A short proof of the Chebotarev density theorem for function fields*

Michiel Kosters†

Department of Mathematics, University of California, Irvine, 340 Rowland Hall, Irvine, CA 92 697, USA

Received June 27, 2016; accepted December 24, 2016

Abstract. In this article, we discuss a version of the Chebotarev density for function fields over perfect fields with procyclic absolute Galois groups. Our version of this density theorem differs from other versions in two aspects: we include ramified primes and we do not have an error term.

AMS subject classifications: 11R58, 11R45

Key words: Chebotarev density theorem, function field, ramified primes

1. Introduction

1.1. Motivation

One of the important results in arithmetic geometry is called 'the' Chebotarev density theorem for function fields. We will first briefly describe such a theorem. Let k be a finite field and let K be a function field over k. Let M/K be a finite Galois extension with group G. To a prime P of K which is unramified in M/K, one can associate a conjugacy class $(P, M/K)$ of G, called the Frobenius class. This Frobenius element for example gives the splitting behavior of P in M/K. The Chebotarev density theorem, in many different forms, gives an equidistribution result for the occurrence of conjugacy classes as the Frobenius class of primes. An example of such a theorem is [3, Theorem 9.13B]:

Theorem 1. *Let M/K be a finite Galois extension of function fields over a finite field k of cardinality q with group G. Assume that k is the full constant field of M. Let $C \subseteq G$ be a conjugacy class and let S_K' be the set of primes in K which are unramified in M. Then for each positive integer n we have*

$$\#\{P \in S_K' \,|\, \deg_k(P) = n,\ (P, M/K) = C\} = \frac{\#C}{\#G}\frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

*This is part of my PhD thesis written under the supervision of Hendrik Lenstra.

†Corresponding author. *Email address:* kosters@gmail.com (M. Kosters)

We will state a different version of a density theorem which is significantly different from the above theorem. Most importantly, our version will include ramified primes. Secondly, our version will not contain an error term. Instead of an equidistribution result, we 'parametrize' the points with a given Frobenius class by primes of twists of our original function field. We can get a version with error terms by taking into account the genus of the auxiliary function fields. Furthermore, our statement applies to a slightly more general field k. We allow k to be perfect with a procyclic absolute Galois group instead of being a finite field, and k does not necessarily need to be the full constant field of M. For simplicity, however, we restrict to the case when $n = 1$, that is, we only treat rational primes. The main reason for our restriction is that we want to obtain very clean statements. One should be able to obtain results for general n by base changing k and by the use of combinatorics.

1.2. New Chebotarev density theorem

Let us describe the new Chebotarev density theorem.

Let k be a perfect field with a procyclic absolute Galois group with $F \in \mathrm{Gal}(\overline{k}/k)$ as a topological generator. Let $r = \prod_p p^{n_p}$ with p prime and let $n_p \in \mathbf{Z}_{\geq 0} \sqcup \{\infty\}$ be the order of the profinite group $\mathrm{Gal}(\overline{k}/k)$, which is a Steinitz number. For example, one can take k to be a quasi-finite field, such as a finite field. There are also quasi-finite fields in characteristic 0 [4, Chapter XIII, Section 2]. One can also take k to be the maximal p-power extension of a finite field, or take $k = \mathbf{R}$. The field k can also be algebraically closed, but the results below will not be interesting in that case.

Let K be a geometrically irreducible function field over k, that is, a finitely generated field extension of k of transcendence degree 1 such that k is integrally closed in K. We denote by $\mathcal{P}_{K/k}$ the set of valuation rings of K containing k which are not equal to K. Let $P \in \mathcal{P}_{K/k}$. By k_P we denote the residue field of the valuation ring P. We set $\deg_k(P) = [\mathrm{k}_P : k]$. The subset of these valuation rings P such that $\mathrm{k}_P = k$, the set of rational primes of K, is denoted by $\mathcal{P}^1_{K/k}$. The restriction of P to a subfield K' of K is denoted by $P|_{K'}$ and we say that P lies above $P|_{K'}$.

Let M/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(M/K)$. Let $P \in \mathcal{P}_{K/k}$ with valuation Q above it in M. The group G acts transitively on the set of primes above P. Set $\mathrm{D}_{Q,K} = \{g \in G : gQ = Q\}$ (*decomposition group*). Note that we have a natural map $\mathrm{D}_{Q,K} \to \mathrm{Gal}(\mathrm{k}_Q/\mathrm{k}_P)$. The kernel of this map is called the *inertia group* and is denoted by $\mathrm{I}_{Q,K}$. In fact, we have an exact sequence

$$1 \to \mathrm{I}_{Q,K} \to \mathrm{D}_{Q,K} \to \mathrm{Gal}(\mathrm{k}_Q/\mathrm{k}_P) \to 1$$

([2, Theorem 3.6]). After a choice of a k-embedding $\mathrm{k}_Q \subseteq \overline{k}$ we have a map $\mathrm{Gal}(\overline{k}/\mathrm{k}_P) \to \mathrm{Gal}(\mathrm{k}_Q/\mathrm{k}_P)$. The image of $F^{[\mathrm{k}_P:k]} \in \mathrm{Gal}(\overline{k}/\mathrm{k}_P)$ is a generator of $\mathrm{Gal}(\mathrm{k}_Q/\mathrm{k}_P)$, which does not depend on the choice of the embedding. The set of elements in $\mathrm{D}_{Q,K}$ mapping to this generator is denoted by $(Q, M/K)$. We set

$$(P, M/K) = \{gxg^{-1} : g \in G,\ x \in (Q, M/K)\} = \bigcup_{Q' \in \mathcal{P}_{M/k}:\ Q'|_K = P} (Q', M/K),$$

which is a union of conjugacy classes. This definition does not depend on the choice of Q. If $\mathrm{I}_{Q,K} = 0$, this is just a single conjugacy class.

We define a probability measure (P, M) on G as follows. This is a function

$$(P, M) : G \to \mathbf{R}_{\geq 0}$$

such that $\sum_{g \in G} (P, M)(g) = 1$. For $\gamma \in G$, with conjugacy class Γ, we set:

$$(P, M)(\gamma) = \frac{\#\left((Q, M/K) \cap \Gamma\right)}{\#\Gamma \cdot \#(Q, M/K)},$$

where Q is any prime of M above P. If for Q above P one has $\mathrm{I}_{Q,K} = 0$, then the distribution is evenly divided over the whole conjugacy class $(P, M/K)$ and zero outside. If $\mathrm{I}_{Q,K} = 0$ and $\gamma \in G$ with $\mathrm{ord}(\gamma) \nmid r$ (divisibility of Steinitz numbers), one has $(P, M)(\gamma) = 0$.

Let k' be the integral closure of k in M (the full constant field of M). Let $N = \mathrm{Gal}(M/Kk')$, which is the geometric Galois group. Note that $G/N = \mathrm{Gal}(Kk'/K) = \mathrm{Gal}(k'/k) = \langle \overline{F} \rangle$, where $\overline{F}$ is the image of F under $\mathrm{Gal}(\overline{k}/k) \to \mathrm{Gal}(k'/k)$. We view $\overline{F}$ as an element of G/N, hence as a coset of G. If P is a rational prime of K, one easily finds $(P, M/K) \subseteq \overline{F} \subseteq G$.

We have the following alternative version of the Chebotarev density theorem.

Theorem 2. *Assume that we are in the situation as described above. Let $\gamma \in \overline{F} \subseteq G$ and assume that $m = \mathrm{ord}(\gamma) | r$. Let k_m be the unique extension of degree m of k in some algebraic closure of K containing M. Then the following hold:*

1. *There is a unique element $\Delta \in \mathrm{Gal}(k_m M/K)$ such that $\Delta|_M = \gamma$ and $\Delta|_{k_m} = F|_{k_m}$;*
2. *$M_\gamma = (k_m M)^{\langle \Delta \rangle}$ is geometrically irreducible over k and satisfies $k_m M_\gamma = k_m M$.*

Let

$$\begin{aligned} \phi \colon \mathcal{P}^1_{M_\gamma/k} &\to \mathcal{P}^1_{K/k} \\ Q &\mapsto Q|_K \end{aligned}$$

be the natural map. For $P \in \mathcal{P}^1_{K/k}$ we have

$$\#\phi^{-1}(P) = \#N \cdot (P, M)(\gamma).$$

Finally, we have

$$\sum_{P \in \mathcal{P}^1_{K/k}} (P, M)(\gamma) = \frac{\#\mathcal{P}^1_{M_\gamma/k}}{\#N}.$$

Note that $M_e = M$, where e is the identity element of G.

To see the resemblance with the conventional versions of the Chebotarev density theorem, we consider the case when k is a finite field. We denote the genus of M by $g_{k'}(M)$. The genus of M, which is equal to the genus of M_γ, allows us to estimate $\#\mathcal{P}^1_{M_\gamma/k}$. We find the following.

Corollary 1. *Assume that k is finite with cardinality q. Let $\gamma \in \overline{F}$. Then we have*

$$\left| \sum_{P \in \mathcal{P}^1_{K/k}} (P, M)(\gamma) - \frac{1}{\#N}(q+1) \right| \leq \frac{1}{\#N} 2 g_{k'}(M)\sqrt{q}.$$

To get to Theorem 1 for $n = 1$ with an explicit error, one sums over all γ inside a conjugacy class and one uses Riemann-Hurwitz to estimate the number of ramified primes. Such an explicit result, using similar 'parametrization methods', can be found in [1, Section 6.4], especially in Lemma 6.4.2, Lemma 6.4.4 and Proposition 6.4.8. Their error term is much more complicated than the error term obtained in Corollary 1, since their error for example also depends on $g_k(K)$ and the gonality of K.

One can easily generalize our results to the case when M/K is just assumed to be normal, since primes extend uniquely in purely inseparable extensions. We leave such results to the reader.

We do not know of any new applications of our results, but we believe that our results can be used to make other theorems look prettier.

We finish this section by giving an example of our approach, which shows how the ramified primes make the results nicer. This example also shows the relation between our result and twists of elliptic curves.

Example 1. *Let k be a finite field of cardinality q. Let*

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

be an elliptic curve over k. Let $M = k(X)[Y]/(Y^2 + a_1XY + \ldots)$ be the function field of E, which is a cyclic extension of degree 2 over $K = k(X)$ with a group say $G = \{e, g\}$. The rational primes which are ramified in the extension M/K correspond to the X-coordinates of the points of $E(k)[2]$. The unramified rational primes which split have e as Frobenius. The unramified primes which do not split have g as Frobenius. The ramified rational primes have Frobenius equally split over e and g. One has $N = G$ and we find:

$$\sum_{P \in \mathcal{P}^1_{K/k}} (P, M)(e) = \frac{\#E(k) - \#E(k)[2]}{2} + \frac{\#E(k)[2]}{2} = \frac{\#E(k)}{2}.$$

Using $\sum_{h \in G} \sum_{P \in \mathcal{P}^1_{K/k}} (P, M)(h) = q + 1$, one finds

$$\sum_{P \in \mathcal{P}^1_{K/k}} (P, M)(g) = (q + 1) - \frac{\#E(k)}{2}.$$

One has $M_e = M$, and M_g is the function field of the quadratic twist of E. Note that the number of unramified rational primes with e as Frobenius has a less clean expression

$$\frac{\#E(k) - \#E(k)[2]}{2}.$$

2. Proof of the Chebotarev density theorem

We continue using the notation introduced before Theorem 2. Set $h = [k' : k] = \# G/N$.

Lemma 1. *Assume that we are in the situation as described above. Let $\gamma \in \overline{F} \subseteq G$ and assume that $m = \operatorname{ord}(\gamma) | r$. Let k_m be the unique extension of degree m of k in some algebraic closure of K containing M. Then the following hold:*

1. *There is a unique element $\Delta \in \operatorname{Gal}(k_m M/K)$ such that $\Delta|_M = \gamma$ and $\Delta|_{k_m} = F|_{k_m}$;*

2. *$M_\gamma = (k_m M)^{\langle \Delta \rangle}$ is geometrically irreducible over k and satisfies $k_m M_\gamma = k_m M$.*

Furthermore, there is a well-defined map

$$\begin{aligned} \varphi \colon \mathcal{P}^1_{M_\gamma/k} &\to S = \{Q \in \mathcal{P}_{M/k} : \deg_k(Q|_K) = 1,\ \gamma \in (Q, M/K)\} \\ Q'|_{M_\gamma} &\mapsto Q'|_M, \end{aligned}$$

where $Q' \in \mathcal{P}_{k_m M/k}$. For $Q \in S$ we have $\# \varphi^{-1}(Q) = \frac{\deg_k(Q)}{h}$.

Proof. Note that γN is a generator in G/N, and hence one finds $m \equiv 0 \pmod{h}$. This shows that $k_m K \cap M = k'K$. We have the following diagram:

$$\begin{tikzcd}
 & k_m M & \\
k_m K \arrow[ur, hook] & & M \arrow[ul, hook] \\
 & k'K = k_m K \cap M \arrow[ul, hook] \arrow[ur, hook] & \\
 & K. \arrow[u, hook] &
\end{tikzcd}$$

Since $\gamma \in \overline{F}$, one obtains

$$\operatorname{Gal}(k_m M/K) = \operatorname{Gal}(k_m K/K) \times_{\operatorname{Gal}(k'K/K)} \operatorname{Gal}(M/K) \ni \Delta$$

and the first statement follows. Note that $M_\gamma \cap k_m K = K$. Furthermore, notice that $k_m M_\gamma$ is not fixed by any non-trivial element of $\langle \Delta \rangle$, and hence it is equal to $k_m M$.

We claim that the following three statements are equivalent for $P' \in \mathcal{P}_{k_m M/k}$:
1. $\gamma \in (P'|_M, M/K)$ and $P'|_K$ is rational;
2. $\Delta \in (P', k_m M/K)$ and $P'|_K$ is rational;
3. $P'|_{M_\gamma}$ is rational.

1 $\implies$ 2: We claim $(P', k_m M/K) = (P'|_{k_m K}, k_m K/K) \times (P'|_M, M/K)$. Indeed, both sets have the same size as $k_m K/K$ is unramified and it follows that the natural

injective map is a bijection. From the rationality of $P'|_K$ and the assumption $\gamma \in (P'|_M, M/K)$, one obtains $\Delta \in (P', k_m M/K)$.

$2 \implies 1$: obvious.

$2 \implies 3$: By 2 one has $\mathrm{Gal}(k_m M/M_\gamma) = \langle \Delta \rangle = \mathrm{D}_{P',M_\gamma}$. It follows that in the constant field extension $k_m M/M_\gamma$ that P' is the unique prime above $P'|_{M_\gamma}$. From 2 it follows that $\deg_k(P')|\mathrm{ord}(\Delta) = m$. By the theory of constant field extensions [5, Theorem 3.6.3], it follows that $P'|_{M_\gamma}$ is rational.

$3 \implies 2$: If $P'|_{M_\gamma}$ is rational, then so is $P'|_K$, and one finds

$$\{\Delta\} = (P', k_m M/M_\gamma) \subset (P', k_m M/K).$$

We will now look at φ. For a rational prime $P \in \mathcal{P}^1_{M_\gamma/k}$ there is a unique prime above it in $k_m M$. The implication $3 \implies 1$ shows that φ is well-defined. We will calculate the sizes of the fibers. Take a prime $Q \in S$. Notice that $[k_m M : M] = m/h$ and that $\deg_k(Q)|m$. In the extension $k_m M/M$, the residue field of Q grows with a degree $m/\deg_k(Q)$ and hence there are

$$\frac{m/h}{m/\deg_k(Q)} = \frac{\deg_k(Q)}{h}$$

primes above it in $k_m M$ [5, Theorem 3.6.3]. Each such prime gives a different preimage under φ and by $1 \implies 3$ we find all preimages. □

Lemma 2. *Let $\gamma \in \overline{F}$ and let Γ be its conjugacy class in G. Consider the natural surjective restriction map, where $S = \{Q \in \mathcal{P}_{M/k} : \deg_k(Q|_K) = 1,\ \gamma \in (Q, M/K)\}$ and $T = \{P \in \mathcal{P}_{K/k} : \deg_k(P) = 1,\ \gamma \in (P, M/K)\}$,*

$$\begin{aligned} \psi\colon S &\to T, \\ Q &\mapsto Q|_K. \end{aligned}$$

Then for $P \in T$ with prime $Q \in S$ above it we have

$$\#\psi^{-1}(P) = \frac{\#G}{\#\Gamma \cdot \#\,\mathrm{D}_{Q,K}} \cdot \#\left((Q, M/K) \cap \Gamma\right).$$

Proof. Let $Q \in S$ lie above P. Then we have $(Q, M/K) = \gamma\,\mathrm{I}_{Q,K}$. For $g \in G$ we have $(gQ, M/K) = g(Q, M/K)g^{-1}$. So $\gamma \in (gQ, M/K)$ iff $\gamma \in g(Q, M/K)g^{-1}$ iff $g^{-1}\gamma g \in (Q, M/K)$. Let G_γ be the stabilizer of γ under the conjugation action of G on itself. Then the number of $g \in G$ such that $\gamma \in (gQ, M/K)$ is equal to

$$\#G_\gamma \cdot \#\left((Q, M/K) \cap \Gamma\right) = \frac{\#G}{\#\Gamma} \cdot \#\left((Q, M/K) \cap \Gamma\right).$$

Furthermore, suppose that for $g, g' \in G$ we have $gQ = g'Q$. Then $g'^{-1}g \in \mathrm{D}_{Q,K}$. This shows that

$$\#\psi^{-1}(P) = \frac{\#G}{\#\Gamma \cdot \#\,\mathrm{D}_{Q,K}} \cdot \#\left((Q, M/K) \cap \Gamma\right).$$

□

We can finally prove the new version of the Chebotarev density theorem.

Proof of Theorem 2. The first part directly follows from Lemma 1. The rest of the proof will follow from combining Lemma 1 and Lemma 2. We follow the notation from these lemmas. Note that $\phi = \psi \circ \varphi$. Let $P \in T$ and let $Q \in \psi^{-1}(P)$. Note that $\deg_k(Q)$ does not depend on the choice of Q. One has:

$$\begin{aligned}
\#\phi^{-1}(P) &= \#\varphi^{-1} \circ \psi^{-1}(P) \\
&= \frac{\deg_k(Q)}{h} \cdot \frac{\#G}{\#\Gamma \cdot \#\,\mathrm{D}_{Q,K}} \cdot \#\left((Q, M/K) \cap \Gamma\right) \\
&= \frac{\#N}{\#\Gamma} \cdot \frac{\deg_k(Q) \cdot \#\left((Q, M/K) \cap \Gamma\right)}{\#\,\mathrm{D}_{Q,K}} \cdot \frac{\#(Q, M/K)}{\#(Q, M/K)} \\
&= \#N \cdot (P, M)(\gamma) \cdot \deg_k(Q) \cdot \frac{\#(Q, M/K)}{\#\,\mathrm{D}_{Q,K}} \\
&= \#N \cdot (P, M)(\gamma).
\end{aligned}$$

The last statement follows very easily. □

We will now prove the corollary.

Proof of Corollary 1. We use Theorem 2. By Hasse-Weil ([5, Theorem 5.2.3]) we have

$$|\{P \in \mathcal{P}_{M_\gamma/k} : \deg_k(P) = 1\} - (q+1)\}| \leq 2g_k(M_\gamma)\sqrt{q} = 2g_{k'}(M)\sqrt{q}.$$

This gives the required result. □

References

[1] M. D. Fried, M. Jarden, *Field arithmetic, results in mathematics and related areas. 3rd series. A series of modern surveys in mathematics*, Springer-Verlag, Berlin, 2008.

[2] M. Kosters, *The algebraic theory of valued fields*, preprint.

[3] M. Rosen, *Number theory in function fields, graduate texts in mathematics*, Springer-Verlag, New York, 2002.

[4] J. -P. Serre, *Local fields, graduate texts in mathematics*, Springer-Verlag, New York, 1979.

[5] H. Stichtenoth, *Algebraic function fields and codes, graduate texts in mathematics*, Springer-Verlag, Berlin, 2009.