 개수는 $\sum\limits_{\substack{d|n\\ \neq}}N(q,\ d\,;k)\cdot d$이다.(증명끝)

따름 1 n이 k보다 작지 않은 약수(n을 제외한)를 가지지 않을 때 n차 $k-$불변다항식의 개수는 $\mathbf{F}_q$에 관한 $\mathbf{F}_{q^n}$의 $(n-k)-$불변원소의 개수를 n으로 나눈 값과 같다. 즉

$$N_p(q,\ n\,;k)=N_e(q,\ n\,;n-k)/n.$$

따름 2 $n\geq3$일 때 n차$(n-1)-$불변다항식의 개수는 1−불변원소의 개수를 n으로 나눈 값과 같다.

실례 3 $q=2,\ n=6$일 때 0−불변원소는 24개, 1−불변원소는 12개, 2−불변원소는 18개, 3−불변원소는 3개, 4−불변원소는 5개, 5−불변원소는 1개이다.

6−불변다항식의 개수는 $N(2,\ 6\,;6)=\frac{N_e(2,\ 6\,;0)}{6}=4$이다.

마찬가지로 5−불변다항식과 4−불변다항식의 개수는 각각 2, 3이다.

3−불변다항식의 개수는 $N(2,\ 6\,;3)=\frac{N_e(2,\ 6\,;3)-N(2,\ 3\,;3)\cdot 3}{6}$으로 주어진다.

3차기약다항식 x^3+x^2+1은 3−불변다항식이고 x^3+x+1은 2−불변다항식이므로 $N(2,3\,;3)=1$이고 따라서 $N(2,\ 6\,;3)=0$이다.

마찬가지로 2−불변다항식과 1−불변다항식의 개수도 0이라는것을 알수 있다.

다음의 정리는 k_1, k_2를 정의옹근수라고 할 때 k_1-불변다항식과 k_2-불변다항식으로부터 새로운 $k-$불변다항식을 얻는 방법을 보여준다.

정리 4 $(v,\ t)=1$, $n=vt$라고 하고 $f(x)=\sum_{i=0}^{v} a_i x^i \in \mathbf{F}_q[x]$와 $g(x)=\sum_{j=0}^{t} b_j x^j \in \mathbf{F}_q[x]$를 각각 v차 $N_{k_1}-$다항식, t차 $N_{k_2}-$다항식이라고 하자. 그리고 A, B를 각각 $f(x)$, $g(x)$의 생성행렬, $C=A\otimes B$를 A와 B의 크로네카적이라고 하자.

이때 다항식 $\det(Ix-C)$는 n차 $N_{k_1k_2}-$다항식이다.

증명 α와 β를 각각 $f(x)$, $g(x)$의 뿌리라고 하자.

그러면 $\alpha, \alpha^q, \cdots, \alpha^{q^{v-1}}$은 A의 고유값이며 $\beta, \beta^q, \cdots, \beta^{q^{t-1}}$은 B의 고유값으로 된다.

이때 $C=A\otimes B$의 고유값은 $\alpha^{q^i}\beta^{q^j}$, $0\le i\le v-1$, $0\le j\le t-1$이며 따라서

$$\det(Ix-C)=\prod_{\substack{0\le i\le v-1\\ 0\le j\le t-1}}(x-\alpha^{q^i}\beta^{q^j})$$

이 성립된다. 벡토르단 $\{\alpha^{q^i}\beta^{q^j}\mid 0\le i\le v-1,\ 0\le j\le t-1\}$의 위수는 k_1k_2이므로 다항식 $\det(Ix-C)$가 n차 $N_{k_1k_2}-$다항식이라는것을 알수 있다.(증명끝)

참 고 문 헌

[1] 권일진 등; 조선민주주의인민공화국 과학원통보, 2, 8, 주체105(2016).

[2] S. Huczynska et al.; Finite Fields Appl., 24, 170, 2013.

주체105(2016)년 10월 5일 원고접수

Existence and Some Properties of *k*-Normal Polynomials over Finite Fields

Kwon Il Jin, Kim Ryul

We defined *k*-normal polynomial by generalizing the concept of normal polynomial, introduced the recursive formula of their numbers and studied some properties of *k*-normal polynomial including recurrent methods for constructing *k*-normal polynomial of higher degree from the one of lower degree.

Key words: finite field, *k*-normal polynomial