김일성종합대학학보
(자연과학)
주체105(2016)년 제62권 제5호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 62 No. 5 JUCHE105(2016).

유한체우에서 한가지 완전치환다항식클라스

김광천, 김광연

경애하는 **김정은**동지께서는 다음과 같이 말씀하시였다.

《과학자, 기술자들은 당이 마련해준 과학기술룡마의 날개를 활짝 펴고 과학적재능과 열정을 총폭발시켜 누구나 다 높은 과학기술성과들을 내놓음으로써 부강조국건설에 이바지하는 참된 애국자가 되여야 합니다.》

q를 씨수의 제곱, $\mathbf{F}_q$를 q개의 원소를 가지는 유한체, $\mathbf{F}_q^*$을 그것의 곱하기군이라고 할 때 다항식 $f\in\mathbf{F}_q[X]$에 대하여 $\mathbf{F}_q$를 그자체로 넘기는 다항식넘기기 $f:c\mapsto f(c)$가 우로의 1：1넘기기이면 다항식 f를 $\mathbf{F}_q$의 치환다항식이라고 부른다.

다항식 $f(X)\in\mathbf{F}_q[X]$에 대하여 $f(X)$와 $f(X)+X$가 $\mathbf{F}_q$의 치환다항식이면 그 다항식들을 $\mathbf{F}_q$의 완전치환다항식이라고 부른다.

선행연구[3]에서는 여러 완전치환다항식클라스가 연구되였으며 선행연구[1, 2]에서는 $\mathbf{F}_{2^{2m}}$우에서 vX^{2^m+2}과 $v^{-1}X^{2^{m+1}+3}$형태의 단항식이 완전치환다항식이 될 조건을 밝혔다.

론문에서는 $v^{-1}X^{\frac{2^{2m+1}+1}{3}}$형태의 단항식이 $\mathbf{F}_{2^{2m}}$의 완전치환다항식이 될 조건을 밝힌다.

α를 유한체 $\mathbf{F}_{2^{2m}}$의 원시원소라고 하고 $D_0=\langle\alpha^3\rangle$, $D_1=\alpha D_0$, $D_2=\alpha^2D_0$이라고 놓으면 $2^{2m}-1\equiv 0(\mathrm{mod}3)$이므로 $\mathbf{F}_{2^{2m}}$은 $\{0\}$, D_0, D_1, D_2의 사귀지 않는 합으로 표시된다.

$\alpha^{(2^{2m}-1)/3}=\beta$라고 놓으면 $\beta^3=\alpha^{2^{2m}-1}=1$이고 이로부터 $0=\beta^3-1=(\beta-1)(\beta^2+\beta+1)$이며 α가 원시원소이므로 $\beta\neq 1$이다. 즉

$$\beta^2+\beta+1=0. \qquad (*)$$

$v\in\mathbf{F}_q^*$이라고 가정하고 $v^{-1}X^{\frac{2^{2m+1}+1}{3}}$이 완전치환다항식이 되는 v에 대한 조건을 얻기 위하여 먼저 $f(X)=X^{\frac{2^{2m+1}+1}{3}}+vX$가 치환다항식이 되는 v에 대한 조건을 보자.

보조정리 1 $f(X)=X^{\frac{2^{2m+1}+1}{3}}+vX$가 치환다항식이기 위해서는 $v^3\neq 1$이고

$$\frac{\beta^2+v}{1+v},\ \frac{\beta+v}{\beta^2+v},\ \frac{1+v}{\beta+v}\notin D_2$$

일것이 필요하고 충분하다.

증명 $$f(X)=X^{(2^{2m+1}+1)/3}+vX=X(X^{2(2^{2m}-1)/3}+v)$$

$x\in D_0$이면 x는 α^{3k}형태로 표시되며

$$x^{2\frac{2^{2m}-1}{3}}+v=\alpha^{3k\cdot 2\frac{2^{2m}-1}{3}}+v=\alpha^{2k(2^{2m}-1)}+v=1+v$$

이고 $f(x)=(1+v)x$ 로 된다.

$x\in D_1$ 이면 x는 α^{3k+1} 형태로 표시되며

$$x^{2\frac{2^{2m}-1}{3}}+v=\alpha^{(3k+1)\cdot 2\frac{2^{2m}-1}{3}}+v=\alpha^{2k(2^{2m}-1)+2\frac{2^{2m}-1}{3}}+v=\alpha^{2\frac{2^{2m}-1}{3}}+v=\beta^2+v$$

이고 $f(x)=(\beta^2+v)x$ 로 된다.

마찬가지로 $x\in D_2$ 이면 x는 α^{3k+2} 형태로 표시되며

$$x^{2\frac{2^{2m}-1}{3}}+v=\alpha^{(3k+2)\cdot 2\frac{2^{2m}-1}{3}}+v=\alpha^{2k(2^{2m}-1)+4\frac{2^{2m}-1}{3}}+v=\alpha^{\frac{2^{2m}-1}{3}}+v=\beta+v$$

이고 $f(x)=(\beta+v)x$ 로 된다.

이로부터 $f(x)=\begin{cases}0, & x=0\\ (1+v)x, & x\in D_0\\ (\beta^2+v)x, & x\in D_1\\ (\beta+v)x, & x\in D_2\end{cases}$ 로 된다.

먼저 필요성을 증명하기 위하여 f가 치환다항식이라고 가정하자.

$1+v=0$ 이면 $x\in D_0$ 인 임의의 x에 대하여 $f(x)=0$ 이며 이것은 f의 치환성에 모순이다. 그러므로 $1+v\neq 0$ 이고 마찬가지로 $\beta^2+v,\ \beta+v\neq 0$ 이다.

$1,\ \beta^2,\ \beta$가 $X^3=1$의 세 뿌리이므로 이로부터 $v^3\neq 1$ 이다.

$(\beta^2+v)/(1+v)\in D_2$ 라고 하고 $x_1\in D_1$ 인 x_1을 취하면 $(\beta^2+v)/(1+v)x_1\in D_0$ 이므로 $f\left(\dfrac{\beta^2+v}{1+v}x_1\right)=(1+v)\dfrac{\beta^2+v}{1+v}x_1=(\beta^2+v)x_1$ 이다.

$f(x_1)=(\beta^2+v)x_1$ 이므로 $f(x_1)=f\left(\dfrac{\beta^2+v}{1+v}x_1\right)$ 이다. 이것은 f의 치환성에 모순이고 결국 $(\beta^2+v)/(1+v)\notin D_2$ 라는것이 나온다.

마찬가지로 $\dfrac{\beta+v}{\beta^2+v},\ \dfrac{1+v}{\beta+v}\notin D_2$ 라는것이 나오며 이로부터 필요성이 증명된다.

충분성을 증명하자.

$v^3\neq 1$ 이므로 $v\neq 1,\ \beta^2,\ \beta$ 이고 이로부터 $1+v,\ \beta^2+v,\ \beta+v\neq 0$ 이라는것이 나온다.

그러므로 $x\neq 0$ 이면 $f(x)\neq 0$ 이 나온다. $x_0,\ x_1$이 같은 D_i에 들면 $f(x_0)=f(x_1)$ 로부터 $x_0=x_1$이 쉽게 나온다.

x_0과 x_1이 각각 서로 다른 모임에 속하는 경우를 보자.

먼저 $x_0\in D_0,\ x_1\in D_1$ 인 경우 $f(x_0)=f(x_1)$ 이라고 하면 $(1+v)x_0=(\beta^2+v)x_1$ 이고 $\dfrac{\beta^2+v}{1+v}=\dfrac{x_0}{x_1}\in D_2$ 이며 이것은 조건에 모순이다.

다른 경우도 마찬가지이며 이로부터 충분성이 증명된다.(증명끝)

따름 1 $f_1(X)=X^{\frac{2^{2m+1}+1}{3}}+vX$ 가 치환다항식이기 위해서는 $f_2(X)=X^{\frac{2^{2m+1}+1}{3}}+v^2X$ 가 치환다항식일것이 필요하고 충분하다.

증명 먼저 필요성을 증명하자.

$f_1(X)$ 가 치환다항식이므로 보조정리 1에 의하여 $v^3\neq 1$ 이다. $v^6-1=(v^3-1)^2\neq 0$ 이므로 $v^6\neq 1$ 이다. $\dfrac{\beta^2+v^2}{1+v^2}=\left(\dfrac{\beta+v}{1+v}\right)^2$ 이고 보조정리 1에 의하여 $\dfrac{\beta+v}{1+v}\notin D_1$ 이며 이로부터 $\dfrac{\beta^2+v^2}{1+v^2}\notin D_2$ 라는것이 나온다.

마찬가지로 $\dfrac{\beta+v^2}{\beta^2+v^2},\ \dfrac{1+v^2}{\beta+v^2}\notin D_2$ 이며 보조정리 1에 의하여 $f_2(X)$ 는 치환다항식이다.

$f_2(X)$ 가 치환다항식이므로 $X^{\frac{2^{2m+1}+1}{3}}+v^{2^2}X,\ \cdots,\ X^{\frac{2^{2m+1}+1}{3}}+v^{2^{2m}}X$ 도 치환다항식이며 $X^{\frac{2^{2m+1}+1}{3}}+v^{2^{2m}}X=X^{\frac{2^{2m+1}+1}{3}}+vX$ 라는것을 고려하면 충분성이 증명된다.(증명끝)

따름 2 $f_1(X)=X^{\frac{2^{2m+1}+1}{3}}+vX$ 가 치환다항식이기 위해서는 $f_2(X)=X^{\frac{2^{2m+1}+1}{3}}+\beta vX$ 가 치환다항식일것이 필요하고 충분하다.

증명 $v^3\neq 1$ 과 $(\beta v)^3\neq 1$ 이 동등하고 $\dfrac{\beta^2+\beta v}{1+\beta v}=\dfrac{\beta+v}{\beta^2+v}$ 라는데로부터 따름 1과 꼭같이 증명된다.(증명끝)

$1/(1+v)+\beta=u$ 라고 놓고 v 에 대한 조건을 u 에 대한 조건으로 주기로 한다.

보조정리 2 $f(X)=X^{\frac{2^{2m+1}+1}{3}}+vX$ 가 치환다항식이기 위해서는 $\beta(u+1),\ \beta^2u\in D_0$ 이거나 $\beta(u+1)\in D_1,\ \beta^2u\in D_2$ 일것이 필요하고 충분하다.

증명 보조정리 1의 조건으로부터 $\dfrac{\beta^2+v}{1+v},\ \dfrac{1+v}{\beta+v}$ 는 D_0 또는 D_1 에 속하는데 그것들의 적이 D_1 에 속하지 않으므로 보조정리 1의 조건은 $\dfrac{\beta^2+v}{1+v},\ \dfrac{1+v}{\beta+v}$ 가 다 D_0 에 속하든가 D_1 에 속한다는것과 동등하다.

다시 이것은 $\dfrac{\beta^2+v}{1+v},\ \dfrac{\beta+v}{1+v}\in D_0$ 이거나 $\dfrac{\beta^2+v}{1+v}\in D_1,\ \dfrac{\beta+v}{1+v}\in D_2$ 가 성립된다는것과 동등하며 $1+v=w^{-1}$ 으로 놓으면 식 (*)로부터

$$\frac{\beta^2+v}{1+v}=\frac{\beta^2-1+w^{-1}}{w^{-1}}=\beta w+1=\beta(w+\beta^2),\ \ \frac{\beta+v}{1+v}=\beta^2(w+\beta)$$

로 되고 결국 보조정리 1의 조건과 동등한 조건은 $\beta(w+\beta^2),\ \beta^2(w+\beta)\in D_0$ 이거나 $\beta(w+\beta^2)\in D_1,\ \beta^2(w+\beta)\in D_2$ 라는것이다.

$w+\beta=u$ 라고 놓으면 우의 조건은 $\beta(u+1),\ \beta^2u\in D_0$ 이거나 $\beta(u+1)\in D_1,\ \beta^2u\in D_2$ 로 된다.(증명끝)

따름 3 $m\not\equiv 1 \pmod 3$ 일 때 $u+1\in D_1,\ u\in D_2$ 이면 $f(X)=X^{(2^{2m+1}+1)/3}+vX$ 는 치환다항식이다.

증명 $m\equiv 0 \pmod 3$ 이면 $2^{2m}-1=2^{6m/3}-1=64^{m/3}-1\equiv 0 \pmod 9$, $(2^{2m}-1)/3\equiv 0 \pmod 3$ 이며 $\beta\in D_0$ 이다. 그러므로 $\beta(u+1)\in D_1,\ \beta^2u\in D_2$ 이고 $f(X)=X^{(2^{2m+1}+1)/3}+vX$ 는 치환다항식이다.

$m\equiv 2 \pmod 3$ 이면 $2^{2m}-1\equiv 2^4-1\equiv 6 \pmod 9$ 이고 $(2^{2m}-1)/3\equiv 2 \pmod 3$ 이며 $\beta\in D_2$ 이다. 즉 $\beta(u+1),\ \beta^2u\in D_0$ 이고 보조정리 2에 의하여 $f(X)=X^{(2^{2m+1}+1)/3}+vX$ 는 치환다항식이다.(증명끝)

정리 $v^{-1}X^{(2^{2m+1}+1)/3}$이 완전치환다항식이기 위해서는 $m\not\equiv 1 \pmod 3$ 이면서 $\beta(u+1),\ \beta^2u\in D_0$ 이거나 $\beta(u+1)\in D_1,\ \beta^2u\in D_2$ 일것이 필요하고 충분하다.

증명 $m\not\equiv 1 \pmod 3$ 이면 $\gcd((2^{2m+1}+1)/3,\ 2^{2m}-1)=1$ 이고 $v^{-1}X^{(2^{2m+1}+1)/3}$ 은 치환다항식이다. 거꾸로 $v^{-1}X^{(2^{2m+1}+1)/3}$ 이 치환다항식이면 $\gcd((2^{2m+1}+1)/3,\ 2^{2m}-1)=1$ 이고 $m\not\equiv 1 \pmod 3$ 라는것이 나온다.

$v^{-1}X^{(2^{2m+1}+1)/3}+X$ 가 치환다항식이기 위해서는 $f(X)=X^{(2^{2m+1}+1)/3}+vX$ 가 치환다항식일것이 필요충분하며 이것은 $\beta(u+1),\ \beta^2u\in D_0$ 이거나 $\beta(u+1)\in D_1,\ \beta^2u\in D_2$ 라는것과 동등하다. 따라서 $v^{-1}X^{(2^{2m+1}+1)/3}$가 완전치환다항식이기 위해서는 $m\not\equiv 1 \pmod 3$ 이면서 $\beta(u+1),\ \beta^2u\in D_0$ 이거나 $\beta(u+1)\in D_1,\ \beta^2u\in D_2$ 일것이 필요하고 충분하다.(증명끝)

참 고 문 헌

[1] P. Charpin et al.; SIAM J. Discrete Math., **22**, 2, 650, 2008.

[2] Z. Tu et al.; Finite Fields Appl., **25**, 182, 2014.

[3] P. Yuan et al.; Finite Fields Appl., **17**, 6, 560, 2011.

주체105(2016)년 1월 5일 원고접수

A Class of Complete Permutation Polynomials on Finite Fields

Kim Kwang Chon, Kim Kwang Yon

We determined the conditions for binomials of the given form to be permutation polynomials and studied the properties of those binomials. And we proposed a class of complete permutation monomials of a form on finite fields based on the above results.

Key words: complete permutation polynomial, monomial, finite field