유한체와 2차확대체우의 기약다항식들사이의 관계

김 룔

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《기초과학에 대한 근시안적인 관점을 버리고 기초과학연구에 계속 힘을 넣어 첨단과학기술을 비롯한 과학기술발전의 원리적, 방법론적기초를 튼튼히 다져나가야 합니다.》(《**김정일**선집》 증보판 제22권 22페지)

$\mathbf{F}_q$ 를 표수가 p 인 유한체, $\mathbf{F}_{q^2}$ 을 $\mathbf{F}_q$ 의 2차확대체라고 하고 n 을 정의 옹근수라고 하자. 그리고 다항식이라고 할 때 그것은 모니크다항식이라고 약속하겠다.

$\mathbf{F}_q$ 우의 n 차기약다항식들의 개수를 $N_q(n)$ 으로 표시하면

$$N_q(n)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d=\frac{1}{n}\sum_{d|n}\mu(d)q^{n/d} \tag{1}$$

이다.[3]

이제 $f(x)(\in\mathbf{F}_q[x])$ 가 n 차다항식이고 $f(0)\neq 0$ 이라고 하자. 이때 다항식 $f^*(x):=x^nf(0)^{-1}f(1/x)$ 을 $f(x)$ 의 상반다항식이라고 부른다. 특히 $f^*(x)=f(x)$ 일 때 $f(x)$ 를 자기상반다항식이라고 부른다.

차수가 2이상인 기약다항식은 그것의 뿌리모임이 거꿀연산에 관하여 닫길 때에만 자기상반기약다항식으로 되므로 차수가 2이상인 자기상반기약다항식의 차수는 짝수이다.[5]

2차확대체 $\mathbf{F}_{q^2}$ 우의 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 $\bar{}:\mathbf{F}_{q^2}\to\mathbf{F}_{q^2}$ 은 임의의 $\alpha(\in\mathbf{F}_{q^2})$ 에 대하여 $\alpha\mapsto\alpha^q$ 으로 정의된 체우의 자기동형넘기기이다. 그리고 $f(0)\neq 0$ 인 다항식 $f(x)(\in\mathbf{F}_q[x])$ 가 그것의 공액상반다항식 $f^\dagger(x)(:=\overline{f^*(x)})$ 와 같을 때 $f(x)$ 를 자기공액상반다항식이라고 부른다.

자기공액상반기약다항식의 차수는 홀수이다.[2]

$\mathbf{F}_q$ 우의 n 차자기상반기약다항식들의 개수와 이 n 차자기상반기약다항식들전부의 적을 각각 $\mathrm{NSRIM}_q(n)$, $\mathrm{PSRIM}_q(n)$ 으로 표시하자. 그러면 다음과 같은 식들이 성립한다.[4]

$$\mathrm{NSRIM}_q(2n)=\begin{cases}\dfrac{1}{2n}(q^n-1) & (2\nmid q,\ n=2^s\text{인 경우})\\ \dfrac{1}{2n}\displaystyle\sum_{\substack{d\mid n\\ 2\nmid d}}\mu(d)q^{n/d} & (\text{기타의 경우})\end{cases} \tag{2}$$

$$\mathrm{PSRIM}_q(2n)=\prod_{\substack{d\mid n\\ 2\nmid d}}\left(\frac{x^{q^{n/d}+1}-1}{x^{1+e_q}-1}\right)^{\mu(d)} \tag{3}$$

여기서 μ는 뫼비우스의 함수이고 $e_q = q \pmod 2$이다.

또한 $\mathbf{F}_{q^2}$ 우의 n차자기공액상반기약다항식들의 개수와 이 n차자기공액상반기약다항식들전부의 적을 각각 $\mathrm{NSCRIM}_{q^2}(n)$, $\mathrm{PSCRIM}_{q^2}(n)$으로 표시하자. 그러면 $n(\geq 3)$이 홀수일 때

$$\mathrm{NSCRIM}_{q^2}(n) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d} \tag{4}$$

이고[1] $\mathrm{NSCRIM}_{q^2}(1) = q+1$이다.[2]

이상과 같이 선행연구들에서는 유한체 $\mathbf{F}_q$ 우의 자기상반기약다항식들과 $\mathbf{F}_q$의 2차확대체 $\mathbf{F}_{q^2}$ 우의 자기공액상반기약다항식들에 대한 연구가 독립적으로 진행되였으나 그것들사이의 호상관계가 밝혀진것이 없고 특히 $\mathbf{F}_{q^2}$ 우에서 주어진 차수를 가진 자기공액상반기약다항식들전부의 적에 대한 공식은 알려진것이 없다. 그러므로 론문에서는 이미 잘 알려져있는 $\mathbf{F}_q$ 우의 자기상반기약다항식에 대한 결과들로부터 $\mathbf{F}_{q^2}$ 우의 자기공액상반기약다항식에 대한 결과들을 유도하는데 리용할 목적으로 뫼비우스의 함수의 구조와 $\mathbf{F}_q$ 우의 기약다항식이 $\mathbf{F}_{q^2}$ 우의 기약다항식들의 적으로 분해될 때 인수들의 구조를 해명하는 방법으로 $\mathbf{F}_q$와 $\mathbf{F}_{q^2}$ 우의 기약다항식들전부의 개수들사이의 관계, $\mathbf{F}_q$ 우의 자기상반기약다항식들과 $\mathbf{F}_{q^2}$ 우의 자기공액상반기약다항식들전부의 개수들사이의 관계를 밝히고 주어진 차수를 가진 자기공액상반기약다항식들전부의 적에 대한 공식을 얻으려고 한다.

보조정리 1 d가 홀수일 때 $\mu(2d) = -\mu(d)$이다.

증명 우선 $d=1$이면

$$\mu(d) = \mu(1) = 1,\ \mu(2d) = \mu(2) = -1$$

이므로 결과가 성립한다.

다음으로 d가 어떤 씨수의 두제곱으로 완제되면 분명히

$$\mu(d) = \mu(2d) = 0$$

이므로 결과가 성립한다.

또한 d가 서로 다른 k개의 홀씨수들의 적이면

$$\mu(d) = (-1)^k,\ \mu(2d) = (-1)^{k+1} = -\mu(d)$$

이다.(증명끝)

보조정리 2 n이 홀수일 때 다음의 식이 성립한다.

$$N_q(2n) = \frac{1}{2n}\sum_{d|n}\mu(d)(q^{2n/d} - q^{n/d})$$

증명 식 (1)에 의하여

$$N_q(2n) = \frac{1}{2n}\sum_{d|2n}\mu(d)q^{2n/d}$$

이다. 그런데 $2n$의 정의 약수들은 n의 정의 약수들과 그것들의 2배들뿐이다. 그러므로

$$N_q(2n) = \frac{1}{2n}\left(\sum_{d|n}\mu(d)q^{2n/d} + \sum_{d|n}\mu(2d)q^{n/d}\right)$$

이다. 따라서 보조정리 1에 의하여

$$N_q(2n)=\frac{1}{2n}\left(\sum_{d\mid n}\mu(d)q^{2n/d}-\sum_{d\mid n}\mu(d)q^{n/d}\right)=\frac{1}{2n}\sum_{d\mid n}\mu(d)(q^{2n/d}-q^{n/d})$$

이다.(증명끝)

정리 1 다음의 사실이 성립한다.

$$N_{q^2}(n)=\begin{cases}2N_q(2n)+N_q(n), & 2\nmid n\\ 2N_q(2n), & 2\mid n\end{cases}$$

증명 우선 n이 홀수라고 하자. 그러면 식 (1)과 보조정리 2에 의하여

$$N_{q^2}(n)=\frac{1}{n}\sum_{d\mid n}\mu(d)q^{2n/d}=\frac{1}{n}\left[\sum_{d\mid n}\mu(d)q^{2n/d}-\sum_{d\mid n}\mu(d)q^{n/d}\right]+\frac{1}{n}\sum_{d\mid n}\mu(d)q^{n/d}=$$

$$=\frac{1}{n}\sum_{d\mid n}\mu(d)(q^{2n/d}-q^{n/d})+\frac{1}{n}\sum_{d\mid n}\mu(d)q^{n/d}=2N_q(2n)+N_q(n)$$

이 성립한다.

다음으로 n이 짝수라고 하자. 그러면 $n=2^k\cdot h\,(k\ge 1,\ 2\nmid h)$로 쓸수 있다. 따라서

$$N_{q^2}(n)=\frac{1}{n}\sum_{d\mid n}\mu(d)q^{2n/d},\ N_q(2n)=\frac{1}{2n}\sum_{d\mid 2n}\mu(d)q^{2n/d}$$

이므로

$$\sum_{d\mid 2n}\mu(d)q^{2n/d}=\sum_{d\mid n}\mu(d)q^{2n/d}$$

이 성립한다는것을 증명하면 된다. 그런데

$$\sum_{d\mid 2n}\mu(d)q^{2n/d}=\sum_{d\mid n}\mu(d)q^{2n/d}+\sum_{\substack{d\mid 2n\\ d\nmid n}}\mu(d)q^{2n/d}$$

이고 $d\mid 2n,\ d\nmid n$이면 $2^2\mid d$이므로 $\mu(d)=0$이다. 따라서 웃식의 오른변의 둘째 항은 0이다.(증명끝)

보조정리 3 $g(x)$를 $\mathbf{F}_{q^2}$우의 n차기약다항식이라고 하자. 이때 $g(x)=\overline{g(x)}$이면 $g(x)$는 $\mathbf{F}_q$우의 기약다항식이고 $g(x)\ne\overline{g(x)}$이면 $f(x):=g(x)\overline{g(x)}$는 $\mathbf{F}_q$우의 $2n$차기약다항식이다.

증명 $g(x)$는 그것의 분해체에서 다음과 같이 표시된다.

$$g(x)=(x-\beta)(x-\beta^{q^2})\ \cdots\ (x-\beta^{q^{2n-2}})$$

그러므로

$$\overline{g(x)}=(x-\beta^q)(x-\beta^{q^3})\ \cdots\ (x-\beta^{q^{2n-1}})$$

이다. 따라서 $g(x)=\overline{g(x)}$이면 $g(x)$의 매 결수 a_i에 대하여 $a_i^q=a_i$이므로 $g(x)\in\mathbf{F}_q[x]$이다.

또한 $g(x)\ne\overline{g(x)}$이면 원소 $\beta,\ \beta^q,\ \beta^{q^2},\ \cdots,\ \beta^{q^{2n-2}},\ \beta^{q^{2n-1}}$들은 모두 서로 다르므로 $f(x)$는 $\mathbf{F}_q$우에서 기약이다.(증명끝)

보조정리 4 $f(x)$가 $\mathbf{F}_q$우의 $2n$차기약다항식이면 $\mathbf{F}_{q^2}$우의 어떤 n차기약다항식 $g(x)$

가 존재하여

$$f(x)=g(x)\overline{g(x)}$$

로 표시할수 있고 이때 $g(x)\neq\overline{g(x)}$ 이다.

증명 $f(x)$ 는 그것의 분해체에서 다음과 같이 표시된다.

$$f(x)=(x-\beta)(x-\beta^{q})(x-\beta^{q^2})\ \cdots\ (x-\beta^{q^{2n-1}})$$

그러므로

$$g(x):=(x-\beta)(x-\beta^{q^2})\ \cdots\ (x-\beta^{q^{2n-2}})$$

으로 놓으면

$$\overline{g(x)}=(x-\beta^{q})(x-\beta^{q^3})\ \cdots\ (x-\beta^{q^{2n-1}})$$

이고 $f(x)=g(x)\overline{g(x)}$ 이다. 이때 분명히 $g(x)$ 와 $\overline{g(x)}$ 는 $\mathbf{F}_{q^2}$ 우의 n 차기약다항식들이다. 그런데 $g(x)=\overline{g(x)}$ 라고 가정하면 기약다항식 $f(x)$ 가 중복인수를 가지게 되므로 모순된다.(증명끝)

보조정리 5 $f(x)(\in\mathbf{F}_q[x])$ 가 $2n$ 차자기상반기약다항식이고 $f(x)=g(x)\overline{g(x)}$ 는 $f(x)$ 의 보조정리 4에서와 같은 표시라고 하자. 이때 n 이 홀수이면 $g(x)$ 와 $\overline{g(x)}$ 는 둘 다 자기공액상반이고 서로 상반이며 n 이 짝수이면 $g(x)$ 와 $\overline{g(x)}$ 는 둘 다 자기상반이고 서로 공액상반이다.

증명 $f(x)^*=g(x)^*\cdot\overline{g(x)^*}=g(x)\cdot\overline{g(x)}=f(x)$ 이므로 $g(x)=g(x)^*$ 이거나 $g(x)=\overline{g(x)^*}$ 이다.

우선 n 이 홀수라고 하면 $g(x)=g(x)^*$ 로 될수 없다. 그것은 $g(x)=g(x)^*$ 이라고 가정하면 $n\geq 3$ 일 때에는 자기상반기약다항식의 차수가 짝수라는데 모순되며 $n=1$ 일 때에는 q 가 짝수이면 $g(x)=x+1$, q 가 홀수이면 $g(x)=x\pm 1$ 로서 $f(x)$ 가 기약이라는데 모순되기때문이다. 따라서 $g(x)$ 와 $\overline{g(x)}$ 는 자기공액상반다항식들이며 $g(x)^*=\overline{g(x)}$ 이므로 따라서 서로 상반이다.

다음으로 n 이 짝수라고 하면 $g(x)=\overline{g(x)^*}$ 로 될수 없다. 그것은 자기공액상반기약다항식의 차수가 홀수이기때문이다. 그러므로 $g(x)$ 와 $\overline{g(x)}$ 는 자기상반다항식들이며 $\overline{g(x)}=\overline{g(x)^*}$ 이므로 따라서 서로 공액상반이다.(증명끝)

이 보조정리의 거꿀도 성립한다.

보조정리 6 $g(x)(\in\mathbf{F}_{q^2}[x])$ 를 n 이 $n\geq 3$ 인 홀수이면 n 차자기공액상반기약다항식이고 n 이 짝수이면 n 차자기상반기약다항식이라고 하자. 그러면 $g(x)\neq\overline{g(x)}$ 이고 $f(x):=g(x)\overline{g(x)}$ 는 $\mathbf{F}_q$ 에 기초한 $2n$ 차자기상반기약다항식이다.

증명 $g(x)=\overline{g(x)}$ 라고 가정하자. 그러면 n 이 $n\geq 3$ 인 홀수인 경우 $\overline{g(x)^*}=g(x)=\overline{g(x)}$ 로부터 $g(x)^*=g(x)$ 가 성립하는데 이것은 자기상반기약다항식의 차수는 짝수라는데 모순된다. 그리고 n 이 짝수인 경우에는 $g(x)=g(x)^*=\overline{g(x)^*}$ 가 성립하는데 이것은 자기공액상반기약다항식의 차수가 홀수라는데 모순된다. 따라서 $g(x)\neq\overline{g(x)}$ 이다. 그런데 $f(x)^*=g(x)^*\cdot\overline{g(x)^*}=g(x)\cdot\overline{g(x)}=f(x)$ 이다. 그러므로 보조정리 3에 의하여 $f(x)$ 는 $\mathbf{F}_q$ 에 기초한

$2n$ 차자기상반기약다항식이다.(증명끝)

$g(x)(\in \mathbf{F}_{q^2}[x])$ 를 1차자기공액상반기약다항식이라고 하자. 이때 $g(x)=\overline{g(x)}$ 이면 $g(x)=\overline{g^*(x)}=\overline{g(x)}$ 이므로 $g(x)$ 는 자기상반다항식이고 보조정리 5의 증명에서와 같이 하면 q 가 짝수일 때 $g(x)=x+1$, q 가 홀수일 때 $g(x)=x\pm 1$ 로서 $\mathbf{F}_q$ 우의 다항식이라는것을 알수 있다. 그리고 $g(x)\neq\overline{g(x)}$ 인 경우에는 보조정리 6의 증명에서와 같이 하면 $f(x):=g(x)\overline{g(x)}$ 는 $\mathbf{F}_q$ 에 기초한 2차자기상반기약다항식이라는것을 알수 있다.

이상의 사실들과 공식 (2), (4)로부터 다음의 정리가 성립한다.

정리 2 $n\geq 2$ 이면

$$\mathrm{NSRIM}_q(2n)=\begin{cases}\dfrac{\mathrm{NSCRIM}_{q^2}(n)}{2} & (2\nmid n\text{인 경우})\\ \dfrac{\mathrm{NSRIM}_{q^2}(n)}{2} & (2\mid n\text{인 경우})\end{cases}$$

이고

$$\mathrm{NSCRIM}_{q^2}(1)=\begin{cases}2\mathrm{NSRIM}_q(2)+2 & (2\nmid q\text{인 경우})\\ 2\mathrm{NSRIM}_q(2)+1 & (2\mid q\text{인 경우})\end{cases}$$

이다.

정리 3 n이 3이상의 홀수이면

$$\mathrm{PSCRIM}_{q^2}(n)=\prod_{d\mid n}\left(\frac{x^{q^{n/d}+1}-1}{x^{1+e_q}-1}\right)^{\mu(d)}$$

이고

$$\mathrm{PSCRIM}_{q^2}(1)=x^{q+1}-1\ \mathrm{PSCRIM}_{q^2}(1)=x^{q+1}-1$$

이다.

증명 $n\geq 3$ 일 때 $\mathbf{F}_q$ 우의 매 $2n$ 차자기상반기약다항식은 $\mathbf{F}_{q^2}$ 우의 서로 다른 두 n 차자기공액상반기약다항식의 적이므로 정리 2와 식 (3)으로부터 첫식이 나온다. 또한 식 (3)으로부터 $\mathbf{F}_q$ 우의 2차자기상반기약다항식들전부의 적은

$$\frac{x^{q+1}-1}{x^{1+e_q}-1}$$

이고 이것은 $\mathbf{F}_{q^2}$ 우의 $g(x)\neq\overline{g(x)}$ 인 1차자기공액상반기약다항식들전부의 적이다. 그런데 $\mathbf{F}_{q^2}$ 우의 $g(x)=\overline{g(x)}$ 인 1차자기공액상반기약다항식은 q 가 짝수일 때 $g(x)=x+1$ 뿐이고 q 가 홀수일 때에는 $g(x)=x\pm 1$ 뿐이다. 그러므로 그 적은 $x^{1+e_q}-1$ 이고 따라서 정리의 둘째 식이 나온다.(증명끝)

참 고 문 헌

[1] **김일성**종합대학학보 수학, 67, 1, 5, 주체110(2021).
[2] A. Boripan et. al.; arXiv: 1801.08842[math.RA], 2018.
[3] R. Lidl, H. Niederreiter; Finite Fields, Cambridge University Press, 83～96, 2003.
[4] H. Meyn; Appl. Algebra Engrg. Comm. Comput., 1, 43, 1990.
[5] J. L. Yucas, G. L. Mullen; Des. Codes Cryptogr., 33, 275, 2004.

주체110(2021)년 3월 5일 원고접수

The Relation between the Irreducible Polynomials over a Finite Field and Its Quadratic Extension

Kim Ryul

In this paper we establish the relation between the numbers of irreducible polynomials over a finite field $\mathbf{F}_q$ and its quadratic extension $\mathbf{F}_{q^2}$ and one between the number of self-reciprocal irreducible polynomials over $\mathbf{F}_q$ and the number of self-conjugate-reciprocal irreducible polynomials over $\mathbf{F}_{q^2}$. We also present a formula for the product of all self-conjugate-reciprocal irreducible polynomials in $\mathbf{F}_{q^2}[x]$ of fixed degree.

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