Normal high order elements in cyclotomic finite field extensions

Roman Popovych
(Polytechnic National University, Lviv, Ukraine)
E-mail: rombp07@gmail.com

Ruslan Skuratovskii
(Kiev, MAUP)
E-mail: ruslcomp@mail.ru

Let q be a power of a prime number p, and F_q be a finite field with q elements. For any integer m, a normal basis of F_{q^m} over F_q is a basis of the form $\{\alpha, \alpha^q, ..., \alpha^{q^{m-1}}\}$ for some $\alpha \in F_{q^m}$ [4]. In this case the element $\alpha \in F_{q^m}$ is called normal over F_q [1, 3].

Let $r = 2n+1$ be a prime number coprime with q. Let q be a primitive root modulo r, that is the multiplicative order of q modulo r equals to $r-1$. Set $F_q(\theta) = F_{q^{r-1}} = F_q[x]/\Phi_r(x)$, where $\Phi_r(x) = x^{r-1} + ... + x + 1$ is the r-th cyclotomic polynomial and $\theta \equiv x \ (\mathrm{mod}\Phi_r(x))$. It is clear that the equality $\theta^r = 1$ holds. We have the following tower of finite fields: $F_q \subset F_{q^n} \subset F_{q^{2n}}$.

Theorem 1. *Let b be such element of the field F_q that $2nb \neq 1(\bmod p)$. Then the following statements are true:*
(a) element $\theta + b \in F_{q^{2n}}$ is normal over F_q;
(b) element $\theta + \theta^{-1} + 2b \in F_{q^n}$ is normal over F_q.

Note that for $b = 0$ the order of θ equals only to r. But for $b \neq 0$ the element $\theta + b \in F_{q^{2n}}$ has high order according to [3, Theorem 1 (a), (d)]. Also if $2b = (a^2+1)a^{-1}$ and $b \neq 0$, then the element $\theta + \theta^{-1} + 2b = (\theta^{-f} + a)(\theta^f + a)$ has high order according to [3].

Rerefences

[1] Lidl R., Niederreiter H. *Finite Fields.* – Cambridge: Cambridge University Press, 755 p., 1997.
[2] Mullen G. L., Panario D. *Handbook of finite fields.* – Boca Raton: CRC Press, 1068 p., 2013.
[3] Popovych R. *Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$.* Vol. 18, *Finite Fields Appl.*, P.700-710., 2012.
[4] Skuratovskii R. V. *Finding normal basis of finite field during deterministic polynomial time.* Vol. 25. *Visnuk of Kiev's National University. Mechanics and mathematics.* pp. 49 - 54, 2011.
[5] R. V. Skuratovskii *Structure and minimal generating sets of Sylow 2-subgroups of alternating groups.* Source: https://arxiv.org/pdf/1702.05784.pdf, 2017.