KUMMER EXTENSIONS OF FINITE FIELDS

FLAVIO PERISSINOTTO AND ANTONELLA PERUCCA

Let p be a prime number, denote by $\mathbb{F}_p$ the field with p elements, and fix an algebraic closure $\bar{\mathbb{F}}_p$. Let $K \subseteq \bar{\mathbb{F}}_p$ be the finite field with p^k elements, and let G be a subgroup of $K^\times$. Consider positive integers n, N coprime to p such that n divides N: we denote by ζ_N a root of unity in $\bar{\mathbb{F}}_p$ of order N, and we let $\sqrt[n]{G}$ be the subgroup of $\bar{\mathbb{F}}_p^\times$ consisting of those elements whose n-th power lies in G. If x, y are coprime positive integers, then we write $\mathrm{ord}_x(y)$ for the multiplicative order of y in $(\mathbb{Z}/x\mathbb{Z})^\times$, namely the smallest positive integer z such that $x \mid (y^z - 1)$.

Remark 1. Let ℓ be a prime number, and denote by v_ℓ the ℓ-adic valuation for the non-zero integers. Recall that for every integer $a \geqslant 2$ the following holds: if ℓ is odd and $v_\ell(a-1) \geqslant 1$, or if $\ell = 2$ and $v_2(a-1) \geqslant 2$, then we have

$$v_\ell(a^x - 1) = v_\ell(a-1) + v_\ell(x)\,.$$

Noticing that $\mathrm{ord}_N(p^k) = \mathrm{ord}_N(p)/\gcd(k, \mathrm{ord}_N(p^k))$, we get the following:

$$[K(\zeta_N) : K] = \mathrm{ord}_N(\#K) = \frac{\mathrm{lcm}(k, \mathrm{ord}_N(p))}{k}\,. \tag{1}$$

Theorem 2. *We have*

$$[K(\zeta_N, \sqrt[n]{G}) : K] = \mathrm{ord}_{\mathrm{lcm}(N, \#G\cdot n)}(\#K) = \frac{\mathrm{lcm}(k, \mathrm{ord}_N(p), \mathrm{ord}_{\#G\cdot n}(p))}{k}\,. \tag{2}$$

Proof. The finite field $K(\zeta_N, \sqrt[n]{G})$ is the smallest subextension of $\bar{\mathbb{F}}_p/K$ such that the size of its multiplicative group is divisible by $\mathrm{lcm}(N, \#G \cdot n)$, so it is the field $K(\zeta_{\mathrm{lcm}(N,\#G\cdot n)})$. We conclude by (1). □

We are going to make the quantities in Theorem 2 more explicit. For $\ell \neq p$ notice that $\mathrm{ord}_\ell(p)$ divides $\ell - 1$ and that by (1) we have

$$V_\ell(p) := v_\ell(p^{\mathrm{ord}_\ell(p)} - 1) = v_\ell(p^{\ell-1} - 1)\,.$$

Theorem 3. *If q is any prime number, then we have*

$$v_q(\mathrm{ord}_N(p)) = \begin{cases} \max\Big(v_q(N) - V_q(p), M_{q,N}(p)\Big) & \text{if } q \neq 2 \\ \max\Big(v_2(\mathrm{ord}_{2^{v_2(N)}}(p)), M_{2,N}(p)\Big) & \text{if } q = 2\,, \end{cases}$$

where we set

$$M_{q,N}(p) := \max\{0\} \cup \{v_q(\mathrm{ord}_\ell(p)) \ : \ \ell \text{ prime number}, \ell \mid N, \ell \neq q\}\,.$$

Proof. Consider the prime decomposition $N = \prod_{\ell | N} \ell^E$, recalling that $\ell \neq p$. Noticing that $\mathrm{ord}_N(p) = \mathrm{lcm}_\ell(\mathrm{ord}_{\ell^E}(p))$, it suffices to observe that by Remark (1) we have

$$\mathrm{ord}_{\ell^E}(p) = \begin{cases} \mathrm{ord}_\ell(p) \cdot \ell^{\max(E - V_\ell(p), 0)} & \text{if } \ell \neq 2 \\ 2^{\max(E - v_2(p-1), 0)} & \text{if } \ell = 2, p \equiv 1 \bmod 4 \\ 2^{\max(E - v_2(p+1), \min(1, E-1))} & \text{if } \ell = 2, p \equiv 3 \bmod 4\,. \end{cases}$$

□

Suppose w.l.o.g. that $(p^k - 1) \mid N$ and define $N' := \mathrm{lcm}(N, \#G \cdot n)$. Then we have:

$$[K(\zeta_N, \sqrt[n]{G}) : K(\zeta_N)] = \frac{\mathrm{ord}_{N'}(p)}{\mathrm{ord}_N(p)}\,.$$

As N' and N have the same prime divisors, by Theorem 3 for any prime number q the non-negative integer $v_q([K(\zeta_N, \sqrt[n]{G}) : K(\zeta_N)])$ equals

(3)
$$\begin{cases} \max\Big(v_q(N') - V_q(p), M_{q,N}(p)\Big) - \max\Big(v_q(N) - V_q(p), M_{q,N}(p)\Big) & \text{if } q \neq 2 \\ \max\Big(v_2(\mathrm{ord}_{2^{v_2(N')}}(p)), M_{2,N}(p)\Big) - \max\Big(v_2(\mathrm{ord}_{2^{v_2(N)}}(p)), M_{2,N}(p)\Big) & \text{if } q = 2\,. \end{cases}$$

In particular, q does not divide $[K(\zeta_N, \sqrt[n]{G}) : K(\zeta_N)]$ if $v_q(N') = v_q(N)$, which happens for example if $q \nmid n$. Notice that, for $q \mid (p^k - 1)$, by Remark 1 we have $v_q(N) \geqslant V_q(p) + v_q(k)$ hence in the definition of $M_{q,N}(p)$ we could restrict to $\ell \nmid (p^k - 1)$.

Formula (3) allows us to compute at once all Kummer degrees $[K(\zeta_N, \sqrt[n]{G}) : K(\zeta_N)]$ such that the prime divisors of N belong to some fixed finite set (Example 5 shows that we cannot drop this assumption) because $M_{q,N}(p)$ depends on N only through the set of its prime divisors.

Example 4. Let $K = \mathbb{F}_{5^2}$, and let $\#G = 4$. For all non-negative integers A, B, a, b such that $A \geqslant a$ and $B \geqslant b$ we have

$$[K(\zeta_{2^A 17^B}, \sqrt[2^a 17^b]{G}) : K(\zeta_{2^A 17^B})] = 2^{\max(0, a - A + 2, a - 4)}\,.$$

Indeed, the degree is a power of 2 because $17 \nmid \#G$. We apply (3), noticing that $v_2(N) = \max(3, A)$, $v_2(N') = \max(3, A, a + 2)$, and that $v_2(\mathrm{ord}_{17}(5)) = 4$.

Example 5. Let $q \mid (p - 1)$ be an odd prime number such that $V_q(p) = 1$, e.g. $V_3(7) = 1$. For any prime number $\ell \neq p, q$ we have

$$[\mathbb{F}_p(\zeta_{\ell q}, \sqrt[q]{\mathbb{F}_p^\times}) : \mathbb{F}_p(\zeta_{\ell q})] = \frac{\mathrm{ord}_{\ell q(p-1)}(p)}{\mathrm{ord}_{\ell(p-1)}(p)} = 1 \qquad \Leftrightarrow \qquad q \mid \mathrm{ord}_\ell(p)\,.$$