The Čebotarev Density Theorem for Function Fields: An Elementary Approach

Moshe Jarden

School of Mathematical Sciences, Tel-Aviv University, Ramat-Aviv, Tel-Aviv, Israel

Introduction

The Čebotarev density theorem is one of the major results in algebraic number theory. It provides a quantitative measure of sets of prime divisors with qualitative properties related to finite Galois extensions. The basic nature of the theorem makes it very handy for applications. Thus the Čebotarev density theorem plays a central role in the decision procedure for the theory of finite fields of Ax [3] and in the transfer principle [7] from finite fields to the fields $\tilde{K}(\sigma)$, where K is a global field. An immediate application of the theorem, namely Bauer's theorem, is the key ingredient in Neukirch's proof [9], that two finite normal extensions of $\mathbb{Q}$ with isomorphic absolute Galois group must coincide; and there are many more applications.

The Čebotarev density theorem is true for number fields as well as for function fields of one variable over finite fields. The number field case has attracted the most attention. There are at least three versions of the proof, that of Čebotarev [4], that of Artin [1, 2] and that of Deuring [5]. They have also found their way to textbooks, e.g., that of Lang [8]. Serre [11, Theorem 7] sketches a unified treatment for both cases, via L-series

The goal of this note is to provide an elementary proof for the Čebotarev density theorem in the function field case.

Theorem. *Let E be a function field of one variable over a finite field and let F be a finite Galois extension of E. If $\mathfrak{C}$ is a conjugacy class in $\mathfrak{G}(L/K)$, then the Dirichlet density of the set of prime divisors $\mathfrak{p}$ of E whose Artin symbol $\left(\frac{F/E}{\mathfrak{p}}\right)$ is equal to $\mathfrak{C}$ is $\frac{|\mathfrak{C}|}{[F:E]}$.*

The central ingredient in the proof is the Riemann hypothesis for curves; otherwise it consists only of manipulations with fields and prime divisors.

0025-5831/82/0261/0467/$01.80

1. Preliminaries and Notation

Throughout this work K denotes a field with q elements and φ is the Frobenius automorphism of its absolute Galois group: $\varphi x = x^q$, for every x algebraic over K. The unique extension of K of degree n is denoted by K_n. We also fix a transcendental element t over K and consider function fields which are finite separable extensions of $K(t)$. If E is such an extension, then we denote by O_E the integral closure of $K[t]$ in E. The ring O_E is a Dedekind domain and the set of its non-zero prime ideals is denoted by $P(E)$. This set stands in a bijective correspondence with the set of prime divisors of E which are finite on O_E. For a $\mathfrak{p} \in P(E)$ we denote by $\bar{E}_\mathfrak{p} = O_E/\mathfrak{p}$ the residue field at $\mathfrak{p}$ and by $N\mathfrak{p} = |\bar{E}_\mathfrak{p}|$ its absolute norm. The field K is naturally embedded in $\bar{E}_\mathfrak{p}$ and $[\bar{E}_\mathfrak{p} : K] < \infty$. If K is algebraically closed in E, then $\deg \mathfrak{p} = [\bar{E}_\mathfrak{p} : K]$ is the *degree* of $\mathfrak{p}$. In this case we may consider a constant field extension $E' = K'E$, where $K' = K_n$. Then K' is algebraically closed in E' and $[E' : E] = n$. If z is a primitive element for K'/K, then its discriminant over K is non-zero; hence it is a unit of O_E. It follows that $O_{E'} = O_E[z]$ (cf. Zariski-Samuel [12, p. 264]). Moreover, every $\mathfrak{p} \in P(E)$ is unramified in E' and if $\mathfrak{p}' \in P(E')$ lies over $\mathfrak{p}$, then $\bar{E}_{\mathfrak{p}'} = \bar{E}_\mathfrak{p}(z) = K'\bar{E}_\mathfrak{p}$. In particular, if $\deg \mathfrak{p} = j$ and j divides n, then the residue class degree, $f(\mathfrak{p}) = [\bar{E}_{\mathfrak{p}'} : \bar{E}_\mathfrak{p}] = [K' : K_j] = n/j$. Hence, if $g(\mathfrak{p})$ denotes the number of $\mathfrak{p}' \in P(E')$ lying over $\mathfrak{p}$, then the formula $f(\mathfrak{p})g(\mathfrak{p}) = n$ implies that $g(\mathfrak{p}) = j$.

For the rest of this work we assume that indeed K is algebraically closed in E and fix a finite Galois extension F of E. If $\mathfrak{p} \in P(E)$ is unramified in F and $\mathfrak{P} \in P(F)$ lies over $\mathfrak{p}$, then $\left[\frac{F/E}{\mathfrak{P}}\right]$ is the *Frobenius automorphism* attached to $\mathfrak{P}$. It is the unique element of $\mathfrak{G}(F/E)$ that satisfies

$$\left[\frac{F/E}{\mathfrak{P}}\right] x \equiv x^{N\mathfrak{p}} \bmod \mathfrak{P} \quad \text{for every} \quad x \in O_F .$$

The conjugacy class of $\left[\frac{F/E}{\mathfrak{P}}\right]$ is the *Artin symbol* $\left(\frac{F/E}{\mathfrak{p}}\right)$. Consider now a fixed conjugacy class $\mathfrak{C}$ of $\mathfrak{G}(F/E)$ with, say, c elements. The class $\mathfrak{C}$ is associated with the set

$$C = \left\{ \mathfrak{p} \in P(E) \,\middle|\, \left(\frac{F/E}{\mathfrak{p}}\right) = \mathfrak{C} \right\}.$$

Our aim is to prove that

$$\lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in C} N\mathfrak{p}^{-s}}{\sum_{\mathfrak{p} \in P(E)} N\mathfrak{p}^{-s}} = \frac{c}{[F:E]}.$$

In the proof we also use the following notation:

L = the algebraic closure of K in F.
$n = [L : K]$, $m = [F : LE]$.
$P_k(E)$ = the set of prime divisors of E of degree k.
$P'_k(E) = \{\mathfrak{p} \in P(E) \mid \mathfrak{p}$ is unramified in F and $\deg \mathfrak{p} = k\}$.

$$C_k(E)=\left\{\mathfrak{p}\in P_k(E)\,\middle|\,\left(\frac{F/E}{\mathfrak{p}}\right)=\mathfrak{C}\right\}.$$
$$R(F/E)=\{\mathfrak{p}\in P(E)|\,\mathfrak{p}\text{ is ramified in }F\}.$$
$$R_k(F/E)=\{\mathfrak{p}\in R(F/E)|\deg\mathfrak{p}=k\}.$$
$$G=\mathfrak{G}(F/E).$$

2. Prime Ideals of Degree 1

The first and the most decisive step in the computation of the density of C is an interesting and useful result for its own sake.

Lemma 1. *If every element τ of $\mathfrak{C}$ satisfies*

$$\operatorname{res}_L\tau=\operatorname{res}_L\varphi \tag{1}$$

then

$$|C_1(E)|=\frac{c}{m}q+O(\sqrt{q}),$$

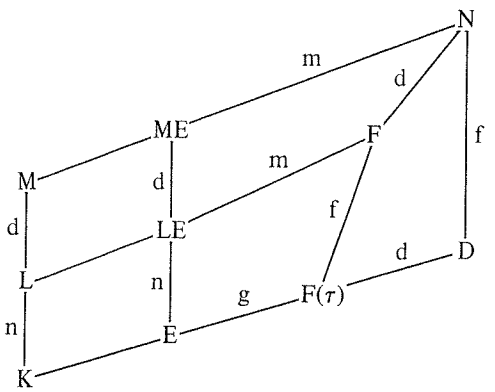
where the constant of the O depends on $[F:K(t)]$ and on the genus of F but otherwise it does not depend on q, on E or on F.

Proof. Let $\tau\in\mathfrak{C}$ and $f=\operatorname{ord}\tau$. Then (1) implies that $n|f$; hence $M=K_f$ contains $L=K_n$. The field M is linearly disjoint from F over L. Thus $N=MF$ is a finite Galois extension of E and $[N:ME]=[F:LE]=m$. Moreover, assumption (1) implies the existence of an element $\tilde{\tau}\in\mathfrak{G}(N/E)$ such that

$$\operatorname{res}_F\tilde{\tau}=\tau\quad\text{and}\quad\operatorname{res}_M\tilde{\tau}=\operatorname{res}_M\varphi. \tag{2}$$

The order of $\tilde{\tau}$ is f, since f is the order of the restriction of $\tilde{\tau}$ to M and to F. Therefore, if we denote by $D=N(\tilde{\tau})$ the fixed field of $\tilde{\tau}$, we have that $[N:D]=\operatorname{ord}\tilde{\tau}=f$. On the other hand, $F(\tau)=F\cap D$ and $[F:F(\tau)]=\operatorname{ord}\tau=f$; hence $FD=N$. In addition (2) implies that $K=M\cap D$; thus using the relation $[M:K]=f$, we have that $MD=N$. Let also $g=[F(\tau):E]$ and $[N:F]=[D:F(\tau)]=d$. Then

$$gd=[D:E]=[N:ME]=m. \tag{3}$$



Now M is algebraically closed in N, since L is algebraically closed in F. Thus $K=M\cap D$ is algebraically closed in D; in other words, D is a function field of one variable over K. It follows from the Riemann hypothesis for curves that

$$|P_1(D/K)|=q+O(\sqrt{q}), \tag{4}$$

where the constant of the O equals twice the genus, g_D, of D, which is equal to the genus of F, since N is a separable constant field extension of both D and F. Let

$$P_1'(D)=\{\mathfrak{q}\in P(D)|\ \deg\mathfrak{q}=1 \text{ and } \mathfrak{q} \text{ is unramified over } E\}.$$

This set differs from $P_1(D)$ by at most $[D:K(t)]$ prime divisors which are not finite on O_D and by at most $m|R_1(D/E)|$. By Hurwitz's genus formula and by (3)

$$|R_1(D/E)|\leqq|R_1(D/K(t))|\leqq 2g_D-2+2[D:K(t)]\leqq 2g_F-2+2[F:K(t)].$$

Thus (4) implies

$$|P_1'(D)|=q+O(\sqrt{q}), \tag{5}$$

where the constant of the O depends only on $[F:K(t)]$ and on g_F.

We consider now the set

$$C_\tau=\left\{\mathfrak{P}\in P(F)|\ \deg(E\cap\mathfrak{P})=1 \text{ and } \left[\frac{F/E}{\mathfrak{P}}\right]=\tau\right\}$$

and define a map $h:P_1'(D)\to C_\tau$ in the following way: We start with an element $\mathfrak{q}\in P_1'(D)$ and note that since $\deg\mathfrak{q}=1$ and since N/D is a constant field extension, there exists a unique $\mathfrak{Q}\in P(N)$ lying over $\mathfrak{q}$ and $\mathfrak{Q}$ is unramified over E. Define $\mathfrak{P}=h(\mathfrak{q})=F\cap\mathfrak{Q}$. If $\mathfrak{p}=E\cap\mathfrak{P}$, then $K\leqq\bar{E}_\mathfrak{p}\subseteq\bar{D}_\mathfrak{q}=K$; hence, $\bar{E}_\mathfrak{p}=K$ and $N\mathfrak{p}=q$. Observe that

$$\begin{aligned} x\in M &\Rightarrow \tilde{\tau}x=\varphi x=x^q \\ x\in O_D &\Rightarrow \tilde{\tau}x=x\equiv x^q \bmod\mathfrak{q}. \end{aligned} \tag{6}$$

Therefore, $\tilde{\tau}x\equiv x^q \bmod\mathfrak{Q}$ for every $x\in O_N=MO_D$; hence, $\tau x\equiv x^{N\mathfrak{p}} \bmod\mathfrak{P}$ for every $x\in O_F$. This means that $\left[\frac{F/E}{\mathfrak{P}}\right]=\tau$ and therefore that $\mathfrak{P}\in C_\tau$.

Claim. The fibers $h^{-1}(\mathfrak{P})$ contain exactly d elements.

Indeed, if $\mathfrak{P}\in C_\tau$ and if $\mathfrak{p}=E\cap\mathfrak{P}$, then the degree of $\bar{F}_\mathfrak{P}$ over $\bar{E}_\mathfrak{p}=K$ is equal to $\operatorname{ord}\tau=f$. Thus $\bar{F}_\mathfrak{P}=M$ and $\deg\mathfrak{P}=d=[N:F]$. It follows that over $\mathfrak{P}$ there lie exactly d elements $\mathfrak{Q}_1,\ldots,\mathfrak{Q}_d\in P(N)$. Let $\mathfrak{q}_i=D\cap\mathfrak{Q}_i$ for $i=1,\ldots,d$. Then

$$x\in O_F \Rightarrow \tilde{\tau}x=\left[\frac{F/E}{\mathfrak{P}}\right]x\equiv x^{N\mathfrak{p}}\equiv x^q \bmod\mathfrak{P}.$$

Therefore, we have, with (6), that $\tilde{\tau}x\equiv x^q \bmod\mathfrak{Q}_i$ for every $x\in O_N=MO_F$. In particular we get for $x\in O_D$ that $x\equiv x^q \bmod\mathfrak{q}_i$. This means that $\bar{D}_{\mathfrak{q}_i}=K$. It follows that $\mathfrak{q}_i\in h^{-1}(\mathfrak{P})$ and also that $\mathfrak{Q}_i$ is the unique element of $P(N)$ that lies over $\mathfrak{q}_i$. Thus $\mathfrak{q}_1,\ldots,\mathfrak{q}_d$ are distinct elements of $h^{-1}(\mathfrak{P})$. If, on the other hand, $\mathfrak{q}\in h^{-1}(\mathfrak{P})$ and

$\mathfrak{Q}$ is the unique prime ideal of O_N lying over $\mathfrak{q}$, then $\mathfrak{q}$ lies also over $\mathfrak{P}$ and therefore must be one of the $\mathfrak{Q}_i$'s. It follows that $\mathfrak{q}$ belongs to the set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_d\}$.

If we apply the claim to (5), we get

$$|C_\tau| = \frac{1}{d} q + O(\sqrt{q})$$

with the above restrictions on the constant of the O. Allowing τ to run over all elements of $\mathfrak{E}$, we have

$$\left| \bigcup_{\tau \in \mathfrak{E}} C_\tau \right| = \frac{c}{d} q + 0(\sqrt{q}). \tag{7}$$

Over every element of $C_1(E)$ there lie exactly g elements of $\bigcup C_\tau$. Hence, (7) and (3) imply that $|C_1(E)| = \frac{c}{m} q + O(\sqrt{q})$. □

Lemma 1 is also proved by Fried [6, p. 223]. Beside the use of the Riemann hypothesis for curves, Fried applies a result of class field theory which asserts that the L-functions associated to a non-trivial character of an abelian function field extension is a polynomial in $t = q^{-s}$. He does it in order to single out those primes whose Artin symbol is the given conjugacy class. The same separation of primes is done in our proof by the fixed field D of $\tilde{\tau}$, and we manage to avoid class field theory.

3. Constant Field Extensions

It is easier to count the number of primes in C of higher degrees for cyclic extensions. In the reduction to the case of degree 1 primes, which is treated in Lemma 1, we would like to avoid primes of small degrees. Therefore, we prove:

Lemma 2. *Let E' be a finite extension of E and let K_b be the algebraic closure of K in E'. For a multiple k of b let*

$$P'_{k/b}(E'/E) = \{\mathfrak{p}' \in P_{k/b}(E') \mid \deg(\mathfrak{p}' \cap E) \neq k\}.$$

Then we have for $\varepsilon > \frac{1}{2}$ that

$$|P'_{k/b}(E'/E)| = 0(q^{\varepsilon k}) \qquad k \to \infty.$$

Proof. If $\mathfrak{p}' \in P'_{k/b}(E'/E)$, then $\bar{E}'_{\mathfrak{p}'} = K_k$ and the residue field of $\mathfrak{p} = E \cap \mathfrak{p}'$ is K_j, where j is a proper divisor of k; hence, $j \leqq \frac{k}{2}$. Over every such $\mathfrak{p}$ there lie at most $[E' : E]$ elements of $P(E')$. Hence,

$$|P'_{k/b}(E'/E)| \leqq [E' : E] \sum_{j \leqq \frac{k}{2}} |P_j(E)| = 0\left(\frac{k}{2} q^{k/2}\right) = O(q^{\varepsilon k}),$$

where we have used the simple estimation $|P_j(E)| = O(q^j)$. □

Lemma 3. *Assume that F/E is a cyclic extension and that the unique element τ of $\mathfrak{E}$ generates $\mathfrak{G}(F/E)$. Let k be a positive integer such that*

$$\mathrm{res}_L \tau = \mathrm{res}_L \varphi^k \tag{8}$$

and let $\varepsilon > \frac{1}{2}$. Then

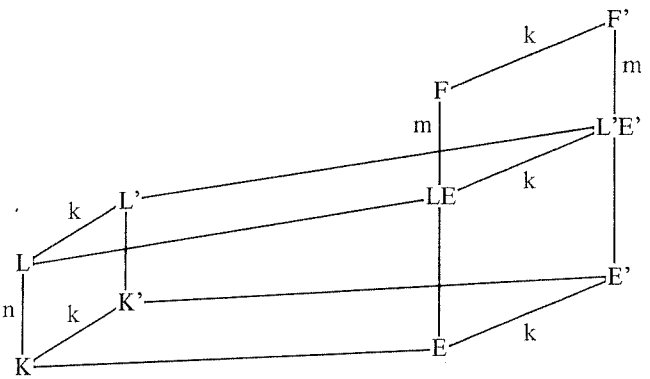
$$|C_k(E)| = \frac{1}{km} q^k + O(q^{\varepsilon k}) \qquad k \to \infty .$$

Proof. Let $K' = K_k$, $L' = LK'$, $E' = EK'$, and $F' = L'F$. Then K' is algebraically closed in E', the field F' is a cyclic extension of E' and L' is the algebraic closure of K' in F'. Also, (8) implies that $L \cap K' = K$. Hence

$$[K' : K] = [L' : L] = [E' : E] = [L'E' : LE] = [F' : F] = k$$

and

$$[F' : L'E'] = [F : LE] = m .$$



Another use of (8) implies that there exists a $\tau' \in \mathrm{Aut}\, F'$ such that $\mathrm{res}_F \tau' = \tau$ and $\mathrm{res}_{L'} \tau' = \mathrm{res}_{L'} \varphi^k$. Then τ' fixes the elements of K' and therefore belongs to $\mathfrak{G}(F'/E')$. Let $C_1(E')$ be the set of all $\mathfrak{p}' \in P(E')$ of degree 1 (over K') such that $\left(\frac{F'/E'}{\mathfrak{p}'}\right) = \{\tau'\}$. Note that F and F' have the same genus and that $[F' : K'(t)] = [F : K(t)]$, since F' is a separable constant field extension of F. Hence we may apply Lemma 1 to E' and conclude that

$$|C_1(E')| = \frac{1}{m} q^k + O(q^{k/2}) \qquad k \to \infty . \tag{9}$$

Let $C_1'(E') = \{\mathfrak{p}' \in C_1(E') \mid \deg(E \cap \mathfrak{p}') = k\}$. Then (9) and Lemma 2 imply that

$$|C_1'(E')| = \frac{1}{m} q^k + O(q^{\varepsilon k}) \qquad k \to \infty . \tag{10}$$

We compare $C_k(E)$ and $C_1'(E')$. Over every element $\mathfrak{p}$ of $C_k(E)$ there exist exactly k prime ideals $\mathfrak{p}_1', \ldots, \mathfrak{p}_k'$ of $O_{E'}$. Then $\mathfrak{p}_1', \ldots, \mathfrak{p}_k'$ are unramified in F' and of degree 1 over K'. Let $\mathfrak{P}_1', \ldots, \mathfrak{P}_k'$ be the elements of $P(F')$ lying over $\mathfrak{p}_1', \ldots, \mathfrak{p}_k'$, respectively, and let $\mathfrak{P}_i = F \cap \mathfrak{P}_1'$, for $i = 1, \ldots, k$. Then

$$x \in O_F \;\Rightarrow\; \tau' x = \tau x \equiv x^{q^k} \bmod \mathfrak{P}_i$$

$$x \in L' \;\Rightarrow\; \tau' x = \varphi^k x = x^{q^k} .$$

Hence $\tau' x \equiv x^{Np_i'} \bmod \mathfrak{P}_i'$ for every $x \in O_{F'} = L' O_F$, which means that $\left(\frac{F'/E'}{\mathfrak{p}_i}\right) = \{\tau'\}$. Thus $\mathfrak{p}_i' \in C_1'(E')$. Conversely, if $\mathfrak{p}' \in C_1'(E')$, then $E \cap \mathfrak{p}' \in C_k(E)$. The asymptotic formula of the lemma follows therefore from (10). □

4. Reduction to the Cyclic Case

In this section we use a well known idea of Deuring [5] and reduce the counting of the number of elements in $C_k(E)$ in the general case to the case, settled in Sect. 3, where F/E is a cyclic extension.

Lemma 4. *Let a and k be positive integers and assume that every element τ of $\mathfrak{E}$ satisfies*

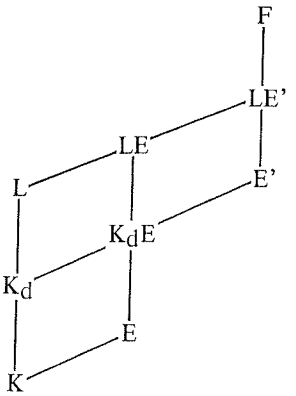
$$\operatorname{res}_L \tau = \operatorname{res}_L \varphi^a. \tag{11}$$

a) *If $k \not\equiv a \bmod n$, then $C_k(E)$ is empty.*
b) *If $k \equiv a \bmod n$ and if $\varepsilon > \frac{1}{2}$, then*

$$|C_k(E)| = \frac{c}{km} q^k + O(q^{\varepsilon k}) \qquad k \to \infty.$$

Proof. a) If $C_k(E)$ contains a prime $\mathfrak{p}$ and if $\mathfrak{P} \in P(F)$ lies over $\mathfrak{p}$, then $\operatorname{res}_L\left[\frac{F/E}{\mathfrak{P}}\right] = \operatorname{res}_L \varphi^k$ on one hand, and by (11), $\operatorname{res}_L\left[\frac{F/E}{\mathfrak{P}}\right] = \operatorname{res}_L \varphi^a$, on the other hand. Hence $k \equiv a \bmod n$.

b) The algebraic closure of K in the fixed field $E' = F(\tau)$ of τ is K_d, where $d = gcd(a, n) = gcd(k, n)$. Let $m' = [F : LE']$ and consider the following diagram of fields.



Let $C_{k/d}'(E') = \left\{\mathfrak{p}' \in P(E') \,\middle|\, \left(\frac{F/E'}{\mathfrak{p}'}\right) = \{\tau\},\ \deg \mathfrak{p}' = \frac{k}{d},\ \mathfrak{p}' \text{ is unramified over } E \text{ and } \deg(E \cap \mathfrak{p}') = k\right\}$. By Lemmas 3 and 2

$$|C_{k/d}'(E')| = \frac{d}{km'} (q^d)^{k/d} + O\left(q^{d\varepsilon \cdot \frac{k}{d}}\right) = \frac{d}{km'} q^k + O(q^{\varepsilon k}), \qquad k \to \infty. \tag{12}$$

We define a map $h: C'_{k/d}(E') \to C_k(E)$ by $h(\mathfrak{p}') = E \cap \mathfrak{p}'$. Indeed, let $\mathfrak{p}' \in C'_{k/d}(E')$ and $\mathfrak{p} = E \cap \mathfrak{p}'$. Then $\left(\frac{F/E'}{\mathfrak{p}'}\right) = \{\tau\}$ and therefore there exists a unique element $\mathfrak{P} \in P(F)$ over $\mathfrak{p}'$ and it satisfies $\left[\frac{F/E'}{\mathfrak{P}}\right] = \tau$. Moreover, since $N\mathfrak{p} = N\mathfrak{p}'$, we have $\tau = \left[\frac{F/E}{\mathfrak{P}}\right]$, hence $\mathfrak{p} \in C_k(E)$.

Conversely, if $\mathfrak{p} \in C_k(E)$ and if $\mathfrak{P} \in P(F)$ lies over $\mathfrak{p}$ and satisfies $\left[\frac{F/E}{\mathfrak{P}}\right] = \tau$, then with $\mathfrak{p}' = E' \cap \mathfrak{P}$, we have $\bar{E}'_{\mathfrak{p}'} = \bar{E}_{\mathfrak{p}}$. Hence $\mathfrak{p}' \in C'_{k/d}(E')$ and $h(\mathfrak{p}') = \mathfrak{p}$.

The order of $h^{-1}(\mathfrak{p})$ is therefore equal to the number of $\mathfrak{Q} \in P(F)$ that lie over $\mathfrak{p}$ and satisfy $\left[\frac{F/E}{\mathfrak{Q}}\right] = \tau$. They are all conjugate to $\mathfrak{P}$ by elements of the centralizer $C_G(\tau)$. Hence

$$|h^{-1}(\mathfrak{p})| = \frac{|C_G(\tau)|}{|D(\mathfrak{P})|} = \frac{|G|}{|D(\mathfrak{P})| \cdot |\mathfrak{E}|} = \frac{[E':E]}{c},$$

where $D(\mathfrak{P}) = G(F/E')$ is the decomposition group of $\mathfrak{P}$ in G. It follows by (12) that

$$\begin{aligned} |C_k(E)| &= \frac{dc}{km'[E':E]} q^k + O(q^{\varepsilon k}) \\ &= \frac{c}{km} q^k + O(q^{\varepsilon k}), \qquad k \to \infty. \end{aligned}$$

5. Summing Up

The fourth step in the proof is to sum up the $|C_k(E)|$'s according to Lemma 4. But first we need an auxiliary result.

Lemma 5. *Let a and n be positive integers. Then*

$$\sum_{j=0}^{\infty} \frac{x^{a+jn}}{a+jn} = -\frac{1}{n} \log(1-x) + O(1) \qquad x \to 1^-.$$

Proof[1]. If $\zeta \neq 1$ is an n-th root of unity, then $1 + \zeta + \ldots + \zeta^{n-1} = 0$. Hence

$$-\frac{1}{n} \sum_{\zeta^n = 1} \log(1-\zeta x)\zeta^{-a} = \frac{1}{n} \sum_{k=1}^{\infty} \frac{x^k}{k} \sum_{\zeta^n = 1} \zeta^{k-a} = \sum_{\substack{k=1 \\ k \equiv a \bmod n}}^{\infty} \frac{x^k}{k}$$

If $\zeta \neq 1$, then $\log(1-\zeta x)$ is bounded as $x \to 1^-$, and the lemma follows.

Lemma 6. *If $0 < a \leqq n$ is an integer such that $\mathrm{res}_L \tau = \mathrm{res}_L \varphi^a$ for every $\tau \in \mathfrak{E}$, then*

$$\sum_{\mathfrak{p} \in C} N\mathfrak{p}^{-s} = -\frac{c}{[F:E]} \log(1 - q^{1-s}) + O(1) \qquad s \to 1^+. \tag{13}$$

1 The author is indebted to David Hayes for this proof

Proof. Fix an $\frac{1}{2}<\varepsilon<1$ and apply Lemmas 4 and 5 for $x=q^{1-s}$ to compute

$$\begin{aligned}\sum_{\mathfrak{p}\in C} N\mathfrak{p}^{-s} &= \sum_{j=0}^{\infty} \sum_{\mathfrak{p}\in C_{a+jn}(E)} N\mathfrak{p}^{-s} \\ &= \sum_{j=0}^{\infty} \left(\frac{c}{m(a+jn)} q^{a+jn} + O(q^{\varepsilon(a+jn)})\right) q^{-(a+jn)s} \\ &= \frac{c}{m} \sum_{j=0}^{\infty} \frac{q^{(1-s)(a+jn)}}{a+jn} + O\left(q^{(\varepsilon-s)a} \sum_{j=0}^{\infty} q^{(\varepsilon-s)jn}\right) \\ &= -\frac{c}{mn}\log(1-q^{1-s}) + O(1) + O\left(\frac{q^{(\varepsilon-s)a}}{1-q^{(\varepsilon-s)n}}\right) \\ &= -\frac{c}{[F:E]}\log(1-q^{1-s}) + O(1), \qquad s\to 1^+. \quad \square\end{aligned}$$

In the special case where $F=E$, Lemma 6 simplifies to

$$\sum_{\mathfrak{p}\in P(E)} N\mathfrak{p}^{-s} = -\log(1-q^{1-s}) + O(1) \qquad s\to 1^+. \tag{14}$$

Dividing up (13) by (14) and going to the limit, we find that the Dirichlet density of C is

$$\delta(C) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in C} N\mathfrak{p}^{-s}}{\sum_{\mathfrak{p}\in P(E)} N\mathfrak{p}^{-s}} = \frac{c}{[F:E]}.$$

Thus the Čebotarev density theorem for function fields has been completely proved.

References

1. Artin, E.: Über eine neue Art von L-Reihen. Abh. Math. Sem. Univ. Hamburg **3**, 89–108 (1924)
2. Artin, E.: Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz. Abh. Math. Sem. Univ. Hamburg **5**, 353–363 (1927)
3. Ax, J.: The elementary theory of finite fields. Ann. Math. **88**, 239–271 (1968)
4. Čebotarev, N.: Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. Math. Ann. **95**, 191–228 (1926)
5. Deuring, M.: Über den Tchebotareffschen Dichtigkeitssatz. Math. Ann. **110**, 414–415 (1934)
6. Fried, M.: On Hilbert's irreducibility theorem. J. Number Theory **6**, 211–231 (1974)
7. Jarden, M.: Elementary statements over large algebraic fields. Trans. AMS **164**, 67–91 (1972)
8. Lang, S.: Algebraic number theory. Reading: Addison-Wesley 1970
9. Neukirch, J.: Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper. Invent. Math. **6**, 296–314 (1969)
10. Samuel, P.: Lectures on old and new results on algebraic curves. Tata Institute for Fundamental Research, Bombay 1966
11. Serre, J.-P.: Zeta and L functions. In: Arithmetical algebraic geometry, pp. 82–92. Schilling, O.F.G., ed. New York: Harper & Row 1965
12. Zariski, O., Samuel, P.: Commutative algebra. I. Berlin, Heidelberg, New York: Springer 1975

Received February 18, 1982; in revised form May 22, 1982