

THE FAREY DENSITY OF NORM SUBGROUPS OF GLOBAL FIELDS (II)

by S. D. COHEN and R. W. K. ODoni

(Received 25 June, 1975)

0. Introduction. In this paper we shall derive for function fields in one variable over finite constant fields results analogous to [1], where algebraic number fields were considered. The ground field \mathbf{P} will be the set of all rational functions in a given transcendent X , with coefficients in $k = \text{GF}(q)$, $q = p^r$, p a prime; thus $\mathbf{P} = k(X)$.

The main new difficulties encountered are the possible existence of inseparable elements in the finite extension Ω/\mathbf{P} , and also the occurrence of constant field extensions. The former phenomenon is overcome in §1 by the device of replacing \mathbf{P} by a suitable purely inseparable extension $K \subseteq \Omega$ for which “descent by norms” to \mathbf{P} behaves in a reasonable manner. We then attempt to imitate where possible the processes of [1] applied to Ω/K . The presence of constant field extensions inevitably complicates the analysis, since the “obvious” analogue of Čebotarëv’s density theorem is unexpectedly false in this case. We append to this paper a section on the appropriate Čebotarëv theorem which, we hope, will fill the gap in the literature of this intriguing topic.

Section 2 of this paper corresponds broadly to §1 of [1], and in it we prove

THEOREM IIA. *Let $\text{GF}(q^f)$ be the constant field of Ω , a finite extension of \mathbf{P} . Then the number of integral ideals of $k[X]$ which have degree d , are prime to a given ideal \mathfrak{n} , and are norms of fractional ideals of Ω is zero unless f divides d , in which case the number is asymptotically*

$$C(\Omega)q^d d^{B-1} \lambda_{\mathfrak{n}}^{-1} \{1 + O(d^{-A} \omega^4(\mathfrak{n}))\} + O(q^{d/2} \cdot \exp 2\sqrt{d\omega(\mathfrak{n})}) \quad (\text{IIA})$$

where $C(\Omega)$, A and B are positive constants depending only on Ω and \mathbf{P} (in fact, $0 < B < 1$), the O -term is uniform for all d , \mathfrak{n} , and

$$\lambda_{\mathfrak{n}} = \prod_{\mathfrak{p}|\mathfrak{n}} \{1 + \delta(\mathfrak{p})q^{-\text{deg } \mathfrak{p}} + \delta(\mathfrak{p}^2)q^{-2 \text{ deg } \mathfrak{p}} + \dots\} \quad (0.1)$$

while $\omega(\mathfrak{n})$ is the number of distinct prime divisors of \mathfrak{n} .

Here, for finite divisors \mathfrak{a} in \mathbf{P} , $\delta(\mathfrak{a}) = 1$ if \mathfrak{a} is the Ω/\mathbf{P} -norm of some divisor of Ω , and is 0 otherwise. If $\bar{\Omega}/\mathbf{P}$ is the normal hull of Ω/\mathbf{P} then B can be interpreted as the relative size in $\text{Gal } \bar{\Omega}/K$ of a certain set of conjugacy classes (see the end of §2 for precise details).

A rather deeper problem is that of finding the number of polynomials $a(X)$ of degree $d \equiv 0 \pmod{f}$ which are Ω/\mathbf{P} -norms of elements of Ω ; as in the corresponding problem in [1] we are led to the use of class-field theory in order to obtain the solution. (A convenient general reference for the classical treatment of class-field theory for function fields is F. K. Schmidt [2].)

In §3 we obtain the following result.

Glasgow Math. J. **18** (1977) 57–67.

THEOREM IIB. *There exists a certain abelian extension $\Omega^\#/\Omega$ of finite degree, involving a constant field extension of degree F , say, with the following properties:*

(a) *if d is a large multiple of fF , then the number of polynomials in X of degree d which are Ω/\mathbf{P} -norms of elements of Ω , and are prime to \mathbf{n} , is asymptotically*

$$F\kappa\lambda_n^{-1}C(\Omega)\frac{q^d \cdot d^{B-1}}{[\Omega^\# : \Omega]} \{1 + O(\omega^A(\mathbf{n})d^{-A'})\} + O(q^{d/2} \exp(2\sqrt{d\omega(\mathbf{n})})) \tag{IIB}$$

where κ is the number of non-zero elements of $\text{GF}(q)$ which are Ω/\mathbf{P} -norms and A' is positive;

(b) *if d is not a multiple of fF , the number in question is only*

$$O(q^d d^{B-1-A'} \cdot \omega^A(\mathbf{n})) + O(q^{d/2} \exp(2\sqrt{d\omega(\mathbf{n})})).$$

In Theorem IIB the constants involved in the O -symbols may be taken uniform in d and \mathbf{n} . The reader is invited to note the curious influence of the constant field extensions in Theorems IIA and IIB.

In §4 we obtain results resembling those of [1, §3]; we define the *Farey section $\mathcal{F}(D)$ of order D* in \mathbf{P} to be the set of all reduced fractions $a(X)/b(X)$ with $b(X)$ monic and $\deg a(X) < \deg b(X) \leq D$. If \mathcal{N} is the set of Ω/\mathbf{P} -norms of elements of Ω , it is natural to call $\text{card } \mathcal{F}(D) \cap \mathcal{N} / \text{card } \mathcal{F}(D)$ the *Farey density of \mathcal{N}* . A straightforward imitation of [1, §3] then yields

THEOREM IB. *If $D \rightarrow \infty$ through multiples of f , we have*

$$D^{2(1-B)} \text{card } \mathcal{F}(D) \cap \mathcal{N} / \text{card } \mathcal{F}(D) \rightarrow \text{a positive limit} \tag{IB}$$

(with B as in Theorem IIA).

We do not include an analogue of Theorem IA of [1], leaving the formulation and proof to the interested reader.

We are indebted to Professor D. Rees of Exeter University for some helpful remarks in connection with §1 of this paper.

1. Lifting the ground field. We allow the possibility that Ω/\mathbf{P} be inseparable, and we wish to assess the damage thus inflicted. We prove two straightforward lemmas which enable us to remove the inseparability.

LEMMA 1.1. *Let F be a perfect field of characteristic $p \neq 0$. If X is an indeterminate and Ω is a finite extension of $F(X)$ of degree of inseparability p^i , then $\Omega = KS$, where $K = F(X^{p^{-i}})$ and S is the maximal subfield of Ω separable over $F(X)$; in particular Ω/K is separable.*

Proof. We write $H = F(X)$, $x^{p^i} = X$. Then $K = H(x)$. We assert that $K\Omega/K$ is separable. Indeed, let $\omega \in \Omega$, so that $\omega^{p^i} \in S$ and ω^{p^i} satisfies a separable equation $\sum a_j(X)\omega^{jp^i} = 0$, where we may assume $a_j(X) \in F[X]$. Since F is perfect, we have $a_j(X) = (a_j^*(x))^{p^i}$, where $a_j^*(x) \in K$. Then $\sum a_j^*(x)\omega^j = 0$ is a separable equation for ω over K .

Now $K\Omega$ is purely inseparable over S , whence also over KS , while, as $K\Omega/K$ is separable,

so is $K\Omega/KS$. We deduce that $K\Omega = KS$, whence $\Omega \subseteq KS$. But $[\Omega : S] = p^i = [KS : S]$, since $K \cap S = H$. We deduce that $\Omega = KS$, and that Ω/K is separable.

Let us now assume that $F = k = GF(q)$ and, as before, let $x^{p^i} = X$. Then $K = \mathbf{P}(x)$. We consider the norm map $N : K^* \rightarrow \mathbf{P}^*$. It is obtained by taking ξ to ξ^{p^i} , $\xi \in K^*$, and so N is bijective. Further, the norm map from fractional ideals of $k[x]$ to those of $k[X]$ is bijective and, in fact, degree-preserving.

We may deduce

LEMMA 1.2. *The fractional ideal $(f(X))$ in \mathbf{P} is the Ω/\mathbf{P} -norm of some fractional ideal of Ω if and only if the fractional ideal $(f(X)^{p^{-i}})$ in K is the Ω/\mathbf{P} -norm of some fractional ideal of Ω . Similarly, $g(X) \in N_{\Omega/\mathbf{P}}(\Omega^*)$ if and only if $(g(X))^{p^{-i}} \in N_{\Omega/K}(\Omega^*)$.*

Since $g(X)$ as a rational function of X has the same net degree as $\{g(X)\}^{p^{-i}}$ as a rational function of x , we now see that we need only work with Ω/K rather than Ω/\mathbf{P} in the sequel, and we shall do so.

NOTATION FOR §2 ONWARDS

- $\mathfrak{p}, \mathfrak{q}$ —finite prime divisors in K or, occasionally, the corresponding prime ideals of $k[x]$.
- $\mathfrak{a}, \mathfrak{b}, \mathfrak{n}$ —finite divisors of K .
- $\hat{\mathfrak{a}}$ —any divisor in Ω with $N_{\Omega/K}\hat{\mathfrak{a}} = \mathfrak{a}$.
- k — $GF(q)$.
- $N_G(\sigma)$ —normaliser in G of $\sigma \in G$.
- $\text{ord}_G \sigma$ —order of σ with respect to G .
- $\omega(\mathfrak{n})$ —number of distinct prime divisors of \mathfrak{n} .

2. Norms of fractional ideals. Our aim here is to prove Theorem IIA, and thus we need to obtain an asymptotic expansion for $\sum \delta(\mathfrak{a})$, where $\delta(\mathfrak{a}) = 1$ or 0 according as or not the K -fractional ideal \mathfrak{a} is the Ω/K -norm of some Ω -fractional ideal, and the sum is taken over all integral ideals of degree d which are prime to \mathfrak{n} . Our approach will be based on an analysis of the “ Dirichlet series ”

$$f(\mathfrak{n}; t) = \sum_{\substack{\mathfrak{a} \text{ integral} \\ (\mathfrak{a}, \mathfrak{n}) = 1}} \delta(\mathfrak{a}) t^{\text{deg } \mathfrak{a}}, |t| < q^{-1}. \tag{2.1}$$

We observe first (c.f. [1, Lemma 1.1]) that the function δ is multiplicative, i.e. if \mathfrak{a} and \mathfrak{b} are coprime fractional ideals in K , then $\delta(\mathfrak{a}\mathfrak{b}) = \delta(\mathfrak{a})\delta(\mathfrak{b})$. Thus, for $|t| < q^{-1}$, we have “ Euler products ”

$$f(\mathfrak{n}; t) = \lambda_{\mathfrak{n}}^{-1}(t) f(t) \tag{2.2}$$

where

$$\lambda_{\mathfrak{n}}(t) = \prod_{\mathfrak{p}|\mathfrak{n}} \{1 + \delta(\mathfrak{p})t^{\text{deg } \mathfrak{p}} + \delta(\mathfrak{p}^2)t^{2 \text{deg } \mathfrak{p}} + \dots\} \tag{2.3}$$

and

$$f(t) = \prod_{\mathfrak{p}} \{1 + \delta(\mathfrak{p})t^{\text{deg } \mathfrak{p}} + \delta(\mathfrak{p}^2)t^{2 \text{deg } \mathfrak{p}} + \dots\}. \tag{2.4}$$

The rational function $\lambda_n(t)$ has no poles or zeros in $|t| < 1$ and thus any singularities possessed by $f(\mathbf{n}, t)$ for $|t| < 1$ must be due to $f(t)$. We now analyse $f(t)$ and its analytic continuations when t is small. The product (2.4) shows that $f(t)$ has no zero or pole for $|t| < q^{-1}$, so we may take logarithms, obtaining

$$\log f(t) = \sum_{\mathbf{p}} \log(1 + \delta(\mathbf{p})t^{\deg \mathbf{p}} + \delta(\mathbf{p}^2)t^{2 \deg \mathbf{p}} + \dots), \quad |t| < q^{-1} \tag{2.5}$$

Using a little care, especially when q is small, we see that irreducibles \mathbf{p} for which $\delta(\mathbf{p})=0$ contribute to (2.5) a term which is regular and bounded by $\log(1/1 - q^{-2\epsilon})$ for $|t| \leq q^{-\frac{1}{2} - \epsilon}$ (for any $\epsilon > 0$). It follows that any singularity of $\log f(t)$ or its analytic continuations which occur in $|t| < q^{-\frac{1}{2} - \epsilon}$ must be due to the term

$$\sum_{\delta(\mathbf{p})=1} \log \frac{1}{1 - t^{\deg \mathbf{p}}}. \tag{2.6}$$

By expanding the logarithms in (2.6) in powers of t we obtain

$$\log f(t) = \sum_{\mathbf{p}} \delta(\mathbf{p})t^{\deg \mathbf{p}} + A(t) \tag{2.7}$$

for small t , where $A(t)$ is regular and $|A(t)| < C \log \frac{1}{1 - q^{-2\epsilon}}$ (C absolute) for $|t| \leq q^{-\frac{1}{2} - \epsilon}$.

Let $\bar{\Omega}/K$ be the Galois hull of Ω/K ; then the condition $\delta(\mathbf{p}) = 1$ (for unramified \mathbf{p}) is equivalent to the Frobenius class $\left(\frac{\bar{\Omega}/K}{\mathbf{p}}\right)$ consisting only of elements (regarded as transitive permutations on the conjugates of a primitive element of Ω/K) whose cycle patterns have cycle lengths with highest common factor unity (c.f. [1, §1]). Let Λ be the set of cycle patterns with the latter property. Then, by (A3) of the appendix (with $L = \bar{\Omega}$), we obtain

$$\sum_{\mathbf{p}} \delta(\mathbf{p})t^{\deg \mathbf{p}} = \sum_{n=1}^{\infty} \frac{q^n t^n \text{card } G_{(n,h)}^{\Lambda}}{n \text{card } G_{(n,h)}} + O\left(\frac{1}{1 - q^{1/2} |t|}\right) \tag{2.8}$$

for small t , where $\text{GF}(q^h)$ is the constant field of $\bar{\Omega}$ and $G_d^{\Lambda} = \bigcup_{\lambda \in \Lambda} G_d^{\lambda}$, all notations of the appendix being preserved.

Let $\text{GF}(q^f) = k_f$ be the constant field of Ω , and suppose $h = fg$. If $\delta(\mathbf{p}) = 1$, then \mathbf{p} must be a norm from Kk_f , and this clearly implies $\deg \mathbf{p} \equiv 0 \pmod{f}$. Hence, writing $B_d = \text{card } G_{df}^{\Lambda} / \text{card } G_{df}$ for each divisor d of g , we find from (2.7) and (2.8) that

$$\log f(t) = C(t) + \sum_{m=1}^{\infty} B_{(m,g)} t^{mf} q^{mf} / mf \tag{2.9}$$

where $C(t)$ is regular and $O_q\left(\frac{1}{1 - q^{-\epsilon}}\right)$ for $|t| \leq q^{-\frac{1}{2} - \epsilon}$.

By elementary manipulations involving the Möbius function $\mu(n)$, we can write

$$\sum_{m=1}^{\infty} B_{(m,g)} t^{mf} q^{mf} / mf = \frac{1}{f} \sum_w \frac{1}{g} \sum_d \frac{1}{w} B_d \mu\left(\frac{w}{d}\right) \log \frac{1}{1 - q^{fw} t^{fw}} \tag{2.10}$$

for small t . Using (2.9) and (2.10) we thus have

$$f(t) = E(t) \prod_{w|g} (t^{fw} - q^{-fw})^{-(fw)^{-1} \sum_{d|w} B_d \mu(w/d)} \tag{2.11}$$

where $E(t)$ is regular, non-zero and $O_q\left(\exp \frac{1}{1-q^{-\epsilon}}\right)$ for $|t| \leq q^{-\frac{1}{2}-\epsilon}$.

Now if $r|g$ and ζ is a primitive r th root of unity, then the net exponent to which the factor $(t^f - \zeta q^{-f})$ occurs in (2.11) is

$$C_r = -f^{-1} \sum_{r|w|g} w^{-1} \sum_{d|w} B_d \mu(w/d) = -f^{-1} \sum_{d|g} B_d \sum_{\substack{w|g \\ r,d|w}} w^{-1} \mu(w/d); \tag{2.12}$$

in particular, if $r = 1$, we have

$$C_1 = -f^{-1} g^{-1} \sum_{d|g} B_d \phi(g/d) \tag{2.13}$$

where ϕ is Euler's totient function. We now show that C_1 is the dominant exponent in (2.11).

LEMMA 2.1. $C_r > C_1$ provided $r > 1$.

Proof. The numbers B_d are all non-negative. Thus (2.12) implies

$$-fC_r \leq \sum_{d|g} B_d \left| \sum_{\substack{w|g \\ r,d|w}} w^{-1} \mu(w/d) \right| \tag{2.14}$$

with strict inequality should any of the inner sums for which $B_d > 0$ be negative. However,

$$\sum_{\substack{w|g \\ r,d|w}} w^{-1} \mu(w/d) = \frac{\mu(r_1)\phi(M)}{r_1 dM},$$

where $r_1 = r/(r, d)$ and M is the largest divisor of g/dr_1 prime to r_1 . Since

$$\left| \mu(r_1)\phi(M)/r_1 dM \right| \leq \phi(g/d)/d,$$

we have $C_r \geq C_1$ by (2.13) and for equality we need that $\mu(r_1) = 1$ for all $d|g$ with $B_d > 0$. Further, for such d we also need $\mu(r_1)\phi(M)/r_1 dM = \phi(g/d)/d$ which implies $r_1 = 1$. Hence $r|d$ for each $d|g$ with $B_d > 0$. However, $B_1 \neq 0$, since G_f contains elements involving 1-cycles (c.f. [5, (5.3)]).

We now imagine the t -plane cut along the radii $\arg t = \arg \omega$, $\omega^h = 1$, $|t| \geq q^{-1}$. Let \mathcal{C} be the anticlockwise circle $|t| = q^{-\epsilon-\frac{1}{2}}$, indented by lacets around each branch cut. It is clear that $\sum_{\deg \mathbf{a} = d} \delta(\mathbf{a}) = 0$ unless $f|d$, and that in general

$$\sum_{\deg \mathbf{a} = d} \delta(\mathbf{a}) = \frac{1}{2\pi i} \int_{\mathcal{C}} f(t) t^{-1-d} dt. \tag{2.15}$$

We now assume that $f|d$. The contribution to the right-hand side of (2.15) due to parts of \mathcal{C} other than the lacets is readily seen to be $O_q(\exp \sqrt{d} \cdot q^{d/2})$, by taking $q^\epsilon = 1 + d^{-\frac{1}{2}}$ so that

$\varepsilon \equiv (\log qd^{\frac{1}{f}})^{-1}$. Each lacet corresponding to an f th root of unity contributes

$$\frac{C(\Omega)}{f} q^d d^{B-1} \{1 + O_{\Omega}(d^{-1})\} \tag{2.16}$$

where $B = -C_1 > 0$ and $C(\Omega) > 0$; this is obtained from a straightforward argument involving beta- and gamma-functions. The remaining lacets contribute $O_q(q^d d^{-1+B^*}) + O_q(q^d \cdot d^{-1})$, where $B^* = \max_{r \geq 2} \{-C_r\}$.

We now identify the exponent B which, by (2.13), is $B = (fg)^{-1} \sum_{d|g} B_d \phi(g/d)$. We have $\text{card } G_{df} = \phi(g/d) \text{card } G/fg$ by simple Galois theory, G being $\text{Gal } \overline{\Omega}/K$ (c.f. [5, Lemma 1]). Consequently, from (2.8), $B = \frac{1}{\text{card } G} \sum_{d|g} \text{card } G_{df}^{\Lambda}$, i.e. B is the proportion of elements of G of cycle pattern belonging to Λ , since $\delta(\mathbf{p}) = 1$ implies that \mathbf{p} splits in Kk_f . This is precisely what one would expect from [1].

Finally, Theorem IIA now follows on replacing $f(t)$ by $f(\mathbf{n}, t)$ in the above analysis. We need the following bounds on the size of $|\lambda_{\mathbf{n}}(t)|$:

$$\text{if } |t| = q^{-1} \text{ then } |\lambda_{\mathbf{n}}(t)|^{\pm 1} < k\omega(\mathbf{n})^2 \tag{2.17}$$

where k depends at most on q ; and

$$\text{if } |t| \leq q^{-\frac{1}{2}} \text{ then } |\lambda_{\mathbf{n}}(t)|^{\pm 1} < k' \exp 2\sqrt{\omega(\mathbf{n})} \tag{2.18}$$

where k' depends at most on q . Both (2.17) and (2.18) arise from extravagant estimation applied to (2.3), using the trivial fact that there are q^r integral ideals of degree r in $k[x]$. These estimates are applied in assessing the contribution to the contour integral analogous to (2.15) of the minor singularities and the portion with $|t| = q^{-\frac{1}{2}-\varepsilon}$.

3. Integral ideals which are norms of principal fractional ideals. Let ∞ denote the valuation of K obtained by assigning to $f(x)/g(x)$ the value $\deg g(x) - \deg f(x)$. By abuse of language and notation, we use ∞ also to denote the divisor $\sum V$ taken over all valuations V (of a given extension field) which extend ∞ . We now consider in Ω the group \mathcal{D} of all divisors, and in it the subgroup \mathcal{D}^{∞} consisting of those divisors prime to ∞ . There is a natural surjection $\phi : \mathcal{D} \rightarrow \mathcal{D}^{\infty}$ obtained by “forgetting components at ∞ ”. We define a subgroup \mathcal{G} of \mathcal{D}^{∞} as follows: the divisor $\mathbf{d} \in \mathcal{D}^{\infty}$ is in \mathcal{G} if and only if $N_{\Omega/K} \mathbf{d} = N_{\Omega/K} \phi(\text{div } \alpha)$ for some $\alpha \in \Omega^*$, where $\text{div } \alpha$ is the “divisor of poles and zeros” of α . It is clear that \mathcal{G} contains all $\text{div } \beta$ where $\beta \equiv 1 \pmod{\infty}$, i.e. $V(\beta - 1) > 0$ for all V/∞ . We assert that $(\mathcal{D}^{\infty} : \mathcal{G})$ is finite; it is enough to show that \mathcal{G} contains a divisor of non-zero degree. Choose $\gamma \in \Omega^*$ such that $V(\gamma) = 1$ for all V/∞ . (This is possible by the approximation theorem, since only finitely many V/∞ .) Then $\phi(\text{div } \gamma) = \sum_{V/\infty} V(\gamma) \cdot V$ and so $\deg \phi(\text{div } \gamma) = \deg(\text{div } \gamma) - \sum_{V/\infty} \deg V < 0$. Since $\phi(\text{div } \gamma) \in \mathcal{G}$, the result follows.

Corresponding to the quotient $\mathcal{D}^{\infty}/\mathcal{G}$ (whose conductor divides ∞) there is a classfield extension $\Omega^{\#}/\Omega$ ramified at most at ∞ . In terms of fractional ideals in Ω , we can say interpret \mathcal{G} as “the set of all fractional ideals \mathfrak{A} in Ω such that $N_{\Omega/K} \mathfrak{A} = N_{\Omega/K}((\alpha))$ for some $\alpha \in \Omega^*$ ”.

This is allowable by the canonical correspondence between fractional ideals and divisors in \mathcal{D}^∞ . Thus we have to some extent preserved the analogy with [1]. If Ω/K were normal, then $\Omega^\# / K$ would be normal, since \mathcal{G} is invariant under all K -automorphisms of Ω ; further we would have $\text{Gal } \Omega^\# / \Omega$ contained in the centre of $\text{Gal } \Omega^\# / K$, by an easy argument. When Ω/K is not normal, we consider instead the extension $\bar{\Omega}^\# / \bar{\Omega}$, obtained as classfield to the partition in $\bar{\Omega}$ given by \mathcal{D}^∞ modulo those $\mathfrak{d} \in \mathcal{D}^\infty$ such that $N_{\bar{\Omega}/K} \mathfrak{d} = N_{\bar{\Omega}/K} \phi(\text{div } \alpha)$ for some $\alpha \in \bar{\Omega}^*$. The transitivity of the norm shows that $\bar{\Omega}^\# \subseteq \bar{\Omega}^\#$. Then $\text{Gal } \bar{\Omega}^\# / \bar{\Omega}^\#$ is a normal subgroup of $\text{Gal } \bar{\Omega}^\# / \bar{\Omega}$ which is itself in the centre of $\text{Gal } \bar{\Omega}^\# / K$. It follows that $\bar{\Omega}^\# / K$ is normal (c.f. [1, p. 164]).

We wish to obtain an asymptotic expansion for $\sum' 1$ taken over all integral ideals of degree d which are norms of principal fractional ideals of Ω . Clearly $\delta(\mathfrak{a}) = 1$ for all such integral ideals \mathfrak{a} . Let χ run through all characters of $\mathcal{D}^\infty / \mathcal{G}$; then the indicator $\delta_0(\mathfrak{a})$ for norms of principal fractional ideals is clearly

$$\delta_0(\mathfrak{a}) = \frac{\delta(\mathfrak{a})}{(\mathcal{D}^\infty : \mathcal{G})} \sum_{\chi} \chi(\hat{\mathfrak{a}}) \tag{3.1}$$

where $\hat{\mathfrak{a}}$ is any fractional ideal in Ω with $N\hat{\mathfrak{a}} = \mathfrak{a}$, and we have identified \mathcal{D}^∞ with the group of fractional ideals. It follows that

$$f_0(t) = \sum_{\mathfrak{a} \text{ integral}} \delta_0(\mathfrak{a}) t^{\text{deg } \mathfrak{a}} = \frac{1}{(\mathcal{D}^\infty : \mathcal{G})} \sum_{\chi} f(t, \chi), \tag{3.2}$$

where

$$f(t, \chi) = \sum_{\mathfrak{a} \text{ integral}} \delta(\mathfrak{a}) t^{\text{deg } \mathfrak{a}} \chi(\hat{\mathfrak{a}}) \text{ for } |t| < q^{-1}. \tag{3.3}$$

We now proceed to analyse the singularities of the various $f(t, \chi)$. The function $\delta(\mathfrak{a})\chi(\hat{\mathfrak{a}})$ is multiplicative, so that, for $|t| < q^{-1}$,

$$f(t, \chi) = \prod_{\mathfrak{p}} \{1 + \delta(\mathfrak{p})\chi(\hat{\mathfrak{p}}) t^{\text{deg } \mathfrak{p}} + \dots\} \tag{3.4}$$

and so

$$\log f(t, \chi) = \sum_{\mathfrak{p}} \delta(\mathfrak{p})\chi(\hat{\mathfrak{p}}) t^{\text{deg } \mathfrak{p}} + G(t, \chi) \tag{3.5}$$

where $G(t, \chi)$ is regular and $|G(t, \chi)| < C \log \frac{1}{1 - q^{-2\epsilon}}$ for $|t| < q^{-1-\epsilon}$ (c.f. (2.7)).

We assert that $\delta(\mathfrak{p})\chi(\hat{\mathfrak{p}})$ is a class function of $\Gamma = \text{Gal } \bar{\Omega}^\# / K$; that is, if \mathfrak{p} and \mathfrak{q} are unramified prime divisors of K with the same Frobenius conjugacy classes in Γ , then $\delta(\mathfrak{p})\chi(\hat{\mathfrak{p}}) = \delta(\mathfrak{q})\chi(\hat{\mathfrak{q}})$. First, it is obvious that $\delta(\mathfrak{p}) = \delta(\mathfrak{q})$ in these circumstances, since $\text{Gal } \bar{\Omega} / K$ is a quotient of Γ . Now assume that $\delta(\mathfrak{p}) = 1 = \delta(\mathfrak{q})$. It is possible to choose $\hat{\mathfrak{p}}$ to contain only primes lying over \mathfrak{p} (and to do the same for \mathfrak{q}). If the Frobenius classes of $\mathfrak{p}, \mathfrak{q}$ are the same, then with suitable labelling, $\left[\frac{\bar{\Omega}^\# / K}{\mathcal{P}_i} \right] = \left[\frac{\bar{\Omega}^\# / K}{\mathcal{Q}_i} \right]$, where the $\mathcal{P}_i, \mathcal{Q}_i$ are the divisors of $\mathfrak{p}, \mathfrak{q}$ in $\bar{\Omega}^\#$. Thus $\left[\frac{\bar{\Omega}^\# / \Omega}{\mathcal{P}_i} \right] = \left[\frac{\bar{\Omega}^\# / \Omega}{\mathcal{Q}_i} \right]$ for each i , so that the Artin symbols $\left(\frac{\Omega^\# / \Omega}{\Omega_\gamma \mathcal{P}_i} \right)$

and $\left(\frac{\Omega^\#/\Omega}{\Omega_\cap \mathcal{P}_i}\right)$ coincide. Hence so do $\chi(\hat{\mathbf{p}})$ and $\chi(\hat{\mathbf{q}})$, since the decomposition types of \mathbf{p}, \mathbf{q} in Ω are the same (indeed, $\left[\frac{\bar{\Omega}/K}{\bar{\Omega}_\cap \mathcal{P}_i}\right] = \left[\frac{\bar{\Omega}/K}{\bar{\Omega}_\cap \mathcal{Q}_i}\right]$ for each i).

We now see that the behaviour of $\sum \delta(\mathbf{p})\chi(\hat{\mathbf{p}})t^{\text{deg } \mathbf{p}}$ can be examined by means of (A2) of the appendix. For a character χ of $\mathcal{D}^\infty/\mathcal{G}$ we let $\phi(\mathbf{p}) = \delta(\mathbf{p})\chi(\hat{\mathbf{p}})$, and also write $\phi(\sigma) = \phi(\mathbf{p})$ whenever $\sigma \in \left(\frac{\bar{\Omega}\Omega^\#/K}{\mathbf{p}}\right)$. Let $\text{GF}(\mathbf{q}^i)$ be the constant field of $L = \bar{\Omega}\Omega^\#$. Then, by A2, the function $\sum \phi(\mathbf{p})t^{\text{deg } \mathbf{p}}$ has at $t = \mathbf{q}^{-1}\lambda$ ($\lambda^i = 1$) a logarithmic singularity

$$\frac{1}{[L:K]} \sum_{\sigma \in \Gamma} \phi(\sigma)\lambda^{\Delta(\sigma) \text{deg } \mathfrak{A}(\sigma)} \cdot \log \frac{1}{t - \lambda \mathbf{q}^{-1}} \tag{3.6}$$

where $\text{GF}(q^{\Delta(\sigma)})$ is the constant field of L^σ , the fixed field of σ , and $\mathfrak{A}(\sigma)$ is any divisor in L^σ whose Artin symbol $\left(\frac{L/L^\sigma}{\mathfrak{A}(\sigma)}\right) = \sigma$. In order that for some $\lambda^i = 1$ the strength of the singularity of $\sum \phi(\mathbf{p})t^{\text{deg } \mathbf{p}}$ at $t = \lambda \mathbf{q}^{-1}$ be greater than or equal to that of $\sum \phi(\mathbf{p})t^{\text{deg } \mathbf{p}}$ at $t^f = \mathbf{q}^{-f}$ we need

$$\left| \sum_{\sigma \in \Gamma} \phi(\sigma)\lambda^{\Delta(\sigma) \text{deg } \mathfrak{A}(\sigma)} \right| \geq \sum_{\sigma \in \Gamma} \delta(\sigma) \tag{3.7}$$

where we regard δ as a class function on Γ (by lifting from $\text{Gal } \bar{\Omega}/K$). But

$$|\phi(\sigma)\lambda^{\Delta(\sigma) \text{deg } \mathfrak{A}(\sigma)}| = |\delta(\sigma)| = \delta(\sigma)$$

for all $\sigma \in \Gamma$, so the left of (3.7) at most equals the right, and equality implies

$$\phi(\sigma)\lambda^{\Delta(\sigma) \text{deg } \mathfrak{A}(\sigma)} = \delta(\sigma), \quad \forall \sigma \in \Gamma. \tag{3.8}$$

By considering the restriction of (3.8) to the subgroup $\text{Gal } L/\Omega$, we conclude that $\chi(\hat{\mathbf{a}}) = \mu^{\text{deg } \hat{\mathbf{a}}}$ for some $\mu^F = 1$, $\text{GF}(q^{Ff})$ being the constant field of Ω . Conversely any such character χ gives a class function ϕ yielding equality in (3.7) for certain λ . For, if $\delta(\mathbf{p}) = 1$, then $\text{deg } \mathbf{p} = f \text{deg } \hat{\mathbf{p}}$ and thus $\sum \delta(\mathbf{p})\chi(\hat{\mathbf{p}})t^{\text{deg } \mathbf{p}}$ equals $\sum \delta(\mathbf{p})(t\mu^{1/f})^{\text{deg } \mathbf{p}}$, i.e. $f(t\mu^{1/f})$ in the notation of §2.

To summarise, we can now say that the functions $f(t, \chi)$ are of the following types:

(a) if $\chi(\hat{\mathbf{a}}) = \lambda^{\text{deg } \hat{\mathbf{a}}}$, where $\lambda^{fF} = 1$, then

$$f(t, \chi) = f(t\lambda); \tag{3.9}$$

(b) for all other χ corresponding to $\Omega^\#/\Omega$, (3.5) implies that

$$\log f(t, \chi) = G(t, \chi) + \sum_{\lambda^i = 1} s(\lambda) \log \frac{1}{t - \lambda \mathbf{q}^{-1}} \tag{3.10}$$

where $|s(\lambda)| < B$ of §2.

Consequently, returning to (3.2),

$$f_0(t) = \frac{F}{(\mathcal{D}^\infty : \mathcal{G})_{\text{deg } \mathbf{a}}} \sum_{\mathbf{0}(fF)} \delta(\mathbf{a})t^{\text{deg } \mathbf{a}} + H(t) \tag{3.11}$$

where $H(t)$ has at worst singularities of the type $(t - \lambda q^{-1})^{s(\lambda)}$ as in (3.10). The proof of Theorem IIA now adapts readily to the case in hand, working from (3.11). If we wish to handle ideals prime to \mathfrak{n} we can adjust the Euler products for the $f(t, \chi)$ in the appropriate way. Finally, to obtain Theorem IIB, we consider the relation $\mathfrak{a} = N_{\Omega/K}(\alpha)$, where \mathfrak{a} is generated by the monic $a(x)$. The number of constant multiples of $a(x)$ which are norms of elements of Ω^* is equal to the number of elements of k^* (where $k = \text{GF}(q)$) which are Ω/K -norms, and the latter is obviously independent of $a(x)$.

4. Norms in the Farey section. Let $\mathcal{F}(D)$ be as in the introduction; its cardinality satisfies

$$\text{card}^1 \mathcal{F}(D) \sim q^{2D} / (1 + q^{-1}) \quad \text{as } D \rightarrow \infty. \tag{4.1}$$

We are interested in $\mathcal{F}(D) \cap \mathcal{N}$, where \mathcal{N} is the set of all $N_{\Omega/K}(\alpha)$, $\alpha \in \Omega^*$. This is examined (c.f. [1]) by decomposing $\mathcal{F}(D)$ as $\bigcup_{\text{deg } \mathfrak{b} \leq D} \mathcal{F}(\mathfrak{b})$, where $\mathcal{F}(\mathfrak{b})$, for a finite divisor \mathfrak{b} , is

$$\{a(x)/b(x); \text{deg } a(x) \leq \text{deg } \mathfrak{b}, (a(x), b(x)) = 1\},$$

where $b(x)$ is the monic generator of \mathfrak{b} . Then $\text{card } \mathcal{F}(D) = \sum_{\text{deg } \mathfrak{b} \leq D} \text{card } \mathcal{F}(\mathfrak{b})$, and it remains to determine the latter; we deal with each $\text{card } \mathcal{F}(\mathfrak{b})$ separately. Now $\text{card } \mathcal{F}(\mathfrak{b}) = \kappa \text{card } \mathcal{G}(\mathfrak{b})$, where κ is given by (IIB) and $\mathcal{G}(\mathfrak{b})$ is the set of all divisors $\mathfrak{a}\mathfrak{b}^{-1}$ where \mathfrak{a} is finite, integral, prime to \mathfrak{b} , of degree less than $\text{deg } \mathfrak{b}$, and such that $\mathfrak{a}\mathfrak{b}^{-1}$ is the norm of a principal ideal. For fixed \mathfrak{b} with $\delta(\mathfrak{b}) = 1$, this set is in one-one correspondence with the set of integral \mathfrak{a} prime to \mathfrak{b} and of degree less than $\text{deg } \mathfrak{b}$, for which $\delta(\mathfrak{a}) = 1$ and $\chi(\hat{\mathfrak{a}}) = \chi(\hat{\mathfrak{b}})$ for all characters χ of $\Omega^\#/\Omega$, where $\mathfrak{a} = N\hat{\mathfrak{a}}$ and $\mathfrak{b} = N\hat{\mathfrak{b}}$. We deduce that

$$\text{card } \mathcal{G}(\mathfrak{b}) = \frac{1}{(\mathcal{D}^\infty : \mathcal{G})} \sum_{\mathfrak{a}}' \sum_{\chi} \bar{\chi}(\hat{\mathfrak{b}}) \chi(\hat{\mathfrak{a}}) \delta(\mathfrak{a}) \tag{4.2}$$

where $\sum_{\mathfrak{a}}'$ is taken over all integral (finite) divisors \mathfrak{a} prime to \mathfrak{b} and of degree less than $\text{deg } \mathfrak{b}$. An argument analogous to that of §3 shows that

$$\text{card } \mathcal{G}(\mathfrak{b}) = \frac{F}{(\mathcal{D}^\infty : \mathcal{G})} \cdot \sum'' \delta(\mathfrak{a}) \cdot \{1 + O(\omega^4(\mathfrak{b})(\text{deg } \mathfrak{b})^{-c})\} \tag{4.3}$$

where \sum'' is taken over all integral finite \mathfrak{a} prime to \mathfrak{b} , with $\text{deg } \mathfrak{a} < \text{deg } \mathfrak{b}$ and $\text{deg } \mathfrak{a} \equiv \text{deg } \mathfrak{b} \pmod{fF}$, the constant c being positive.

It is also clear that

$$\sum'' \delta(\mathfrak{a}) = \lambda_{\mathfrak{b}}^{-1} \sum \delta(\mathfrak{a}) \cdot \{1 + O(\omega^4(\mathfrak{b}) \cdot (\text{deg } \mathfrak{b})^{-c})\} \tag{4.4}$$

where $\lambda_{\mathfrak{b}}$ is given in (IIA) and the sum $\sum \delta(\mathfrak{a})$ has the restriction $(\mathfrak{a}, \mathfrak{b}) = 1$ lifted. We now obtain

$$\text{card } \mathcal{F}(\mathfrak{b}) \cap \mathcal{N} = \frac{\kappa FC(\Omega)}{(\mathcal{D}^\infty : \mathcal{G})} q^{\text{deg } \mathfrak{b} - 1} \cdot (\text{deg } \mathfrak{b})^{B-1} \cdot \lambda_{\mathfrak{b}}^{-1} \cdot \delta(\mathfrak{b}) \cdot \{1 + O(\omega^4(\mathfrak{n})(\text{deg } \mathfrak{b})^{-c})\}. \tag{4.5}$$

E

An analysis similar to that given in [1, p. 167] now yields

$$D^{2(1-B)} \frac{\text{card } \mathcal{F}(D) \cap \mathcal{N}}{\text{card } \mathcal{F}(D)} \text{ tends to a non-zero limit} \tag{4.6}$$

if $D \rightarrow \infty$ through multiples of f , that is, Theorem IB. In fact, an easy argument shows that if $D \rightarrow \infty$ through a fixed residue class (mod f) then (4.6) still holds, although different limits may occur for different residue classes.

Appendix. Čebotarěv’s density theorem for function fields. We give here some convenient formulations of Čebotarěv’s density theorem. We begin with a reduction to the cyclic case:

PROPOSITION A.1. *Let L/K be a finite Galois extension of function fields in one variable, K having constant field $\text{GF}(q)$ and L having $\text{GF}(q^h)$. If σ belongs to $\text{Gal } L/K$ we let $\langle \sigma \rangle$ be the conjugacy class which it spans, and we suppose that the fixed field L^σ of σ has constant field $\text{GF}(q^{e(\sigma)})$. Then the degree $\text{deg } \mathfrak{A}(\sigma)$ of any divisor in L^σ with Artin symbol $\left(\frac{L/L^\sigma}{\mathfrak{A}(\sigma)}\right) = \sigma$ determines a unique residue class prime to $h/e(\sigma)$ and, for small t ,*

$$\sum_{\substack{\mathfrak{p} \text{ in } K \\ \text{Frob } \mathfrak{p} = \langle \sigma \rangle}} t^{\text{deg } \mathfrak{p}} = \frac{\text{ord}_G \sigma}{\text{card } N_G(\sigma)} \left\{ \sum_{\substack{\mathfrak{p} \text{ in } L^\sigma \\ (L/\mathfrak{p}) = \sigma}} t^{e(\sigma) \text{deg } \mathfrak{p}} + E(t) \right\} \tag{A1}$$

where $N_G(\sigma)$ is the normaliser of σ in G and $|E(t)| \leq \log |Z_K(|t|^2)|$, Z_K being the zeta function of K .

Proof. That $\text{deg } \mathfrak{A}(\sigma)$ determines a unique residue class prime to $h/e(\sigma)$ follows by applying Artin’s reciprocity theorem to L/L^σ . The remainder of the proof of (A1) is a direct imitation of the elegant proof of the analogous result for algebraic number fields given by Deuring [4].

To obtain more explicit analytic information we now need to deal with the right-hand side of (A1). This yields

PROPOSITION A.2. *Let ϕ be a class function of $G = \text{Gal } L/K$; for primes \mathfrak{p} in K unramified in L we write $\phi(\mathfrak{p})$ for $\phi(\text{Frob } \mathfrak{p})$. Then, in the notation of Proposition A1, we have*

$$\sum_{\mathfrak{p}} \phi(\mathfrak{p}) t^{\text{deg } \mathfrak{p}} = \sum_{\lambda^h = 1} \left\{ \frac{1}{\text{card } G} \sum_{\sigma \in G} \lambda^{e(\sigma) \text{deg } \mathfrak{A}(\sigma)} \phi(\sigma) \right\} \log \frac{1}{t - \lambda q^{-1}} + O\left(\sum_{n=1}^{\infty} \frac{|t|^h q^{\frac{1}{2}nh}}{n} \right) \tag{A2}$$

where the constant in the O -term depends only on the genus and degree of L/K .

Proof. $\sum \phi(\mathfrak{p}) t^{\text{deg } \mathfrak{p}} = \sum'_{\langle \sigma \rangle} \phi(\sigma) \sum_{\text{Frob } \mathfrak{p} = \langle \sigma \rangle} t^{\text{deg } \mathfrak{p}}$ where \sum' is taken over a full set of representatives of the conjugacy classes of G . Using (A1) we deduce that

$$\sum \phi(\mathfrak{p}) t^{\text{deg } \mathfrak{p}} = \sum'_{\langle \sigma \rangle} \phi(\sigma) \frac{\text{ord } \sigma}{\text{card } N_G(\sigma)} \sum_{\mathfrak{p} : (L/\mathfrak{p}) = \sigma} t^{e(\sigma) \text{deg } \mathfrak{p}} + R,$$

where $|R| \leq \sum_{\sigma \in G} |\phi(\sigma) \log |Z_K(|t|^2)|$. Now

$$\sum_{\Psi: (L/\mathbb{F}) = \sigma} (t^{e(\sigma)})^{\deg \Psi} = \frac{1}{\text{ord } \sigma} \sum_{\chi} \bar{\chi}(\mathfrak{I}(\sigma)) \log L(t^{e(\sigma)}, \chi) + O(\log Z_{L^\sigma}(|t|^{2e(\sigma)})),$$

where χ runs through all characters of the cyclic extension L/L^σ . The only χ giving significant singularities are those of the type $\chi(\mathfrak{I}) = \mu^{\deg \mathfrak{I}}$ where $\mu^{h/e(\sigma)} = 1$ (see [3, pp. 64–67]), for which $L(t^{e(\sigma)}, \chi)$ is $Z_{L^\sigma}(\mu t^{e(\sigma)})$. We deduce that

$$\sum \phi(\mathfrak{p}) t^{\deg \mathfrak{p}} = \frac{1}{\text{card } G} \sum_{\sigma \in G} \phi(\sigma) \sum_{\mu^{h/e(\sigma)} = 1} \mu^{-\deg \mathfrak{I}(\sigma)} \log \frac{1}{q^{e(\sigma)} t^{e(\sigma)} - \mu^{-1}}$$

plus terms which amount to $O(\log |Z_K(|t|^2)|) + O(\log |Z_{L^\sigma}(|t|^{2e(\sigma)})|)$, in view of the Riemann hypothesis for L - and Z -functions, the constants in $O(\dots)$ depending at most on the genus and degree of L/K . After some elementary rearrangement we arrive at (A2).

From (A2) we can read (if so desired) the analytical properties of Artin L -series over K ; however, a direct application of (A2) often avoids the need to introduce these L -functions in applications. A handy “local version” suitable for applications in which $\text{Gal } L/K$ is regarded directly as a transitive permutation group on the conjugates of a primitive element of L/K is the following:

PROPOSITION A.3. *Let λ be a cycle pattern; we write G_λ for the subset of $G = \text{Gal } L/K$ consisting of those σ for which L^σ has constant field $\text{GF}(q^\lambda)$, and G_λ^λ for the subset of G_λ having cycle pattern λ . Then*

$$\sum_{\substack{\deg \mathfrak{p} = n \\ \text{Frob } \mathfrak{p} \text{ has c.p. } \lambda}} 1 = \frac{q^n \text{card } G_{(n, h)}^\lambda}{n \text{card } G_{(n, h)}} + O(q^{n/2}) \tag{A3}$$

where the constants in $O(\dots)$ depend at most on the degree and genus of L/K .

(A3) may be obtained either from (A2) or by generalising the arguments of Cohen [5] and Fried [6].

REFERENCES

1. R. W. K. Odoni, The Farey density of norm subgroups of global fields—I, *Mathematika* **20** (1973), 155–169.
2. F. K. Schmidt, Die Theorie der Klassenkörper . . . , *Sitzungsberichte der phys. med. Soc. zu Erlangen* **62** (1930), 267–284.
3. M. Deuring, Lectures on the theory of algebraic functions of one variable, Lecture Notes in Mathematics No. 314 (Springer-Verlag, 1973).
4. M. Deuring, Über den Tschebotareffschen Dichtigkeitssatz, *Math. Ann.* **110** (1935), 414–415.
5. S. D. Cohen, The distribution of polynomials over finite fields, *Acta Arithmetica* **17** (1970), 255–271.
6. M. Fried, On Hilbert’s Irreducibility Theorem, *J. Number Theory* **6** (1974), 211–231.

DEPARTMENT OF MATHEMATICS
 UNIVERSITY OF GLASGOW
 and
 DEPARTMENT OF MATHEMATICS
 UNIVERSITY OF EXETER

PRINTERS TO THE UNIVERSITY OF GLASGOW
 PRINTED IN GREAT BRITAIN BY ROBERT MACLEHOSE AND CO. LTD