IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS AS FACTORS OF SPARSE POLYNOMIALS

JARO EICHLER

CONTENTS

Introduction

Let $\mathbb{F}_{q^k}$ be a finite field with q^k elements of characteristic p and let Y/X be a cover of curves over $\mathbb{F}_{q^k}$. It is of interest to count $\mathbb{F}_{q^k}$-rational points on X that have a point of given degree d in their fiber in Y.

One application is described in [2]:

Theorem 0.1. *Given a prime power $q > 61$ that is not a power of 4, an integer $k \geq 18$, coprime polynomials $f_0, f_1 \in \mathbb{F}_{q^k}[t]$ of degree at most two and an irreducible degree d factor h of $f_0 t^q - f_1$, the discrete logarithm problem, i.e. finding solutions to $n^l = m$ in $\mathbb{F}_{q^{kd}} \cong \mathbb{F}_{q^k}[t]/(h)$ can be solved in expected time $q^{\log_2 d + \mathcal{O}(k)}$.*

For $d = q-1$ we can always find a polynomial that can be used for the theorem. Indeed, according to Kummer theory there exists an $a_0 \in \mathbb{F}_{q^k}$ such that $t^{q-1} - a_0$ is irreducible. Let $p \neq 2, 3$. We will look at another family of polynomials given by the equation

$$f = t^{q+2} + t^2 + a^2 t + a.$$

This polynomial turns out to have Galois group $G = \mathrm{S}_{q+2}$.

To a parameter $a_0 \in \mathbb{F}_{q^k}$ we can assign the element $\mathrm{Frob}_{a_0} \in G$. Its cycle lengths, acting on the zeroes of f, amounts to the degree of irreducible factors of $f(t, a_0)$. The Chebotarev density theorem then says that the amount of points with a given cycle type has density $\frac{c}{|G|}$. Using an effective version, in our particular case we will get the result:

Proposition 0.2. *There exists $k \in \mathcal{O}(q)$ and $a_0 \in \mathbb{F}_{q^k}$ such that $f(t, a_0)$ has an irreducible factor of degree d for any $1 \leq d \leq q+2$.*

Calculations in Sagemath suggest that the bound on k is not precise enough. For small q, i.e. $q < 100$, it is enough to choose $k = 2$.

One approach for giving a better bound is to find polynomials with smaller Galois groups. Noting that at the same time this restricts the possible degrees of irreducible factors. An example for such a polynomial was found by Abhyankar, he showed that the Galois group of

$$g = t^{q+1} + at + 1.$$

is $\mathrm{PSL}_2(\mathbb{F}_q)$. Without any restriction on the characteristic we get:

Proposition 0.3. *There exists $k \in \mathcal{O}(1)$ and $a_0 \in \mathbb{F}_{q^k}$ such that $g(t, a_0)$ has an irreducible factor of degree d for*

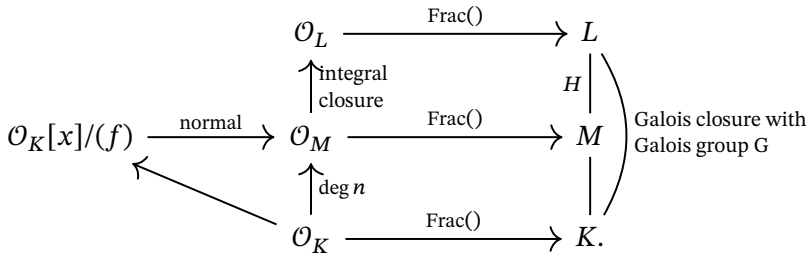
- $d = p$
- $\begin{cases} d \mid \frac{q-1}{2} & p \neq 2 \\ d \mid q-1 & p = 2 \end{cases}$
- $\begin{cases} d \mid \frac{q+1}{2} & p \neq 2 \\ d \mid q+1 & p = 2. \end{cases}$

Acknowledgement. I would like to express my sincere gratitude to my supervisor Prof. Jakob Stix for the opportunity to write this thesis under him, for his guidance, and interesting discussions about the topic. Besides my advisor, I would like to thank everyone who took their time to share their insights about the subject and answered many questions of mine. Especially Nithi Rungtanapirom for offering to be the second reader of this thesis. Last but not least, I would like to thank my family and friends for their support.

1. Local calculations with Galois groups

Let K be a global field, i.e. a number field or a function field over a finite field. Given a separable, irreducible polynomial f of degree n over K we want to calculate its Galois group, by that we mean the Galois group of its splitting field. Let $\mathcal{O}_K$ be the ring of integers of K. Since the transformation $a^n f\left(\frac{x}{a}\right)$ does not change the Galois group, we may assume f to be monic and defined over $\mathcal{O}_K$.

Throughout this section we fix the following notation



The Galois group G acts freely on the roots of f, so there is an embedding $G \subseteq \mathrm{S}_n$. Note that the action is described purely by the field extensions. Namely by letting G act on $G/H = \mathrm{Hom}_K(M, \overline{K}) = \mathrm{Hom}_K(M, L)$ with $\overline{K}$ being the algebraic closure of K. This corresponds to the action on the roots upon a choice of an embedding into the algebraic closure. This action commutes with passing to local fields and specializations. Our goal is to describe G by such local calculations.

Lemma 1.1. *Since f is irreducible, $G \subseteq \mathrm{S}_n$ is transitive.*

Proof. Given zeroes α and α' of f, we get an isomorphism $K(\alpha) \to K(\alpha')$. This map extends to an automorphism of the normal closure. □

Definition 1.2. Let $\alpha_1, \dots, \alpha_n$ be the zeroes of f with multiplicity. The discriminant of f is

$$\Delta_f = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in K.$$

Remark 1.3. The discriminant is zero if and only if f is inseparable.

Remark 1.4. The discriminant equals the resultant of f with its derivative up to a sign

$$\Delta_f = (-1)^{\frac{n(n-1)}{2}} \mathrm{res}(f, f').$$

Furthermore the resultant can be calculated via division with remainder in the following sense. Let $a \in K$, f, g, h be polynomials over K and c the top coefficient of g, then

$$\begin{aligned}
\mathrm{res}(f, a) &= \mathrm{res}(a, f) = a^{\deg(f)} \\
\mathrm{res}(f, g) &= (-1)^{\deg(f)\deg(g)} \mathrm{res}(g, f) \\
\mathrm{res}(f, g) &= c^{\deg(f) - \deg(f - hg)} \mathrm{res}(f - hg, g).
\end{aligned}$$

Lemma 1.5. *Assuming* $\mathrm{char}(K) \neq 2$*, the discriminant is a square if and only if $G \subseteq \mathrm{A}_n$.*

Proof. The discriminant is a square if and only if $\prod_{i<j}(\alpha_i - \alpha_j)$ is invariant under G. The largest subgroup of S_n fixing this term is A_n. □

If not stated otherwise, by a prime in the ring of integers of a field, a codimension one prime ideal is meant. Since $\mathcal{O}_M/\mathcal{O}_K$ and $\mathcal{O}_L/\mathcal{O}_K$ are finite extensions of Dedekind domains, there is a decomposition of primes of $\mathcal{O}_K$ in $\mathcal{O}_M$ and $\mathcal{O}_L$. Given $p = \prod_{q|p} q^{\mathrm{e}_q}$, let e_q denote the ramification index and let $\mathrm{f}_q = [\kappa(q) : \kappa(p)]$ denote the inertia degree. A prime p is said to be unramified if $\mathrm{e}_p = 1$, ramified if $\mathrm{e}_p > 1$, tamely ramified if p is ramified and $p \nmid \mathrm{e}_p$, wildly ramified if $p \mid \mathrm{e}_p$.

By $q \mid p$ we denote primes that lie above p and let $\{q \mid p\}$ denote the set of all of those.

Remark 1.6. For $\mathcal{O}_M$ we have the equation

$$\sum_{q|p} \mathrm{e}_q \mathrm{f}_q = n.$$

And since L is Galois, all primes $\{q \mid p\}$ over a given prime p are conjugate, so for $\mathcal{O}_L$ we get

$$\#\{q \mid p\} \cdot \mathrm{e}_p \mathrm{f}_p = \#G.$$

Definition 1.7. Let p be a prime in $\mathcal{O}_K$ and $q \mid p$ a prime above p. The subgroup

$$\mathcal{D}_{q|p} = \{g \in G \mid gq = q\}$$

is called the decomposition group and

$$\mathcal{I}_{q|p} = \{g \in \mathcal{D}_{q|p} \mid g = id \text{ in } \kappa(q)\}$$

is called the inertia group. Both are well defined up to conjugation on $\{q \mid p\}$. We denote by $\mathcal{D}_p$ and $\mathcal{I}_p$ a representative.

Let $\mathcal{O}_K$ be the ring of integers of a global field K. Given a prime p in $\mathcal{O}_K$, we get a discrete valuation ν_p and a norm on K by taking $e^{-\nu_p}$. The completion of K with respect to that norm, denoted by K_p, is called a (non-Archimedean) local field. This coincides with the fraction field of the completion $\widehat{\mathcal{O}_K}$ of $\mathcal{O}_K$, i. e. $\varprojlim_n \mathcal{O}_K/p^n$.

Proposition 1.8. *Let K be a local field with valuation ν_K and L/K a finite extension. Then ν_K can be uniquely extended to L and L is complete. The extension is given by*

$$\nu_L = \frac{1}{[L : K]} \nu_K(\mathcal{N}_{L/K})$$

where $\mathcal{N}_{L/K}$ denotes the norm.

Proof. [4, Theorem 4.8] □

Lemma 1.9. *Let L/K be an extension of local fields with extension of valuations ν_L/ν_K. Then ν_L has image $\frac{1}{\mathrm{e}}\mathrm{im}(\nu_K)$, where* e *denotes the ramification index.*

Proof. Choose uniformizers π_K, π_L of K, L and write $\pi_K = u\pi_L^{\mathrm{e}}$ for some unit u. We have

$$\nu_K(\pi_K) = \nu_L(\pi_K) = \nu_L(u\pi_L^e) = e.$$

Since $\nu_K(\pi_K)$ and $\nu_L(\pi_L)$ generate their respective valuation group, we get the claim. □

Given an extension of global fields L/K with rings of integers $\mathcal{O}_L/\mathcal{O}_K$ and a prime p we get

$$\mathcal{O}_L \otimes_{\mathcal{O}_K} \widehat{\mathcal{O}_K} = \mathcal{O}_L \otimes_{\mathcal{O}_K} \varprojlim_n \mathcal{O}_K/p^n = \varprojlim_n \mathcal{O}_L/p^n\mathcal{O}_L = \varprojlim_n \mathcal{O}_L/\prod_{q|p} q^{n\mathrm{e}_q} = \prod_{q|p} \widehat{\mathcal{O}_{L_q}}, \tag{1}$$

where $\widehat{\mathcal{O}_{L_q}}$ denotes the completion w. r. t. the prime q. Looking at the fraction fields we then have an isomorphism of étale K_p-algebras

$$L \otimes_K K_p = \prod_{q|p} L_q. \tag{2}$$

The dimension of an étale K-algebra is invariant under base change to a field extension. Hence, we have

$$[L : K] = \dim_{K_p} L \otimes_K K_p = \sum_{q|p} [L_q : K_p]. \tag{3}$$

In the particular case of L/K being Galois this gives rise to the following lemma

Lemma 1.10. *Let q be a prime above p in $\mathcal{O}_L$. The Galois group of the extension of local fields L_q/K_p is given by $\mathcal{D}_p$. This commutes with the action on the roots of f.*

Proof. Since a finite field extension of a complete field is complete, L_q is the splitting field of f, thus L_q is Galois. An automorphism $g \in G$ is continuous with respect to the norms given by q and gq. So there is an induced isomorphism on the completions $L_q \to L_{gq}$. This gives an embedding

$$\mathcal{D}_p \hookrightarrow \mathrm{Gal}(L_q/K_p)$$

which commutes with the choice of an embedding into the algebraic closure $\overline{K}_p$. By (1) all L_q have the same degree $\mathrm{e}_p\mathrm{f}_p$. Since $\mathcal{D}_p$ is the stabilizer of the transitive action on $\{q \mid p\}$, we have

$$\frac{|G|}{|\{q \mid p\}|} = |\mathcal{D}_p| \leq |\mathrm{Gal}(L_q : K_p)| = \frac{|G|}{|\{q \mid p\}|}.$$

Hence the above map is surjective. □

In particular we now have different ways to look at the ramification and decomposition of primes. We can either look at the global field or, according to (1) restrict to the local field.

Lemma 1.11. *The sequence*

$$1 \to \mathcal{I}_p \to \mathcal{D}_p \to \mathrm{Gal}(\kappa(q)/\kappa(p)) \to 1$$

is exact.

Proof. The inertia group is the kernel per definition, so we need to show the surjectivity of $\mathcal{D}_p \to \mathrm{Gal}(\kappa(q)/\kappa(p))$. Let $\alpha \in \mathcal{O}_L$ be a generator of $\kappa(q)/\kappa(p)$ and let $h = \prod_{g \in \mathcal{D}_p}(t - g(\alpha)) \in L^{\mathcal{D}_p}$ be its characteristic polynomial. Since $L^{\mathcal{D}_p}/K$ has trivial residue field extension, h reduces to a polynomial $\bar{h} \in \kappa(p)[t]$. With α being a root of $\bar{h}$, so is $\mathrm{Frob}_{\kappa(p)}(\alpha)$. Hence, some $g \in \mathcal{D}_p$ reduces to the generator $\mathrm{Frob}_{\kappa(p)}$. □

Remark 1.12. The ramification index is given by the order of the inertia group $\#\mathcal{I}_p = \mathrm{e}_p$. This follows from the above exact sequence

$$|\mathcal{I}_p| = \frac{|\mathcal{D}_p|}{|\mathrm{Gal}(\kappa(q)/\kappa(p))|} = \frac{|G|}{\mathrm{f}_p \cdot |\{q \mid p\}|} = \mathrm{e}_p.$$

The Frobenius element gives rise to a special subset in $\mathcal{D}_p$.

Definition 1.13. Let p be a prime in K. Denote by $\mathrm{Frob}_p \subseteq \mathrm{Gal}(L/K)$ the preimage of the Frobenius element $\mathrm{Frob}_{\kappa(p)}$ under the surjection $\mathcal{D}_p \twoheadrightarrow \mathrm{Gal}(\kappa(q)/\kappa(p))$. For p unramified this is just one element, also denoted by Frob_p.

Lemma 1.14 (Dedekind's Theorem)**.** *Let p be unramified and let $f_1, \dots, f_r$ denote the inertia degrees of the primes $q_1, \dots, q_r$ over p in $\mathcal{O}_M$. Then* Frob_p *has cycle type $(f_1, \dots, f_r)$ in $\mathcal{D}_p$, i. e. it is a product of disjoint cycles of corresponding length.*

Proof. Being unramified in p is equivalent to the vanishing of $\mathcal{I}_p$, so the exact sequence from lemma 1.11 results in $\mathcal{D}_p \cong \mathrm{Gal}(\kappa(q)/\kappa(p))$. Since L is built by successive adding of roots of f, so is $\kappa(q)$. In other words, $\kappa(q)$ is the splitting field of f over $\kappa(p)$. Restricted to $\kappa(q_i)$ the Frobenius is a cycle of length f_i. □

Definition 1.15. The normal subgroup $\mathcal{I}_p^w = \ker(\mathcal{D}_p \to \mathrm{Aut}(\mathcal{O}_{L_q}/q^2))$ is called the wild inertia group, again well defined on $\{q \mid p\}$ up to conjugation. The quotient $\mathcal{I}_p^t = \mathcal{I}_p/\mathcal{I}_p^w$ is called the tame inertia group.

Lemma 1.16. *Let $q \mid p$. The sequence*

$$1 \to \mathcal{I}_p^w \to \mathcal{I}_p \to \mathcal{I}_p^t \to 1$$

is exact with $\mathcal{I}_p^w$ a p-group and $\mathcal{I}_p^t \cong \mu_{\mathrm{e}_p}(\kappa(q))$. Furthermore $\mu_{\mathrm{e}_p}(\kappa(q))$ is cyclic of order the prime to $\mathrm{char}\kappa(p)$ *part of* e_p.

Proof. The sequence is exact by definition. We may look at the extension of local rings for the ramification, so assume $\mathcal{O}_L/\mathcal{O}_K$ to be an extension of discrete valuation rings with fraction fields L/K. Let $\pi_{\mathcal{O}_L}$ and $\pi_{\mathcal{O}_K}$ be uniformizers and set $e = \mathrm{e}_p$, we have $\pi_{\mathcal{O}_K} = u\pi_{\mathcal{O}_L}^e$ for some unit u. For $g \in \mathcal{I}_p$ write $g(\pi_{\mathcal{O}_L}) = \theta_g \pi_{\mathcal{O}_L}$ with $\theta_g \in \mathcal{O}_L^\times$. Then we get

$$\pi_{\mathcal{O}_K} = g(\pi_{\mathcal{O}_K}) = g(u\pi_{\mathcal{O}_L}^e) = g(u)g(\pi_{\mathcal{O}_L})^e = g(u)\theta_g^e \pi_{\mathcal{O}_L}^e = \frac{g(u)}{u}\theta_g^e \pi_{\mathcal{O}_K}.$$

Since g acts trivial on $\kappa(q)$, we have a group homomorphism

$$\theta : \mathcal{I}_p \to \mu_e(\kappa(q)), g \mapsto \theta_g$$

with kernel $\mathcal{I}_p^w$. One then shows that the kernel is a p-group. (cf. [6, Lemma 09EE]) □

Lemma 1.17. *Let p be a prime in $\mathcal{O}_K$ that is unramified in the extension $R = \mathcal{O}_K[t]/(f)$. Denote by $q_1, \dots, q_r$ the primes above p in R. Then the local rings R_{q_i} are DVRs. Hence, p is unramified in $\mathcal{O}_M$.*

Proof. Since p is unramified in R, the reduction $\bar{f} \in \kappa(p)$ is separable. Write

$$\bar{f} = \prod \bar{f}_i \in \kappa(p)[t]$$

as a decomposition of irreducible factors with $\mathrm{f}_i \in \mathcal{O}_K[t]$ that reduce to $\bar{f}_i$. Take a uniformizer π of the local ring $\mathcal{O}_{K,p}$ and denote by m_i the maximal ideal of R_{q_i}. Upon the right choice of the numbering, we have

$$m_i = (\pi, f_i) = (\pi, f_i \underbrace{\prod_{j \neq i} f_j}_{\in R_{q_i}^\times}) = (\pi).$$

By [5, Proposition 2], the local ring R_{q_i} is a DVR since it is principle. □

Remark 1.18. Since the ring extensions we are looking at are of finite type and the residue fields are perfect, we see that our definition of unramified coincides with the definition of an unramified morphism of rings. (cf. [6, Section 00US])

Lemma 1.19 (Abhyankar's lemma). *Let M/K be a finite, separable extension of local fields with ramification index e. Assume $M = M_1M_2$ to be the compositum of two intermediate fields with ramification indices e_1 and e_2. If at least one of those extensions is tamely ramified, then*

$$e = \mathrm{lcm}(e_1, e_2).$$

Proof. The proof in [7, Theorem 3.9.1] for function fields works as well in this case. □

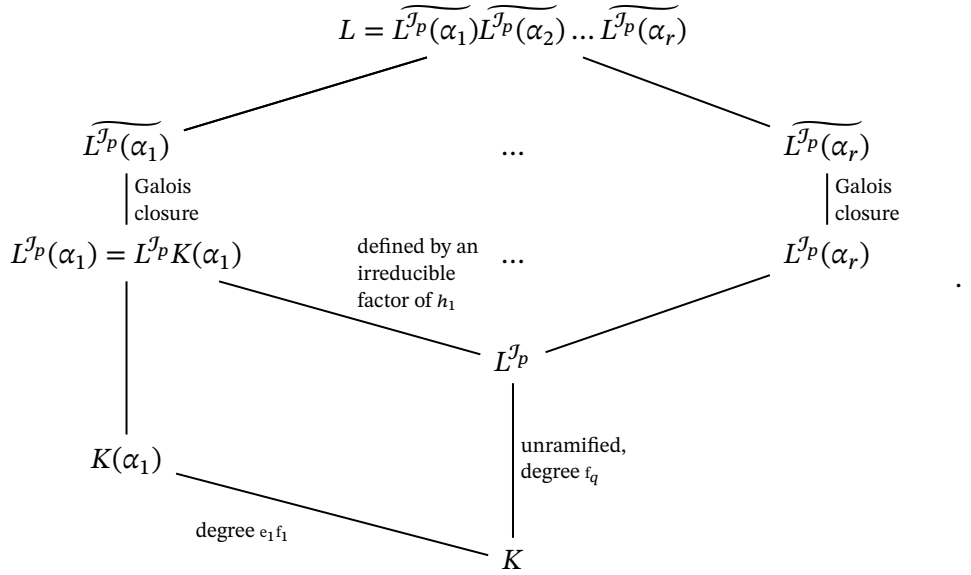
Remark 1.20. Similar to Dedekind's theorem (lemma 1.14) we can assign a cycle type to tamely ramified primes. Let p be a prime in $\mathcal{O}_K$ and let $q_1, \dots, q_r$ be the primes above p in $\mathcal{O}_M$. Denote by $e_1, \dots, e_r$ their ramification indices and by $f_1, \dots, f_r$ their inertia degrees. By (2) the polynomial f decomposes into irreducible factors $h_1, \dots, h_r$ of degree $\deg h_i = e_i f_i$ over K_p. So we get an embedding

$$\mathcal{D}_p \subseteq \mathrm{S}_{e_1 f_1} \times \dots \times \mathrm{S}_{e_r f_r} \subseteq \mathrm{S}_n$$

with transitive action on each of those $e_i f_i$ zeroes.

Fix a prime $q \mid p$ in $\mathcal{O}_L$ and a zero α_i of h_i for each i. We are interested in the action of the inertia group on the zeroes of f. Hence, let $K = K_p$ and $L = L_q$. Looking at the fixed field of the inertia

group we have



Note that it is enough to take one zero of each h_i, since the irreducible factors of h_i are already permuted by $\mathcal{D}_p/\mathcal{I}_p$. Since $L/L^{\mathcal{I}_p}$ is totally ramified of degree e_q, every subextension is also totally ramified. Hence, using Abhyankar's lemma (lemma 1.19), we see that the degree of $L^{\mathcal{I}_p}(\alpha_i)/L^{\mathcal{I}_p}$ equals e_i.

So we get an embedding

$$\mathcal{I}_p \subseteq \underbrace{S_{e_1} \times \dots \times S_{e_1}}_{f_1} \times \dots \times S_{e_r}$$

with transitive image under the projection onto each factor.

If all primes above p in $\mathcal{O}_M$ are tamely ramified, they are also tamely ramified in $\mathcal{O}_L$ by Abhyankar's Lemma, so the inertia group $\mathcal{I}_p = \mathcal{I}_P^t$ is cyclic. Hence, any generator has cycle type

$$\underbrace{(e_1) \dots (e_1)}_{f_1} \dots \underbrace{(e_r) \dots (e_r)}_{f_r} \in \mathcal{I}_p.$$

Definition 1.21. Let $f = a_n x^n + \dots + a_0$ be a polynomial and ν a discrete valuation on the coefficients. The lower convex hull of the nodes $(i, \nu(a_i))$ is called the Newton polygon of f.

Lemma 1.22. *Let K be a local field and let f be a polynomial over K. Denote by ν the unique continuation of the valuation on K to the splitting field of f. Given a line segment l in the Newton polygon of f, let $-s_l$ be the slope and d_l the i-distance of l. Then there are exactly d_l roots of f with ν-valuation s_l.*

Proof. [4, Proposition 6.3] □

Lemma 1.23. *If G is both 2-transitive and contains a transposition, then G equals S_n.*

Proof. Let the transposition be given by (ij). For any k, l there is a $\sigma \in G$, such that $\sigma(i) = k$ and $\sigma(j) = l$. Since $(kl) = \sigma(ij)\sigma^{-1}$, all transpositions are already contained in G. The only group containing all transpositions is S_n. □

Ramification. Let $f: Y \to X$ be a morphism of k-schemes for a field k. Denote by $\Omega_{X/Y}$ the sheaf of relative differentials. I will list a few basics about differentials that we are going to use later on (cf. [6, Section 01UM] and [6, Section 0C1B]).

Lemma 2.1. *Let $\iota: Y \hookrightarrow Z$ be a closed immersion of schemes over X with ideal sheaf $\mathcal{I}$. The sequence*

$$\mathcal{I}/\mathcal{I}^2 \xrightarrow{\mathrm{d}} \iota^*\Omega_{Z/X} \to \Omega_{Y/X} \to 0$$

is exact.

Lemma 2.2. *The sequence*

$$f^*\Omega_{X/k} \xrightarrow{f^*} \Omega_{Y/k} \to \Omega_{Y/X} \to 0$$

is exact.

Denote by $\mathfrak{D}_f$ the different of f, i. e. the annihilator of the relative differentials. By counting the degree, for curves we get:

Lemma 2.3 (Riemann-Hurwitz formula)**.** *Let X, Y be geometrically connected, smooth projective curves and let f be generically étale. Then we have*

$$2\mathrm{g}_Y - 2 = \deg(f)(2\mathrm{g}_X - 2) + \deg \mathfrak{D}_f = \deg(f)(2\mathrm{g}_X - 2) + \sum_{y \in Y} \nu_y(\mathfrak{D}_f) \deg y.$$

Remark 2.4. If Y/X is further generically Galois with Galois group G we can rewrite the formula to

$$2\mathrm{g}_Y - 2 = |G| \left(2\mathrm{g}_X - 2 + \sum_{x \in X} \frac{\nu_y(\mathfrak{D}_f)}{\mathrm{e}_x} \deg x \right)$$

where we take any y in the fiber of x.

Remark 2.5. To give a more explicit formula for $\nu_y(\mathfrak{D}_f)$ we look at local generators. Let π_x, π_y be uniformizers of $\mathcal{O}_{X,x}, \mathcal{O}_{Y,y}$. Since X and Y are smooth, the module of differentials is an invertible sheaf. Assume $\kappa(y)/k$ to be separable, then $\mathrm{d}\pi_x$ (resp. $\mathrm{d}\pi_y$) generate $\Omega_{X/k,x}$ (resp. $\Omega_{Y/k,x}$). We have

$$\pi_x = u\pi_y^{\mathrm{e}_y}$$

for some unit u. In terms of these generators we can give f^* in lemma 2.2 explicitly

$$f^*(\mathrm{d}\pi_x) = \mathrm{d}(f^*\pi_x) = \mathrm{d}(u\pi_y^{\mathrm{e}_y}) = u\mathrm{e}_y\pi_y^{\mathrm{e}_y - 1}\mathrm{d}\pi_y + \pi_y^{\mathrm{e}_y}\mathrm{d}u.$$

Write $\mathrm{d}u = v\mathrm{d}\pi_y$. Since $f^*(\mathrm{d}\pi_x)$ generates $\mathfrak{D}_f$, we have

$$\nu_y(\mathfrak{D}_f) = \nu_y(u\mathrm{e}_y\pi_y^{\mathrm{e}_y - 1} + v\pi_y^{\mathrm{e}_y}) = (\mathrm{e}_y - 1) + \nu_y(\mathrm{e}_y + v\pi_y) \geq (\mathrm{e}_y - 1) + \min\{\nu_y(\mathrm{e}_y), \nu_y(v) + 1\}.$$

For tame ramification we get

$$\nu_y(\mathfrak{D}_f) = \mathrm{e}_y - 1$$

and for wild ramification we have

$$\nu_y(\mathfrak{D}_f) \geq \mathrm{e}_y.$$

Chebotarev density theorem. Let $\mathbb{F}_q$ be a finite field of order a prime power q. For the rest of the section we fix the following notation

$$\begin{array}{lll} Y & & \text{geometrically smooth, connected projective curve} \\ \Big\downarrow & \text{finite étale geometric cover,} & \\ & \text{generically Galois with group } G & \\ B \subseteq X/\mathbb{F}_q & & \text{geometrically smooth, connected projective curve} \end{array}$$

branch locus

A cover is said to be geometric if the field of constants is the same for both X and Y, or equivalently the Galois group stays the same under base change to an algebraic closure of $\mathbb{F}_q$.

To each complex representation $\chi : G \to \mathrm{GL}(V)$ we can assign a character χ by taking the trace.

A conjugacy class is the orbit of an element under conjugation. Let $\mathbb{C}(G)$ denote the space of class functions on G, i. e. maps $G \to \mathbb{C}$ that are constant on conjugacy classes. Characters are class functions since the trace is invariant under conjugation.

For a subset $C \subseteq G$ and a class function χ set

$$\chi(C) = \frac{1}{|C|} \sum_{g \in C} \chi(g).$$

Recall that Frob_x is defined as the preimage of the Frobenius element in x (cf. definition 1.13). In order to count points on X we define the linear map $\pi : \mathbb{C}(G) \to \mathbb{C}$ by

$$\pi(\chi) = \sum_{x \in X(\mathbb{F}_q)} \chi(\mathrm{Frob}_x) = \sum_{x \in X(\mathbb{F}_q)} \frac{1}{J_x} \sum_{g \in \mathrm{Frob}_x} \chi(g).$$

Let 1 denote the constant character and let $\mathbf{1}_C$ be the indicator function for a conjugacy class C. We get

$$\begin{aligned} \pi(1) &= \#X(\mathbb{F}_q), \\ \pi(\mathbf{1}_C) &= \#\{x \in X(\mathbb{F}_q) \setminus B \mid \mathrm{Frob}_x \in C\} + \sum_{x \in B(\mathbb{F}_q)} \frac{1}{J_x} \sum_{g \in \mathrm{Frob}_x} \mathbf{1}_C(g). \end{aligned}$$

Lemma 2.6. *We have*

$$\sum_{\substack{C \\ \text{conjugacy} \\ \text{class}}} \frac{1}{|C|} \left(\pi(\mathbf{1}_C) - \frac{|C|}{|G|} \pi(1) \right)^2 = \frac{1}{|G|} \sum_{\substack{\chi \neq 1 \\ \text{irred. char.}}} |\pi(\chi)|^2.$$

Proof. Setting

$$\langle \chi, \chi' \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\chi'(g)}$$

we get a Hermitian inner product on $\mathbb{C}(g)$ with orthonormal basis given by the irreducible characters of G.

Let

$$f = \sum_{\substack{\chi \neq 1 \\ \text{irred.}}} \pi(\chi) \overline{\chi}.$$

Hence,

$$\begin{aligned} \langle f, f \rangle &= \frac{1}{|G|} \sum_{g \in G} \left(\sum_{\substack{\chi \neq 1 \\ \text{irred.}}} \pi(\chi) \overline{\chi(g)} \right) \left(\sum_{\substack{\chi \neq 1 \\ \text{irred.}}} \overline{\pi(\chi)} \chi(g) \right) \\ &= \frac{1}{|G|} \sum_{\substack{C \\ \text{conj.} \\ \text{class}}} |C| \left(\sum_{\substack{\chi \neq 1 \\ \text{irred.}}} \pi(\chi) \overline{\chi(C)} \right) \left(\sum_{\substack{\chi \neq 1 \\ \text{irred.}}} \overline{\pi(\chi)} \chi(C) \right). \end{aligned}$$

Using

$$\overline{\mathbf{1}_C} = \mathbf{1}_C = \sum_{\chi \text{ irred.}} \langle \mathbf{1}_C, \chi \rangle \chi = \frac{|C|}{|G|} \sum_{\chi \text{ irred.}} \overline{\chi(C)} \chi$$

and the linearity of π, the above term becomes

$$|G| \sum_{\substack{C \\ \text{conj.} \\ \text{class}}} \frac{1}{|C|} \left(\pi(\mathbf{1}_C) - \frac{|C|}{|G|} \pi(1) \right)^2.$$

On the other hand we can write the sum as

$$\begin{aligned}\langle f, f\rangle &= \frac{1}{|G|}\sum_{\substack{\chi,\chi'\neq 1\\ \text{irred.}}} \pi(\chi)\overline{\pi(\chi')}\sum_{g\in G}\overline{\chi(g)}\chi'(g)\\ &= \frac{1}{|G|}\sum_{\substack{\chi=\chi'\neq 1\\ \text{irred.}}} |G|\pi(\chi)\overline{\pi(\chi')}\\ &= \sum_{\substack{\chi\neq 1\\ \text{irred.}}} |\pi(\chi)|^2\end{aligned}$$

where we use the orthogonality of the irreducible characters. Thus, we get

$$|G|\sum_{\substack{C\\ \text{conj.}\\ \text{class}}}\frac{1}{|C|}\left(\pi(\mathbf{1}_C)-\frac{|C|}{|G|}\pi(1)\right)^2 = \langle f, f\rangle = \sum_{\substack{\chi\neq 1\\ \text{irred.}}}|\pi(\chi)|^2.$$

□

Definition 2.7. Let $x \in X$ be a closed point and $q \in Y$ a point above x with local ring $\mathcal{O}_{Y,q}$ and maximal ideal m_q. The kernel

$$G_i = \ker\left(\mathcal{D}_x \to \mathrm{Aut}(\mathcal{O}_{Y,q}/m_q^{i+1})\right)$$

is called the i-th ramification group in x.

Remark 2.8. For small i these occurred already, $G_{-1} = \mathcal{D}_x$, $G_0 = \mathcal{I}_x$, $G_1 = \mathcal{I}_x^w$ and $G_1/G_0 = \mathcal{I}_x^t$.

Remark 2.9. By going to the completion, we can assume the extensions of rings of integers to be generated by one element $\mathcal{O}_Y = \mathcal{O}_X[\alpha]$ (cf. [4, Lemma 10.4]). Since the action of $\mathcal{D}_x$ is determined by α, for i large enough, the ramification groups are trivial.

Definition 2.10. For a character χ and a closed point $x \in X$ set

$$f(\chi, x) = \sum_{i\geq 0}\frac{|G_i|}{|G_0|}\left(\chi(1)-\chi(G_i)\right).$$

The ideal

$$\mathcal{F}(\chi) = \prod_x x^{f(\chi,x)}$$

is called the Artin conductor of χ.

Lemma 2.11. *We have*

$$\nu_x(\mathcal{F}(\chi)) \leq \frac{2}{\mathrm{e}_x}\chi(1)\nu_q(\mathfrak{D}_{Y/X})$$

for any q lying over x.

Proof. By going to the completion, assume $\mathcal{O}_Y = \mathcal{O}_X[\alpha]$ with monic minimal polynomial f. It is enough to show the claim for the totally ramified case. For $g \in G_0$ we get

$$\nu_q(g\alpha-\alpha) = \max\{i, g\in G_{i-1}\}.$$

Hence,

$$\sum_{i\geq 0}\sum_{1\neq g\in G_i}\chi(g) = \sum_{1\neq g\in G_0}\nu_q(g\alpha-\alpha)\chi(g).$$

And for $\chi = 1$ this gives

$$\sum_{i\geq 0}(|G_i|-1) = \sum_{1\neq g\in G_0}\nu_q(g\alpha-\alpha).$$

The different is generated by df according to lemma 2.1. Writing

$$f = \prod_{g\in G_0}(x-g\alpha),$$

we get

$$\sum_{1\neq g\in G_0} \nu_q(g\alpha-\alpha) = \nu_q\left(\prod_{1\neq g\in G_0}(\alpha-g\alpha)\right) = \nu_q(f') = \nu_q(\mathfrak{D}_{Y/X}).$$

Combining all of this, we have

$$\begin{aligned}
\nu_x(\mathcal{F}(\chi)) &= \sum_{i\geq 0}\frac{|G_i|}{|G_0|}\left(\chi(1)-\chi(G_i)\right)\\
&= \frac{\chi(1)}{\mathrm{e}_x}\sum_{i\geq 0}(G_i-1) - \frac{1}{\mathrm{e}_x}\sum_{1\neq g\in G_0}\nu_q(g\alpha-\alpha)\chi(g)\\
&= \frac{1}{\mathrm{e}_x}\sum_{1\neq g\in G_0}\nu_q(g\alpha-\alpha)(\chi(1)-\chi(g))\\
&\leq \frac{2}{\mathrm{e}_x}\chi(1)\nu_q(\mathfrak{D}_{Y/X})
\end{aligned}$$

where the inequality follows from

$$|\chi(g)| \leq \dim\chi = \chi(1).$$

□

Theorem 2.12. *We have the inequality*

$$\sum_{\substack{C\\ \text{conjugacy}\\ \text{class}}}\frac{1}{|C|}\left(\pi(\mathbf{1}_C)-\frac{|C|}{|G|}\pi(1)\right)^2 \leq 4q\left(\frac{1}{|G|}(2\mathrm{g}_Y-2)-(\mathrm{g}_X-1)\right)^2.$$

Proof. According to [3, Equation (1.4), (4.1)] we have

$$|\pi(\chi)| \leq ((2\mathrm{g}_X-2)\chi(1)+\deg\mathcal{F}(\chi))\,q^{\frac{1}{2}}.$$

Combining this with lemma 2.6 and lemma 2.11 we get

$$\begin{aligned}
&\sum_{\substack{C\\ \text{conjugacy}\\ \text{class}}}\frac{1}{|C|}\left(\pi(\mathbf{1}_C)-\frac{|C|}{|G|}\pi(1)\right)^2 = \frac{1}{|G|}\sum_{\substack{\chi\neq 1\\ \text{irred.}}}|\pi(\chi)|^2\\
&\leq \frac{1}{|G|}\sum_{\substack{\chi\neq 1\\ \text{irred.}}}\left((2\mathrm{g}_X-2)\chi(1)+\deg\mathcal{F}(\chi)\right)q^{\frac{1}{2}}\Big)^2\\
&\leq \frac{1}{|G|}\sum_{\substack{\chi\neq 1\\ \text{irred.}}} q\left((2\mathrm{g}_X-2)\chi(1)+\sum_{x\in X}\frac{2}{\mathrm{e}_x}\chi(1)\nu_q(\mathfrak{D}_{Y/X})\deg(x)\right)^2.
\end{aligned}$$

Since

$$\sum_{\text{irred.}}\chi(1)^2 = \sum_{\text{irred.}}\dim_{\mathbb{C}}(\chi)^2 = \dim_{\mathbb{C}}\left(\bigoplus_{\text{irred.}}\chi^{\dim_{\mathbb{C}}\chi}\right) = \dim_{\mathbb{C}}\mathrm{Reg} = |G|,$$

together with the Riemann-Hurwitz formula (remark 2.4) we get

$$\begin{aligned}
\sum_{\substack{C\\ \text{conjugacy}\\ \text{class}}}\frac{1}{|C|}\left(\pi(\mathbf{1}_C)-\frac{|C|}{|G|}\pi(1)\right)^2 &\leq 4q\left(\mathrm{g}_X-1+\sum_{x\in X}\frac{1}{\mathrm{e}_x}\nu_q(\mathfrak{D}_{Y/X})\deg(x)\right)^2\\
&= 4q\left(\frac{1}{|G|}(2\mathrm{g}_Y-2)-(\mathrm{g}_X-1)\right)^2
\end{aligned}$$

□

Denote by $X^{\mathrm{ur}} = X \setminus B$ the unramified points in X and denote by $\pi_{\restriction X^{\mathrm{ur}}}$ the restriction of π to X^{ur}, i. e. taking the sum over unramified points.

Corollary 2.13 (Chebotarev density theorem)**.** *The amount of unramified rational points with given Frobenius conjugacy class C admits the inequality*

$$|\pi_{\restriction X^{\mathrm{ur}}}(\mathbf{1}_C) - \frac{|C|}{|G|}\pi_{\restriction X^{\mathrm{ur}}}(1)| \leq 2\sqrt{|C|}q^{\frac{1}{2}}\left(\frac{1}{|G|}(2\mathrm{g}_Y - 2) - (\mathrm{g}_X - 1)\right) + \deg B.$$

Proof. We have

$$\frac{1}{|C|}\left(\pi(\mathbf{1}_C) - \frac{|C|}{|G|}\pi(1)\right)^2 \leq \sum_{\substack{C \\ \text{conjugacy} \\ \text{class}}} \frac{1}{|C|}\left(\pi(\mathbf{1}_C) - \frac{|C|}{|G|}\pi(1)\right)^2.$$

Applying theorem 2.12, taking the square root and using

$$|\pi_{\restriction X^{\mathrm{ur}}}(\mathbf{1}_C) - \frac{|C|}{|G|}\pi_{\restriction X^{\mathrm{ur}}}(1)| \leq |\pi(\mathbf{1}_C) - \frac{|C|}{|G|}\pi(1)| + \deg B,$$

we get the result. □

3. A POLYNOMIAL TO SOLVE THE DLP

Let $p \neq 2, 3$ be a prime, q a power of p and $k \in \mathbb{N}$. Let $\mathbb{F}_{q^k}$ be the finite field with q^k elements and $K = \mathbb{F}_{q^k}(a)$ the function field in one variable.

The polynomial we are looking at is

$$f = t^{q+2} + t^2 + a^2 t + a \in \mathbb{F}_{q^k}[a, t] \subset K[t].$$

The aim is to describe the degree of its irreducible factors in specializations $a = a_0$ for some $a_0 \in \mathbb{F}_{q^k}$.

Lemma 3.1. *The polynomial f is irreducible over K. Furthermore it is geometrically irreducible in $\mathbb{F}_{q^k}[a, t]$, i. e. stays irreducible under the base change to the algebraic closure $\overline{\mathbb{F}}_{q^k}$.*

Proof. The polynomial f is primitive as a polynomial in a as well as a polynomial in t, i. e. the greatest common divisor of the coefficients is 1. Hence, by Gauss's lemma we can verify irreducibility in either $K[t], \mathbb{F}_{q^k}[a, t]$ or $\mathbb{F}_{q^k}(t)[a]$. Take f to be a polynomial over $\mathbb{F}_{q^k}(t)$

$$f = a^2 + \frac{a}{t} + (t^{q+1} + t).$$

Since this is a quadratic expression, irreducible factors correspond to zeroes of the form

$$-\frac{1}{2t} \pm \sqrt{\frac{1}{4t^2} - t^{q+1} - t} = -\frac{1}{2t} \pm \frac{1}{2t}\sqrt{1 - 4t^{q+3} - 4t^3}.$$

We want to show that $s = 1 - 4t^{q+3} - 4t^3$ is not a square. The discriminant is given by

$$\begin{aligned}
\Delta_{1-4t^{q+3}-t^3} &= (-1)^{\frac{(q+3)(q+2)}{2}} \operatorname{res}(s, s') \\
&= (-1)^{\frac{(q+3)(q+2)}{2}} 12^{q+3} \operatorname{res}(s - 12ts', s') \\
&= (-1)^{\frac{(q+3)(q+2)}{2}} 12^{q+3} \operatorname{res}(1, s') \\
&= (-1)^{\frac{(q+3)(q+2)}{2}} 12^{q+3} \neq 0
\end{aligned}$$

This implies that the polynomial s has distinct roots, in particular s is not a square. The same argument holds over the algebraic closure. □

Lemma 3.2. *The discriminant of f is given by*

$$\Delta_f = (-1)^{\frac{(q+2)(q+1)}{2}} a^{q+1} \left(a^{q+3} - 4a^q + 8\right),$$

in particular $f \in K[t]$ is separable.

Proof. We have

$$\begin{aligned}
f &= t^{q+2} + t^2 + a^2 t + a \\
f' &= 2t^{q+1} + 2t + a^2
\end{aligned}$$

and by division with remainder

$$\begin{aligned}
f &= \frac{t}{2} f' + \frac{1}{2} a^2 t + a \\
f' &= \left(\left(\sum_{i=0}^{q} (-1)^i \left(\frac{2}{a}\right)^{i+2} t^{q-i}\right) + \left(\frac{2}{a}\right)^2\right)\left(\frac{1}{2}a^2 t + a\right) + a\left(a - \left(\frac{2}{a}\right)^2 + \left(\frac{2}{a}\right)^{q+2}\right).
\end{aligned}$$

By remark 1.4 we get

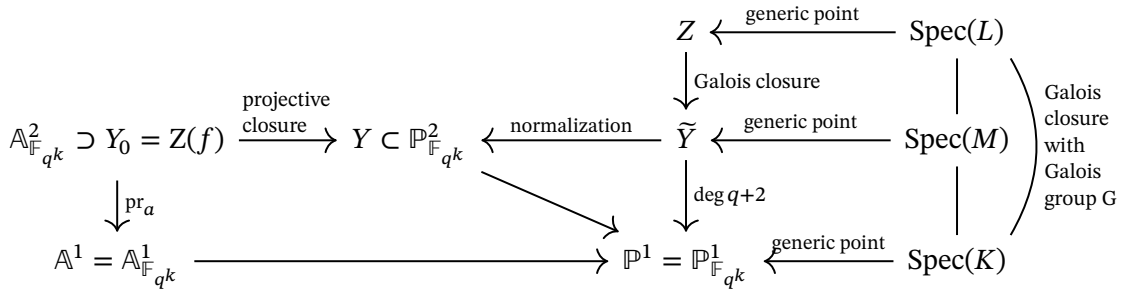
$$\begin{aligned}
\operatorname{res}(f,f') &= 2^{q+2-1}\operatorname{res}\left(\frac{1}{2}a^2t+a, f'\right)\\
&= 2^{q+2-1}\operatorname{res}\left(f', \frac{1}{2}a^2t+a\right)\\
&= \left(\frac{a^2}{2}\right)^{q+1} 2^{q+1}\operatorname{res}\left(a\left(a-\left(\frac{2}{a}\right)^2+\left(\frac{2}{a}\right)^{q+2}\right), \frac{1}{2}a^2t+a\right)\\
&= \left(a^2\right)^{q+1} a\left(a-\left(\frac{2}{a}\right)^2+\left(\frac{2}{a}\right)^{q+2}\right)\\
&= a^{q+1}\left(a^{q+3}-4a^q+2^{q+2}\right)\\
&= a^{q+1}\left(a^{q+3}-4a^q+8\right),
\end{aligned}$$

hence

$$\begin{aligned}
\Delta_f &= (-1)^{\frac{(q+2)(q+1)}{2}}\operatorname{res}(f,f')\\
&= (-1)^{\frac{(q+2)(q+1)}{2}} a^{q+1}\left(a^{q+3}-4a^q+8\right).
\end{aligned}$$

□

This shows that f is both irreducible and separable, so the setting is as in section 1. Geometrically, we get



The projective closure Y of Y_0 is given by the homogenization $f^{\#} = t^{q+2} + b^q t^2 + a^2 b^{q-1} t + b^{q+1} a$. Since the t term dominates, pr_a can be extended to the projective closure by mapping the extra points to infinity. Thus, the two standard affines $Y_0 = D(b)$ and $Y_\infty = D(a)$ in $\mathbb{P}^2$ already cover Y.

By the Galois closure Z we mean a smooth, geometrically connected projective curve with field of fractions L extending $\widetilde{Y}$ (cf. [6, Theorem 0BY1] for the existence).

Remark 3.3. The curve Y is not smooth over infinity, so the normalization is a proper extension. Indeed on Y_0 the Jacobi matrix is given by

$$\mathbf{J}_f = \left(2t^{q+1} + 2t + a^2, \quad 2at + 1\right).$$

So Y is smooth if and only if the ideal

$$\mathfrak{J} = (t^{q+2} + t^2 + a^2 t + a, 2t^{q+1} + 2t + a^2, 2at + 1)$$

has no common zero. Since $2at + 1 = 1$ for $at = 0$, the zero locus of $\mathfrak{J}$ does not intersect with the line $\mathrm{Z}(at)$ and we may restrict to the open $\mathrm{D}(at)$. The calculation

$$a(at + 2) = a^2 t + 2a = 2(t^{q+2} + t^2 + a^2 t + a) - t(2t^{q+1} + 2t + a^2)$$

shows that the singular points are given by the ideal

$$\mathfrak{J}_{(at)} = (2at + 1, 2t^{q+1} + 2t + a^2, at + 2).$$

Since $2at + 1 - 2(at + 2) = 3 \neq 0$, this does not vanish, hence, Y is smooth.

The equation

$$h = t^{q+2} + b^q t^2 + b^{q-1} t + b^{q+1}$$

defines Y_∞. Its Jacobi matrix is

$$\mathbf{J}_h = \left(2t^{q+1} + 2b^q t + b^{q-1}, \quad -tb^{q-2} + b^q\right).$$

This vanishes for $t = b = 0$, so Y is singular in $[1 : 0 : 0]$.

Proposition 3.4. *The ramification of the cover $\widetilde{Y} \to \mathbb{P}^1$ is given by*

- *one wildly ramified point over 0 with $e = q$, $f = 1$*
- *one simply ramified point over 0, i. e. $e = 2$, $f = 1$*
- *one simply ramified points over each of the $q + 3$ solutions of $a^{q+3} - 4a^q + 8$*
- *one tamely ramified point over ∞ with $e = \frac{q+1}{2}$, $f = 2$ or*
  two tamely ramified points over ∞ with $e = \frac{q+1}{2}$, $f = 1$.

Proof. We will first look at the ramification above 0. Denote by $\overline{f}$ the reduction of f modulo a. We have

$$\overline{f} = t^{q+2} + t^2 = t^2(t^q + 1) = t^2(t + 1)^q \in \mathbb{F}_{q^k}[t],$$

so the extension of residue fields is trivial.

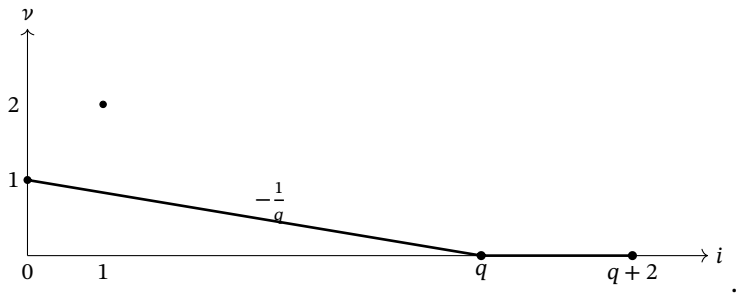
The Newton polygon (see definition 1.21) for $f = t^{q+2} + t^2 + a^2 t + a$ with respect to the valuation at $a = 0$ is given by

Hence, by lemma 1.22 there is a zero α of valuation $\frac{1}{2}$ in the splitting field of f. For the right choice of a point y in $K(\alpha)$ we have $\nu_y(\alpha) = \frac{1}{2}$. It should be noted that we switch to the local field in y here and take the extension of the a-valuation. By lemma 1.9, the valuation ν_y has image in $\frac{1}{e_y}$, thus $2 \mid e_y$.

Setting $s = t + 1$ the Newton Polygon for

$$\begin{aligned} f(s, a) &= (s-1)^{q+2} + (s-1)^2 + a^2(s-1) + a \\ &= (s-1)^2(s^q - 1) + (s-1)^2 + a^2 s + a - a^2 \\ &= s^{q+2} - 2s^{q+1} + s^q + a^2 s + a(1-a) \end{aligned}$$

in $a = 0$ is given by



The transformation is linear and respects the cover. Hence, there is some point with ramification index divisible by q. Since q and 2 add up to the degree $q + 2$, these numbers need to correspond to the ramification indices of two different points above 0.

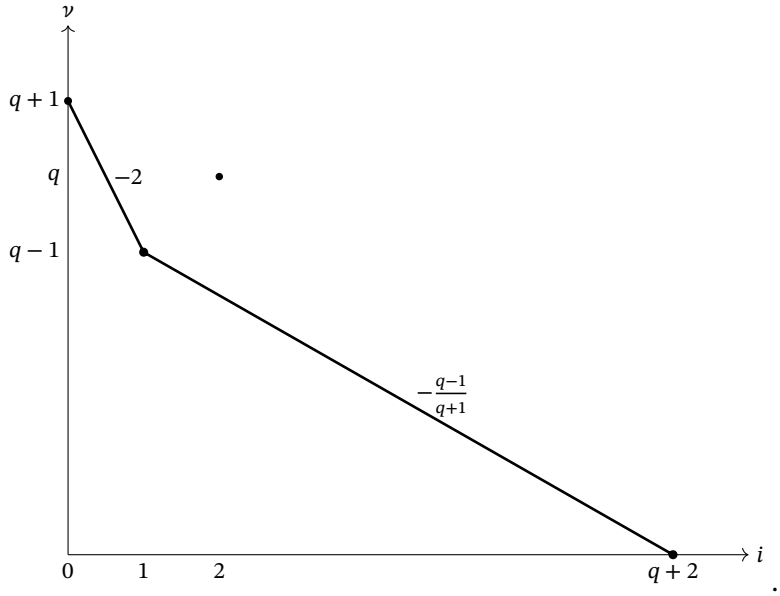
We will now look at the ramification above $a = \infty$. Taking the affine chart Y_∞ with defining equation $h = t^{q+2} + b^q t^2 + b^{q-1} t + b^{q+1}$, the point we are interested in is $b = 0$. Let K'/K be defined by the equation $\beta^{\frac{q+1}{2}} = b$ and let $M' = MK'$ be the compositum. The extension K'/K is totally ramified in $b = 0$ with ramification index $\frac{q+1}{2}$. In K' we can rewrite

$$h = t^{q+2} + (\beta^{\frac{q-1}{2}})^{q+1} t + b^q (t^2 + b).$$

Set

$$\widetilde{h} = \frac{1}{(\beta^{\frac{q-1}{2}})^{q+2}} h(\beta^{\frac{q-1}{2}} t) = t^{q+2} + t + \underbrace{r}_{\nu_\beta > 0}.$$

The reduction $t^{q+2} + t$ of $\widetilde{h}$ modulo β is separable, so f is unramified in $\beta = 0$. Thus, by lemma 1.17, the polynomial $\widetilde{h}$ locally defines the normalization. Hence, the ramification index of M'/K over ∞ equals $\frac{q+1}{2}$ and we get $e_q \mid \frac{q+1}{2}$ for any point in $\widetilde{Y}$ lying over ∞. Looking at the Newton polygon of g, we get



Thus there are $q + 1$ points, counted with multiplicity and degree above ∞ with $\frac{q+1}{\gcd(q-1,q+1)} = \frac{q+1}{2}$ dividing their ramification index. Combined with the upper bound, we see that there are two geometric points with ramification index $\frac{q+1}{2}$.

In order to get the remaining ramification, we look at the support of the relative differentials $\Omega_{\widetilde{Y}/\mathbb{P}^1}$ outside of $a = 0$ and $a = \infty$. According to lemma 2.2, on $\mathrm{D}(a) \subset Y$ those are given by

$$(\Omega_{Y/\mathbb{A}^1})_{\restriction \mathrm{D}(a)} = \mathbb{F}_{q^k}[a,t]_{(a)}/(f, f')_{(a)} \mathrm{d}t.$$

By the division with remainder done in lemma 3.2, we obtain an equality of $\mathcal{O}_{\mathrm{D}(a)}$-ideals

$$(f, f') = (\frac{1}{2}a^2 t + a, a\left(a - \left(\frac{2}{a}\right)^2 + \left(\frac{2}{a}\right)^{q+2}\right)) = (at + 2, a^{q+3} - 4a^q + 8).$$

Let $a_0 \in \mathbb{A}^1$ be a point in $\mathrm{Z}(a^{q+3} - 4a^q + 8)$. Since $at + 2$ is linear in t, there is exactly one point above a_0 that is ramified with trivial residue field extension. The second derivative does not vanish in that point

$$\frac{a^q}{2} f''(a_0, -\frac{2}{a_0}) = \frac{a^q}{2}(2t^q + 2)(a_0, -\frac{2}{a_0}) = a_0^q - 2 \neq 0.$$

Thus, the ramification index is bounded from above by 2, but then it has to equal 2, already. The derivative $3a^{q+2}$ of $a^{q+3} - 4a^q + 8$ does not vanish outside of zero. Hence, there are exactly $q + 3$ of such branch points counted with degree. □

Corollary 3.5. *The Galois group of f is given by the full symmetric group $G = \mathrm{S}_{q+2}$.*

Proof. We show that G is 2-transitive and contains a transposition, the claim then follows from lemma 1.23. Applying remark 1.20 to the ramification described in proposition 3.4, we see that the inertia group in the $q+3$ simply ramified points contains a transposition and $\mathcal{I}_0$ is embedded into $\mathrm{S}_q \times \mathrm{S}_2$ with transitive image under the projections.

Denote by W the q zeroes that S_q is acting on and denote by T the other two zeroes. The exact sequence

$$1 \to \underbrace{\mathcal{I}_0^w}_{p\text{-group}} \to \mathcal{I}_0 \to \underbrace{\mathcal{I}_0^t}_{\text{prime to } p} \to 1$$

from lemma 1.16 then tells us that $\mathcal{I}_0^w$ is embedded into the first factor S_q. Since $\mathcal{I}_0$ acts transitively on W and $\mathcal{I}_0^w$ is normal in $\mathcal{I}_0$, the orbits $\mathcal{I}_0^w.w$ have the same length for every $w \in W$. The tame inertia group $\mathcal{I}_0^t$ acts transitively on the orbits $W/\mathcal{I}_0^w$. Indeed, it is defined as the cokernel of $\mathcal{I}_0^w \to \mathcal{I}_0$. Thus we get the equation

$$\underbrace{|W|}_{q} = \underbrace{|\mathcal{I}_0^w.w|}_{p\text{-power}} \cdot \underbrace{|W/\mathcal{I}_0^w|}_{\text{prime to } p}.$$

Hence, $|W/\mathcal{I}_0^w| = 1$ and the action of $\mathcal{I}_0^w$ on W is transitive.

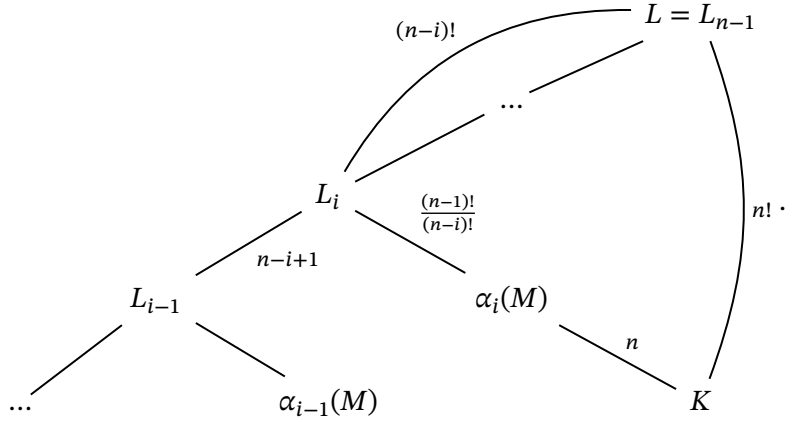
Fix an element $t \in T$. We want to know if the stabilizer G_t acts transitively on $Z = W \cup T \setminus \{t\}$. Let $z, z' \in Z$, we want to find $g \in G_t$ with $gz = z'$. For $z, z' \in W$ we can find such an element in $\mathcal{I}_0^w \subset G_t$ because of the observation above, so we may assume $z \in T \setminus \{t\}$. We know that G acts transitively on $W \cup T$. Hence, since $|T| = 2$ and $|W \cup T| = q+2$ is odd, there exists an element $g \in G$ with $|T \cap gT| = 1$. If we can find such a g in G_t, looking at gz, z', we are in the setting from before. So assume $g \notin G_t$ and upon the right choice of t we have $gt = z$. Take some $h \in \mathcal{I}_0^w$ not fixing gz, then $g^{-1}hg \in G_t$ is the element we are looking for. □

For a field K let g_K denote the genus of a smooth projective model of K.

Lemma 3.6. *Let L/K be a finite, geometric Galois extension with Galois group S_n. Let M/K be an intermediate field of degree n with Galois closure L. Then the genus of L is bounded by*

$$\mathrm{g}_L \leq (n-1)! \left((n-1)\mathrm{g}_M + \frac{(n-2)(n-1)}{2} \right).$$

Proof. Write the Galois closure as the compositum $L = \prod_{\alpha\colon M \to L} \alpha(M)$. Choose an order $\alpha_1, \dots, \alpha_n$ of those embeddings and set $L_i = K(\alpha_1, \dots, \alpha_i)$. We can successively build the compositum to get L



The genus of L_{i+1} can then be bounded by Castelnuovo's Inequality (cf. [7, Theorem 3.11.3])

$$\begin{aligned}
\mathrm{g}_{L_i} &\leq [L_i : L_{i-1}]\mathrm{g}_{L_{i-1}} + [L_i : \alpha_i(M)]\mathrm{g}_M + ([L_i : L_{i-1}] - 1)([L_i : \alpha_i(M)] - 1) \\
&= (n-i+1)\mathrm{g}_{L_{i-1}} + \frac{(n-1)!}{(n-i)!}\mathrm{g}_M + (n-i)\left(\frac{(n-1)!}{(n-i)!} - 1\right) \\
&= (n-i+1)(\mathrm{g}_{L_{i-1}} - 1) + 1 + \frac{(n-1)!}{(n-i)!}(\mathrm{g}_M + n - i).
\end{aligned}$$

Thus

$$g_{L_i} - 1 \leq (n-i+1)(g_{L_{i-1}} - 1) + \frac{(n-1)!}{(n-i)!}(g_M + n - i).$$

Setting

$$a_i = \frac{(n-i)!}{(n-1)!}(g_{L_i} - 1),$$

we get

$$a_i \leq a_{i-1} + (g_M + n - i).$$

So in total

$$\begin{aligned} a_{n-1} &\leq a_1 + \sum_{i=1}^{n-2}(g_M + n - i - 1) \\ &= a_1 + (n-2)g_M + (n-2)(n-1) - \frac{(n-2)(n-1)}{2} \\ &= a_1 + (n-2)g_M + \frac{(n-2)(n-1)}{2}. \end{aligned}$$

In terms of g_L with

$$\begin{aligned} g_{L_{n-1}} &= (n-1)!a_{n-1} + 1, \\ a_1 &= g_{L_1} - 1 = g_M - 1 \end{aligned}$$

we have

$$\begin{aligned} g_L = g_{L_{n-1}} &= (n-1)!a_{n-1} + 1 \\ &\leq (n-1)!\left(a_1 + (n-2)g_M + \frac{(n-2)(n-1)}{2}\right) + 1 \\ &= (n-1)!\left(g_M - 1 + (n-2)g_M + \frac{(n-2)(n-1)}{2}\right) + 1 \\ &\leq (n-1)!\left((n-1)g_M + \frac{(n-2)(n-1)}{2}\right). \end{aligned}$$

□

Lemma 3.7. *The genus of L is bounded by*

$$q(q+2)! \leq g_L \leq (q+1)^2(q+1)!.$$

Proof. We will calculate the genus of M first. Since $\widetilde{Y}$ is a smooth projective curve, we may calculate its genus by applying the Riemann-Hurwitz formula (lemma 2.3) to the cover $\widetilde{Y}/\mathbb{P}^1$. We have

$$2g_M - 2 = (q+2)(2g_K - 2) + \sum_{\substack{q \in \widetilde{Y} \\ \text{tame}}} (e_q - 1)\deg q + \sum_{\substack{q \in \widetilde{Y} \\ \text{wild}}} \nu_q(\mathfrak{D}_{\widetilde{Y}/\mathbb{P}^1})\deg q.$$

The tame ramification is given by a simply ramified point above 0, further $q+3$ simply ramified points and two geometric points above ∞ with ramification index $\frac{q+1}{2}$.

We now calculate the wild ramification, let y_w be the wildly ramified point above 0. Set $s = t + 1$. In the proof of proposition 3.4 we have seen that s has valuation $\frac{1}{q}$, so s is a uniformizer in the local ring $\mathcal{O}_{\widetilde{Y},y_w}$. Hence, the equation $f_w = s^{q+2} - 2s^{q+1} + s^q + a^2 s + a(1-a)$ defines $\mathcal{O}_{\widetilde{Y},y_w}$. Thus, according to lemma 2.1, $\mathrm{d}f_w$ generates the different in y_w and we get

$$\nu_y(\mathrm{d}f_w) = \nu_y(2(y-1)y^q + a^2) = \min\{\underbrace{\nu(2(y-1)y^q)}_{=q}, \underbrace{\nu_y(a^2)}_{=2q}\} = q.$$

In total we get

$$g_M = \frac{1}{2}\left((q+2)(0-2) + 1 + (q+3) + 2\frac{q-1}{2} + q + 2\right) = \frac{q+1}{2}.$$

According to lemma 3.5 the Galois group of L/K is S_{q+2}, so lemma 3.6 gives

$$g_L \leq (q+1)!\left((q+1)g_M + \frac{q(q+1)}{2}\right) = \frac{q+1}{2}(2q+1)(q+1)! \leq (q+1)^2(q+1)!.$$

By Abhyankar's lemma (lemma 1.19) the $q+3$ points $a_1, \dots, a_{q+3}$ have ramification index $e_{a_i} = 2$ and $e_\infty = \frac{q+1}{2}$ in L. Over 0 we just get the lower bound $e_0 \geq 2q$. Noting that $\nu_y(\mathfrak{D}_{Z/\mathbb{P}^1}) \geq e_y - 1$, we have

$$\begin{aligned}
2g_L - 2 &= [L : K]\left(g_K - 2 + \sum_{x\in\mathbb{P}^1} \frac{\nu_y(\mathfrak{D}_{Z/\mathbb{P}^1})}{e_x}\right) \\
&\geq (q+2)!\left(-2 + (q+3)\frac{1}{2} + \frac{q-1}{q+1} + \frac{2q-1}{2q}\right) \\
&= (q+2)!\left(\frac{q-1}{2} + \frac{q-1}{q+1} + \frac{2q-1}{2q}\right) \\
&\geq q(q+2)!.
\end{aligned}$$

□

Theorem 3.8. [2, Theorem 2.] *Given a prime power $q > 61$ that is not a power of 4, an integer $k \geq 18$, coprime polynomials $f_0, f_1 \in \mathbb{F}_{q^k}[t]$ of degree at most two and an irreducible degree d factor h of $f_0 t^q - f_1$, the DLP (discrete logarithm problem) in $\mathbb{F}_{q^{kd}} \cong \mathbb{F}_{q^k}[t]/(h)$ can be solved in expected time*

$$q^{\log_2 d + \mathcal{O}(k)}.$$

Taking two at most quadratic polynomials f_0, f_1 amounts to a selection of 6 parameters. Hence, we have a family F over $\mathbb{A}^6_{\mathbb{F}_{q^k}}$ defined by the equation $f_0 t^q - f_1$. Irreducible divisors of degree d in a specialization then correspond to degree d points on F that lie above a $\mathbb{F}_{q^k}$-rational point of $\mathbb{A}^6$.

The family $Y_0/\mathbb{A}^1$ is a specialization to a quadratic curve in $\mathbb{A}^6$. Hence, we want to find points of arbitrary degree $\leq q+2$ on Y_0. Note that the only point leading to non-coprime polynomials f_0, f_1 is $a = 0$.

Proposition 3.9. *Let $k > q + 10$ and $1 \leq d \leq q+2$. There is a point of degree d on Y lying over an unramified, $\mathbb{F}_{q^k}$-rational point.*

Proof. Denote by $C \subset G$ the conjugacy class of elements of cycle type $(d, q+2-d)$. There are

$$\binom{q+2}{d}(d-1)!\,(q-d+1)! = \frac{(q+2)!}{d(q+2-d)}$$

elements in C.

Assume there is no rational, unramified point $x \in X$ with a degree d point in its fiber in Y. By Dedekind's theorem (lemma 1.14), such a x corresponds to a rational point with Frob_x having cycle type $(d, \dots)$. In particular $\pi_{\restriction X^{\mathrm{ur}}}(\mathbf{1}_C) = 0$. Applying Chebotarev's density theorem (corollary 2.13), we have

$$\begin{aligned}
&|\underbrace{\pi_{\restriction X^{\mathrm{ur}}}(\mathbf{1}_C)}_{=0} - \frac{|C|}{|G|}\underbrace{\pi_{\restriction X^{\mathrm{ur}}}(1)}_{\geq q^k - q - 5}| \leq 2\sqrt{|C|}q^{\frac{k}{2}}\left(\frac{1}{|G|}(2g_L - 2) - (g_K - 1)\right) + (q+5) \\
&\leq 2\sqrt{\frac{(q+2)!}{d(q+2-d)}}q^{\frac{k}{2}}\left(\frac{1}{(q+2)!}\left(\left(2(q+1)^2(q+1)! - 2\right) + 1\right)\right) + q + 5 \\
&\leq 2\sqrt{\frac{(q+2)!}{d(q+2-d)}}q^{\frac{k}{2}}(2q+3) + q + 5
\end{aligned}$$

Multiplying with $\frac{|G|}{|C|} = d(q+2-d)$, we get

$$\begin{aligned} q^k &\leq 2\sqrt{d(q+2-d)(q+2)!q^{\frac{k}{2}}}(2q+3) + d(q+2-d)(q+5) + q + 5 \\ &\leq 2\sqrt{(q+2)^4 q! q^{\frac{k}{2}}}(2q+3) + (q+5)(q+2)^2 + q + 5 \\ &\leq 2\sqrt{(q+2)^4 q^q q^{\frac{k}{2}}}(2q+3) + (q+5)(q+2)^2 + q + 5 \\ &= 2(q+2)^2 q^{\frac{q}{2}} q^{\frac{k}{2}}(2q+3) + (q+5)(q+2)^2 + q + 5 \\ &\leq 3(q+2)^2 q^{\frac{q}{2}} q^{\frac{k}{2}}(2q+3) \leq q^{\frac{q}{2}+5} q^{\frac{k}{2}}. \end{aligned}$$

Taking the logarithm gives

$$k \leq \frac{q}{2} + 5 + \frac{k}{2}.$$

So for $k > q + 10$ there has to be a point with the desired properties. □

Remark 3.10. The cover $F/\mathbb{A}^6$ specializes to $Y/\mathbb{A}^1$. Hence, it has Galois group S_{q+2} itself.

We see that the obstruction for a smaller bound on k in the proof is the order of G. So we may be interested in polynomials with smaller Galois groups, even though such a polynomial will not admit irreducible factors of arbitrary degree. We drop the assumption on $p \neq 2, 3$ from now on. As an example we look at [1, Appendix by Serre] where Serre gives a proof that the Galois group of

$$g = t^{q+1} + at + 1$$

is given by the projective special linear group $\mathrm{PSL}(2, q)$. In order to understand the action of the Galois group on the roots, I will give a short outline of the proof.

Lemma 3.11. *The polynomial g defines a geometric cover with Galois group* $\mathrm{PSL}(2, q)$.

Proof. Let $G = \mathrm{PGL}(2, q)$ act on $L = \mathbb{F}_{q^k}(z)$ via Möbius transformation, i. e.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} t = \frac{at+b}{ct+d}.$$

Taking invariants $K = \mathbb{F}_{q^k}(t)^G$, we get a geometric Galois extension L/K with Galois group G. According to Lüroth's theorem, $K/\mathbb{F}_{q^k}$ is purely transcendental, so write $K = \mathbb{F}_{q^k}(u)$. In other words, we have a geometric cover

$$\begin{array}{c} Z = \mathbb{P}^1 \\ \downarrow \\ X = Z/G = \mathbb{P}^1 \end{array}.$$

The ramification is given by

- the $q^2 - q$ points $Z(\mathbb{F}_2) \setminus Z(\mathbb{F}_q)$ that are tamely ramified over 0 with $\mathrm{e}_0 = q + 1$,
- the $q + 1$ points $Z(\mathbb{F}_q)$ that are wildly ramified over ∞ with inertia group a triangular subgroup of order $q(q-1)$.

Set $M = L^{\mathcal{I}_\infty}$. The intersection of the triangular subgroups of $\mathrm{PGL}(2, q)$ is trivial, so $L = L^{\bigcap_{z|\infty} \mathcal{I}_z}$ is the Galois closure of M/K. We again have that $M = \mathbb{F}_{q^k}(y)$ is purely transcendental. A defining equation for M/K is given by

$$\tilde{g} = (y+1)^{q+1} - uy^q,$$

while L/K is given by the relation

$$u = \frac{(b(t)^{q-1} + 1)^{q+1}}{b(t)^{q(q-1)}}$$

with

$$b = t^q - 1.$$

Let K'/K be defined by the equation $a^{q+1} = u$ and let $L' = K'L$ denote the compositum. We have the intersection $K' \cap L = K(u^{\frac{1}{2}})$. This coincides with the geometric intersection, so the Galois group and the geometric Galois group coincide. Hence, L'/K' is a geometric cover with Galois group PSL_2. Note that the intersection is trivial in characteristic 2, but in that case we have $\mathrm{PGL}(2,q) = \mathrm{PSL}(2,q)$. Now writing $\tilde{g}$ in terms of a and substituting $t = \frac{y+1}{ay}$, we get

$$g = t^{q+1} - at + 1$$

which gives the same Galois group as the polynomial stated. □

Lemma 3.12. *The following cycle lengths d occur for elements in* $\mathrm{PSL}(2,q)$ *under the action on* $\mathbb{P}^1(\mathbf{F}_q)$

- $d = p$
- $\begin{cases} d \mid \frac{q-1}{2} & p \neq 2 \\ d \mid q-1 & p = 2 \end{cases}$
- $\begin{cases} d \mid \frac{q+1}{2} & p \neq 2 \\ d \mid q+1 & p = 2. \end{cases}$

Proof. Assume $p \neq 2$ first. We have

$$|\mathrm{PSL}(2,q)| = \frac{(q-1)q(q+1)}{2}.$$

Take $A \in \mathrm{SL}(2,q)$ and let f be its characteristic polynomial.

We first consider f to be reducible, then A has Jordan normal form

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Since the cycle type is invariant under conjugation, we may assume A to be of this form already. We then either have

$$A = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$$

with $a^2 = 1$, or

$$A = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}.$$

In the first case we get $At = t+1$ or $At = t-1$ which fixes ∞ and has cycle type $(p, \dots, p, 1)$. In the second case we have $At = a^2 t$, fixing 0 and ∞. Hence,

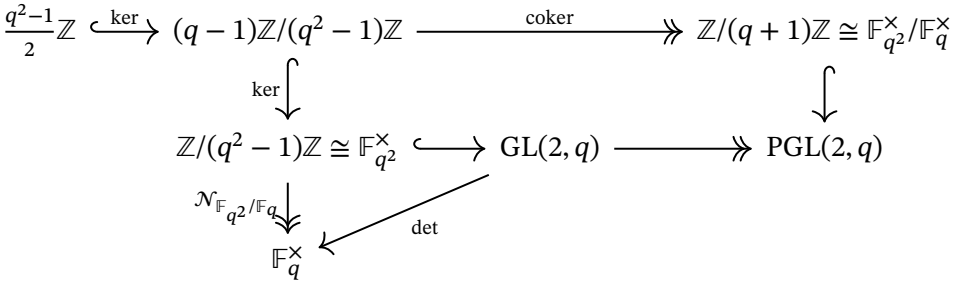
$$\langle a^2 \rangle \subseteq \underbrace{(\mathbb{F}_q^\times)^2}_{\frac{q-1}{2}} \subset \underbrace{\mathbb{F}_q^\times}_{q-1}$$

describes the cycle of the action on 1 with order equaling the cycle length. Since these groups are cyclic we get all divisors of $\frac{q-1}{2}$ as possible cycle lengths.

Now assuming f to be irreducible, we get the commutative diagram

$$\begin{array}{ccccc} \mathbb{F}_q[t]/f & \hookrightarrow & \mathrm{M}(2,q) & \overset{conj.}{=\!=} & \mathrm{M}(2, \langle 1, t \rangle_{\mathbb{F}_q}) \\ \| & & & \diagup\!\diagup & \\ \mathbb{F}_{q^2} & \xhookrightarrow{a \mapsto \cdot a} & \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^2}) & & \end{array}.$$

Hence,



commutes. The cycle length of a matrix in $\mathbb{F}_{q^2}^\times \cap \mathrm{SL}(2,q) = (q-1)\mathbb{Z}/(q^2-1)\mathbb{Z}$ is then given by the order of its image in $\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times$. Since the image is cyclic of order $\frac{q-1}{2}$, we get divisors of $\frac{q-1}{2}$ as cycle lengths.

For characteristic 2 we have equality $(\mathbb{F}_q^\times)^2 = \mathbb{F}_q^\times$ and

$$(q-1)\mathbb{Z}/(q^2-1)\mathbb{Z} \to \mathbb{Z}/(q+1)Z$$

is an isomorphism. Hence, giving the stated cycle lengths. □

Proposition 3.13. *Let*

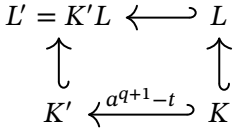
$$k > 12$$

and let d be of the following type

- $d = p$
- $\begin{cases} d \mid \frac{q-1}{2} & p \neq 2 \\ d \mid q-1 & p = 2 \end{cases}$
- $\begin{cases} d \mid \frac{q+1}{2} & p \neq 2 \\ d \mid q+1 & p = 2. \end{cases}$

There is an irreducible divisor of degree d of $g(t, a_0)$ for some $a_0 \in \mathbb{F}_{q^k}$.

Proof. With the notation from lemma 3.11



we want to first calculate the genus of L'. Recall that L/K has ramification indices $\mathrm{e}_0 = q+1$ and $\mathrm{e}_\infty = q(q-1)$. Since K'/K is ramified over 0 and ∞ with ramification index $q+1$, by Abhyankar's lemma 1.19 the ramification indices of L'/L are given by

$$\mathrm{e}_0 = \frac{\mathrm{lcm}(q+1, q+1)}{q+1} = 1$$
$$\mathrm{e}_\infty = \frac{\mathrm{lcm}(q+1, q(q-1))}{q(q-1)} = \frac{q+1}{2} \qquad (e_\infty = q+1 \text{ for } \mathrm{p} = 2).$$

There are $q+1$ such totally ramified points over ∞, so by the Riemann-Hurwitz formula

$$2\mathrm{g}_{L'} - 2 = \frac{q+1}{2}(\mathrm{g}_{\mathbb{P}^1} - 2) + (q+1)\frac{q-1}{2} = (q+1)\frac{q-3}{2},$$

and for $p = 2$

$$2\mathrm{g}_{L'} - 2 = (q+1)(\mathrm{g}_{\mathbb{P}^1} - 2) + (q+1)q = q^2 - q - 2.$$

The action of $\mathrm{PSL}(2,q)$ on the zeroes of g corresponds to the action of $\mathrm{PGL}(2,q)$ on

$$\mathrm{PGL}(2,q)/\mathcal{I}_\infty = \{q \mid \infty\} = \mathbb{P}^1(\mathbb{F}_q).$$

Thus, the cycle types of conjugacy classes in $\mathrm{PSL}(2,q)$ are as described in lemma 3.12. We have

$$|\mathrm{PSL}(2,q)| = \begin{cases} \frac{(q-1)q(q+1)}{2} & p \neq 2 \\ (q-1)q(q+1) & p = 2. \end{cases}$$

Assuming there is no unramified point on K' with Frobenius in a given conjugacy class C, Chebotarev's density theorem (corollary 2.13) gives

$$\begin{aligned} q^k &\leq 2\frac{|G|}{\sqrt{|C|}} q^{\frac{k}{2}} \left(\frac{1}{|G|} (2\mathrm{g}_{L'} - 2) + 1 \right) + \frac{|G|}{|C|} \\ &\leq 2q^{\frac{k}{2}} \left((q+1)\frac{q-3}{2} + |G| \right) + |G| \\ &= q^{\frac{k}{2}} \left((q+1)(q-3) + (q-1)q(q+1) \right) + \frac{(q-1)q(q+1)}{2} \\ &\leq q^{\frac{k}{2}} \left(q^2 + q^3 \right) + q^3 \leq 3q^{\frac{k}{2}+3}. \end{aligned}$$

Taking the logarithm we get

$$k \leq 1 + \frac{k}{2} + 3,$$

thus $k \leq 8$. The same calculations for $p = 2$ lead to the bound $k \leq 12$. Hence, for $k > 12$ there has to be a point with Frobenius in C. □

REFERENCES

[1] Shreeram S Abhyankar, *Galois theory on the line in nonzero characteristic*, Bull. Amer. Math. Soc.(NS) **27** (1992), no. 1, 68–133.

[2] Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel, *On the discrete logarithm problem in finite fields of fixed characteristic*, Transactions of the American Mathematical Society **370** (2018), no. 5, 3129–3145.

[3] Vijaya Kumar Murty and John Scherk, *Effective versions of the chebotarev density theorem for function fields*, Comptes rendus de l'Académie des sciences. Série 1, Mathématique **319** (1994), no. 6, 523–528.

[4] Jürgen Neukirch, *Algebraic number theory*, (1999).

[5] Jean-Pierre Serre, *Local class field theory*, Local Fields, Springer, 1979, pp. 188–203.

[6] The Stacks Project Authors, *Stacks Project*, `https://stacks.math.columbia.edu`, 2019.

[7] Henning Stichtenoth, *Algebraic function fields and codes*, vol. 254, Springer Science & Business Media, 2009.