김일성종합대학학보 주체110(2021)년
수 학 제67권 제1호

유한체우의 자기공액상반기약다항식들의 개수

김 률

경애하는 **김정은**동지께서는 다음과 같이 말씀하시였다.

《수학, 물리학, 화학, 생물학과 같은 기초과학부문에서 과학기술발전의 원리적, 방법론적기초를 다져나가면서 세계적인 연구성과들을 내놓아야 합니다.》

$f(x)$는 표수가 p인 유한체 $\mathbf{F}_q$우의 n차다항식이고 $f(0)\neq 0$이라고 하자. 이때 다항식 $f^*(x):=x^n f(0)^{-1}f(1/x)$을 $f(x)$의 상반다항식이라고 부르고 $f^*(x)=f(x)$일 때 $f(x)$를 자기상반다항식이라고 부른다. 선행연구[5]에서는 차수가 2이상인 기약다항식은 그것의 뿌리모임이 거꿀연산에 관하여 닫길 때에만 자기상반기약다항식으로 되므로 차수가 2이상인 자기상반기약다항식의 차수는 짝수라는것을 밝혔다.

또한 $S_q(m)$을 $\mathbf{F}_q$우의 $2m$차자기상반기약다항식들전부의 개수라고 하자. 그러면 선행연구[4]에서는

$$S_q(m)=\begin{cases}\dfrac{1}{2m}(q^m-1), & 2\nmid q\wedge m=2^s\\ \dfrac{1}{2m}\sum\limits_{\substack{d\mid m\\ 2\nmid d}}\mu(d)q^{m/d}, & \text{기타}\end{cases}\tag{1}$$

이라는것이 밝혀졌다. 여기서 μ는 뫼비우스함수이다.

최근에는 $\mathbf{F}_q$의 2차확대체 $\mathbf{F}_{q^2}$우에서의 자기공액상반다항식의 개념이 정의되고 그것의 성질들이 연구되고있다.

다항식 $f(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbf{F}_{q^2}[x]$에 대하여 다항식 $\overline{f(x)}:=\overline{a_0}+\overline{a_1}x+\cdots+\overline{a_n}x^n$을 $f(x)$의 공액다항식이라고 부른다. 여기서 $\overline{}:\mathbf{F}_{q^2}\to\mathbf{F}_{q^2}$은 임의의 $\alpha\in\mathbf{F}_{q^2}$에 대하여 $\alpha\mapsto\alpha^q$으로 정의된 체자기동형넘기기이다. 또한 $f(0)\neq 0$인 다항식 $f(x)\in\mathbf{F}_{q^2}[x]$가 그것의 공액상반다항식 $f^\dagger(x):=\overline{f^*(x)}$와 같을 때 $f(x)$를 자기공액상반다항식이라고 부른다.[2]

선행연구[1]에서는 $\mathbf{F}_{q^2}$우의 기약모니크다항식이 자기공액상반다항식이기 위한 필요충분조건이 구해졌고 자기공액상반기약다항식의 차수는 홀수이며 $\mathbf{F}_{q^2}$우의 n차자기공액상반기약다항식들의 개수가

$$\frac{1}{n}\sum_{d\in D_n}\phi(d)\tag{2}$$

라는것이 밝혀졌다. 여기서 D_n은 $0\leq k<n$인 모든 k에 대하여 q^k+1을 완제하지 않는 q^n+1의 정의 약수들전부의 모임이고 ϕ는 오일러함수이다.

론문에서는 $\mathbf{F}_q$ 우의 자기상반기약다항식과 $\mathbf{F}_{q^2}$ 우의 기약다항식들사이의 관계를 밝히고 그에 기초하여 $\mathbf{F}_{q^2}$ 우의 자기공액상반기약다항식들의 개수를 q 와 다항식의 차수에 의하여 결정하는 공식을 유도한다.

우선 다항식들의 적과 공액상반성과의 관계를 보기로 하자.

보조정리 1 $\mathbf{F}_{q^2}$ 우의 두 다항식의 적의 공액상반다항식은 매 다항식의 공액상반다항식들의 적과 같다.

따름 $\mathbf{F}_{q^2}$ 우의 임의의 다항식과 그것의 공액상반다항식의 적은 자기공액상반다항식이다.

보조정리 2 $\mathbf{F}_q$ 우의 임의의 $2m$ 차자기상반기약다항식은 m 이 홀수이면 $\mathbf{F}_{q^2}$ 우의 두 m 차자기공액상반기약다항식의 적이고 m 이 짝수이면 $\mathbf{F}_{q^2}$ 우의 서로 공액상반인 두 기약다항식의 적이다.

$\mathbf{F}_q$ 우의 $2m$ (m 은 홀수)차자기상반기약다항식 $f(x)$ 가 $\mathbf{F}_{q^2}$ 우의 m 차자기공액상반기약다항식 $g(x)$ 와 $\overline{g(x)}$ 의 적으로 표시될 때

$$\mathrm{ord}f = \mathrm{ord}g = \mathrm{ord}\bar{g}$$

이다. 여기서 $\mathrm{ord}f$ 는 다항식 f 의 위수 즉 f 가 $x^e - 1$ 을 완제할 때 그러한 e 들가운데서 최소의 정의 옹근수이다. 사실 $f(x)$ 가 $\mathbf{F}_q$ 우의 $2m$ 차기약다항식이므로 선행연구[3]에서의 정리 3.3에 의하여 $f(x)$ 의 위수는 $\mathbf{F}_{q^{2m}}$ 에서의 $f(x)$ 의 뿌리의 위수와 같고 또 $g(x)$ 가 $\mathbf{F}_{q^2}$ 우에서 m 차기약다항식이므로 $g(x)$ 의 위수는 $\mathbf{F}_{q^{2m}}$ 에서의 $g(x)$ 의 뿌리의 위수와 같다. 그런데 $g(x)$ 의 뿌리는 $f(x)$ 의 뿌리이므로 따라서 $g(x)$ 의 위수는 $f(x)$ 의 위수와 같다.

마찬가지로 $\mathrm{ord}g = \mathrm{ord}\bar{g}$ 가 성립한다는것이 증명된다.

보조정리 3 m 이 3이상의 홀수일 때 $g(x) \in \mathbf{F}_{q^2}[x]$ 가 m 차자기공액상반기약다항식이면 $\overline{g(x)} \neq g(x)$ 이다.

보조정리 4 m 이 3이상의 홀수일 때 $g(x) \in \mathbf{F}_{q^2}[x]$ 가 m 차자기공액상반기약다항식이면 $f(x) := g(x)\overline{g(x)}$ 는 $\mathbf{F}_q$ 우의 $2m$ 차자기상반기약다항식이다.

주의 1 보조정리 3, 4에서 《자기공액상반》이라는 조건이 없으면 결과가 성립하지 않는다. 실례로 $\mathbf{F}_4$ 우의 3차기약다항식 $g(x) := x^3 + x + 1$ 에 대하여 $\overline{g(x)} = g(x)$ 이고 $f(x) := g(x)\overline{g(x)} = g(x)^2$ 은 $\mathbf{F}_2$ 우에서 기약이 아니다.

정리 m 이 3이상의 홀수일 때 $\mathbf{F}_{q^2}$ 우의 m 차자기공액상반기약다항식들전부의 개수는 다음과 같다.

$$\frac{1}{m}\sum_{\substack{d|m \\ 2\nmid d}} \mu(d) q^{m/d} \tag{3}$$

증명 보조정리 2－4로부터 $\mathbf{F}_{q^2}$ 우의 m (m 은 홀수)차자기공액상반기약다항식들전부의 개수는 $\mathbf{F}_q$ 우의 $2m$ 차자기상반기약다항식들전부의 개수의 2배이다. 그러므로 $\mathbf{F}_q$ 우의 $2m$ 차자기상반기약다항식들전부의 개수에 대한 공식 (1)로부터 결과가 나온다.(증명끝)

따름 q가 씨수의 제곱이고 m이 3이상의 홀수이면 다음의 관계식이 성립한다.

$$\sum_{\substack{d|m \\ 2\nmid d}} \mu(d) q^{m/d} = \sum_{d \in D_m} \phi(d) \tag{4}$$

증명 식 (2)와 (3)으로부터 곧 나온다.(증명끝)

주의 2 m이 짝수인 경우 식 (4)는 일반적으로 성립하지 않는다. 실례로 $q=3,\ m=4$일 때 왼변은 81이고 오른변은 80으로서 서로 다르다.

참 고 문 헌

[1] A. Boripan et al.; arXiv: 1801.08842 [math.RA], 2018.

[2] A. Boripan et al.; Finite Fields Appl., 55, 78, 2019.

[3] R. Lidl, H. Niederreiter; Finite Fields, Cambridge University Press, 83～148, 2003.

[4] H. Meyn; Appl. Algebra Engrg. Comm. Comput., 1, 43, 1990.

[5] J. L. Yucas, G. L. Mullen; Design, Des. Codes Cryptogr., 33, 275, 2004.

주체109(2020)년 9월 5일 원고접수

The Number of Self-conjugate-reciprocal Irreducible Polynomials over Finite Fields

Kim Ryul

In this paper we establish a relation between the self-reciprocal irreducible polynomials over a finite field $\mathbf{F}_q$ and the irreducible ones over $\mathbf{F}_{q^2}$ and based on it, propose a formula of determining the number of self-conjugate-reciprocal irreducible polynomials over $\mathbf{F}_{q^2}$ in terms of q and a given degree m.

Keywords: finite field, self-conjugate-reciprocal polynomial, irreducible polynomial