Chapter 2
Artin L-Functions

§1 Group-theoretic background

In this section, we shall collect together a few group theoretic preliminaries. We begin by reviewing the basic aspects of characters and class functions.

Let G be a finite group. If $f_1, f_2 : G \to \mathbb{C}$ are two $\mathbb{C}$-valued functions on G, we define their inner product by

$$(f_1, f_2) = \frac{1}{|G|} \sum_{g \in G} f_1(g) \overline{f_2(g)}.$$

If $f : G \to \mathbb{C}$ is a $\mathbb{C}$-valued function on G, and $\sigma \in G$, we define $f^\sigma : G \to \mathbb{C}$ by $f^\sigma(g) = f(\sigma g \sigma^{-1})$. We say f is a *class function* if $f^\sigma = f$ for all $\sigma \in G$.

Let $H \subseteq G$ be a subgroup and $f : H \to \mathbb{C}$ a class function on H. We define a class function

$$\operatorname{Ind}_H^G f : G \to \mathbb{C}$$

on G as follows. Let $g_1, \ldots, g_r$ ($r = [G : H]$) be coset representatives for H in G (so that $G = \cup g_i H$). Extend f to a function $\dot{f}$ on G by setting

$$\dot{f}(g) = \begin{cases} f(g) & g \in H \\ 0 & g \notin H \end{cases}$$

Then

$$(\operatorname{Ind}_H^G f)(g) = \sum_{i=1}^{r} \dot{f}(g_i^{-1} g g_i) = \frac{1}{|H|} \sum_{s \in G} \dot{f}(s^{-1} g s).$$

Let f_1 be a class function on the subgroup H and f_2 a class function on G. The *Frobenius reciprocity theorem* tells us that

$$(f_1, f_2 \mid_H) = (\operatorname{Ind}_H^G f_1, f_2).$$

M.R. Murty and V.K. Murty, *Non-vanishing of L-Functions and Applications*,
Modern Birkhäuser Classics, DOI 10.1007/978-3-0348-0274-1_3, © Springer Basel AG 1997

Let H_1, H_2 be subgroups of G and let f be a class function on H_2. Suppose that $G = H_1 H_2$. Then one of *Mackey's theorems* tells us that

$$\begin{tikzcd}[column sep=small] & G \arrow[dl, dash] \arrow[dr, dash] & \\ H_1 \arrow[dr, dash] & & H_2 \arrow[dl, dash] \\ & H_1 \bigcap H_2 & \end{tikzcd}$$

$$(\mathrm{Ind}_{H_2}^G f)|_{H_1} = \mathrm{Ind}_{H_1 \cap H_2}^{H_1} (f|_{H_1 \cap H_2}).$$

Let $\rho : G \to GL_n(\mathbb{C})$ be an irreducible representation of G and set $\chi = Tr\,\rho$, the character of ρ. Then χ is a class function on G and every class function is a $\mathbb{C}$-linear combination of characters χ of irreducible representations. A class function which is a $\mathbb{Z}$-linear combination of characters will be called a *generalized character.*

For each $g \in G$, define a symbol x_g and consider the $\mathbb{C}$-vector space

$$V = \oplus_{g \epsilon G} \mathbb{C} x_g .$$

If $|G| = n$, then $\dim V = n$. The *regular representation* reg_G of G

$$\mathrm{reg}_G : G \to GL(V)$$

is defined by

$$\sigma \mapsto (x_g \mapsto x_{\sigma g}) \, .$$

Its character will be denoted by the same letter and we easily see that

$$\mathrm{reg}_G(\sigma) = \begin{cases} n & \sigma = e \text{ (identity)} \\ 0 & \sigma \neq e. \end{cases}$$

In terms of characters

$$\mathrm{reg}_G = \sum_{\chi} \chi(1) \chi$$

where the sum is over all irreducible characters of G. In terms of induction,

$$\mathrm{reg}_G = \mathrm{Ind}_{\{e\}}^G 1$$

where 1 denotes the (trivial) character of the identity subgroup $\{e\}$.

The reader is referred to Serre [Se1] for an excellent introduction to the representation theory of finite groups.

§2 Definition and basic properties of Artin L-functions

Now let L/K be a Galois extension of number fields, with group G. For each prime $\mathfrak{p}$ of K, and a prime $\mathfrak{q}$ of L with $\mathfrak{q}|\mathfrak{p}$, we define the *decomposition group* $D_{\mathfrak{q}}$ to be $\mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ where $L_{\mathfrak{q}}$ (resp. $K_{\mathfrak{p}}$) is the completion of L (resp. K) at $\mathfrak{q}$ (resp. $\mathfrak{p}$). We have a map from $D_{\mathfrak{q}}$ to $\mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$ (the Galois group of the residue field extension) which by Hensel's lemma is surjective. The kernel $I_{\mathfrak{q}}$ is the *inertia group*. We thus have an exact sequence

$$1 \to I_{\mathfrak{q}} \to D_{\mathfrak{q}} \to \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}}) \to 1.$$

The group $\mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$ is cyclic with a generator $x \mapsto x^{\mathbf{N}\mathfrak{p}}$ where $\mathbf{N}\mathfrak{p}$ is the cardinality of $k_{\mathfrak{p}}$. We can *choose* an element $\sigma_{\mathfrak{q}} \in D_{\mathfrak{q}}$ whose image in $\mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$ is this generator. We call $\sigma_{\mathfrak{q}}$ a *Frobenius element* at $\mathfrak{q}$ and it is only defined $\bmod\, I_{\mathfrak{q}}$. We have $I_{\mathfrak{q}} = 1$ for all unramified $\mathfrak{p}$ (and in particular, these are all but finitely many $\mathfrak{p}$) and so for these $\mathfrak{p}$, $\sigma_{\mathfrak{q}}$ is well-defined. If we choose another prime $\mathfrak{q}'$ above $\mathfrak{p}$,then $I_{\mathfrak{q}'}$ and $D_{\mathfrak{q}'}$ are conjugates of $I_{\mathfrak{q}}$ and $D_{\mathfrak{q}}$. For $\mathfrak{p}$ unramified, we denote by $\sigma_{\mathfrak{p}}$ the *conjugacy class* of Frobenius elements at primes $\mathfrak{q}$ above $\mathfrak{p}$.

Let ρ be a representation of G :

$$\rho : G \to \mathrm{GL}_n(\mathbb{C}).$$

Let χ denote its character. For $\mathrm{Re}(s) > 1$, we define the partial L-function by

$$L_{\text{unramified}}(s, \chi, K) = \prod_{\mathfrak{p} \text{ unramified}} \det(I - \rho(\sigma_{\mathfrak{p}})(\mathbf{N}\mathfrak{p})^{-s})^{-1}$$

where the product is over primes $\mathfrak{p}$ of K with $I_{\mathfrak{q}} = 1$ for any $\mathfrak{q}$ of L with $\mathfrak{q}|\mathfrak{p}$. To obtain an L-function which has good analytic properties (such as functional equation), it is necessary to also define Euler factors at the primes $\mathfrak{p}$ which are ramified in L and also at infinite primes of K.

Let $\mathfrak{p}$ be a prime of K which is ramified in L, and $\mathfrak{q}$ a prime of L above $\mathfrak{p}$. Let V be the underlying complex vector space on which ρ acts. Then we may restrict this action to the decomposition group $D_{\mathfrak{q}}$ and we see that the quotient $D_{\mathfrak{q}}/I_{\mathfrak{q}}$ acts on the subspace $V^{I_{\mathfrak{q}}}$ of V on which $I_{\mathfrak{q}}$ acts trivially. Now we see that any $\sigma_{\mathfrak{q}}$ will have the same characteristic polynomial on this subspace and we define the Euler factor at $\mathfrak{p}$ to be this polynomial:

$$L_{\mathfrak{p}}(s, \chi, K) = \det(I - \rho(\sigma_{\mathfrak{q}})|V^{I_{\mathfrak{q}}}(\mathbf{N}\mathfrak{p})^{-s})^{-1}.$$

This is well-defined and gives the Euler factors at all finite primes.

Remark. Since G is a finite group, once ρ is given, there are only a finite number of characteristic polynomials that can occur. For example, if we take the trivial one-dimensional representation, only the polynomial $(1 - T)$ occurs. But the subtlety in the Artin L-function is the assignment $\mathfrak{p} \mapsto \sigma_{\mathfrak{p}}$. In other words, which one of the finite number of characteristic polynomials is assigned to a given prime $\mathfrak{p}$ determines and is determined by the arithmetic of the field extension, in particular the splitting of primes.

We have also to define the Archimedean Euler factors. For each Archimedean prime v of K we set

$$L_v(s,\chi,K)=\begin{cases}((2\pi)^{-s}\Gamma(s))^{\chi(1)} & \text{if } v \text{ is complex}\\ ((\pi^{-s/2}\Gamma(s/2))^a(\pi^{-(s+1)/2}\Gamma((s+1)/2))^b & \text{if } v \text{ is real.}\end{cases}$$

Here

$$a+b=\chi(1)$$

and a (resp. b) is the dimension of the $+1$ eigenspace (resp. -1 eigenspace) of complex conjugation.

We shall write

$$\gamma(s,\chi,K)=\prod_{v \text{ infinite}} L_v(s,\chi,K).$$

The Artin L-function $L(s,\chi,K)$ satisfies a functional equation of the following type. First, one defines the Artin conductor $\mathfrak{f}_\chi$ associated to χ. It is an ideal of K and is defined in terms of the restriction of χ to the inertia groups and its various subgroups.

More precisely, let ν be a place of K. Let w be a place of L dividing ν and let G_0 denote the inertia group I_w at w. We have a descending filtration of higher ramification groups (see [CF], p. 33]).

$$G_0 \supseteq G_1 \supseteq \cdots.$$

Let V be the underlying representation space for ρ. Define

$$n(\chi,\nu)=\sum_{i=0}^{\infty}\frac{|G_i|}{|G_0|}\operatorname{codim}(V^{G_i}).$$

Then $n(\chi,\nu)$ is an integer and is well-defined (that is, it is independent of the choice of w above ν). Moreover, it is equal to zero apart from a finite number of ν. This allows us to define the ideal

$$\mathfrak{f}_\chi=\prod_\nu \mathfrak{p}_\nu^{n(\chi,\nu)}.$$

We also set

$$A_\chi=d_K^{\chi(1)}\mathbf{N}_{K/\mathbb{Q}}\mathfrak{f}_\chi.$$

Let us set

$$\Lambda(s,\chi,K)=A_\chi^{s/2}\gamma(s,\chi,K)L(s,\chi,K).$$

Then we have the functional equation

$$\Lambda(s,\chi,K)=W(\chi)\Lambda(1-s,\bar{\chi},K)$$

where $W(\chi)$ is a complex number of absolute value 1.

The number $W(\chi)$ itself carries deep arithmetic information. For example, it is related to Galois module structure. The reader is referred to the monograph [Fr] of Fröhlich for an introduction to this subject.

We now recall some of the formalism of Artin L-functions and their basic properties. It is summarized in the two properties:

$$L(s, \sum_\chi a_\chi \chi, K) = \prod_\chi L(s,\chi,K)^{a_\chi} \qquad \text{for any} \qquad a_\chi \in \mathbb{Z} \tag{1}$$

$$L(s,\ \mathrm{Ind}_H^G \chi, K) = L(s,\chi,L^H) \text{ where } L^H \text{ is the subfield of } L \text{ fixed by } H. \tag{2}$$

Using (1) and (2), we find that

$$\begin{aligned}\prod_{\chi \text{ irred}} L(s,\chi,K)^{\chi(1)} &= L(s, \mathrm{reg}_G, K) = L(s,1,L) = \zeta_L(s)\\ &= \prod_{\mathfrak{q}} (1-(\mathbf{N}\mathfrak{q})^{-s})^{-1}.\end{aligned}$$

There is a theorem of Brauer which says that for any irreducible χ, there are subgroups $\{H_i\}$, one-dimensional characters ψ_i of H_i and integers $m_i \epsilon\ \mathbb{Z}$ with

$$\chi = \sum_i m_i \,\mathrm{Ind}_{H_i}^G \psi_i.$$

Using (1) and (2), we see that

$$L(s,\chi,K) = \prod_i L(s,\psi_i,L^{H_i})^{m_i}.$$

If χ is one-dimensional, then Artin's reciprocity theorem identifies $L(s,\chi,K)$ with a Hecke L-series for a ray class character. By Hecke and Tate, we know the analytic continuation of these L-series (see Chapters 13 and 14 of [La]).

From the Brauer induction theorem, it follows that any Artin L-function has a meromorphic continuation. **Artin's conjecture** asserts that every Artin L function $L(s,\chi,K)$ associated to a character χ of $\mathrm{Gal}(\bar{K}/K)$ has an analytic continuation for all s except possibly for a pole at $s=1$ of order equal to the multiplicity of the trivial representation in ρ. (Note that χ determines ρ up to isomorphism and so our notation is justified).

This is a very central and important conjecture in number theory. It is part of a general reciprocity law. The conjecture of Artin is known to hold in many cases. Most of these arise from a combination of the one-dimensional case and group theory. Some examples are given in the exercises.

Returning to the general case, we see from the factorization

$$\zeta_L(s) = \prod_{\chi \text{ irred}} L(s,\chi,K)^{\chi(1)}$$

that Artin's conjecture implies that $\zeta_L(s)/\zeta_K(s)$ is entire. In fact, let L/K be a (not necessarily Galois) finite extension and let $\tilde{K}/K$ be its normal closure. Say $G = \mathrm{Gal}(\tilde{K}/K)$ and $H = \mathrm{Gal}(\tilde{K}/L)$. Then

$$L(s, \mathrm{Ind}_H^G(1_H), K) = L(s, 1_H, L) = \zeta_L(s).$$

On the other hand,

$$\mathrm{Ind}_H^G 1_H = 1_G + \sum_{1 \neq \chi \ \text{irred}} a_\chi \chi$$

with $0 \leq a_\chi \in \mathbb{Z}$. So,

$$L(s, \mathrm{Ind}_H^G 1_H, K) = \zeta_K(s) \prod L(s, \chi, K)^{a_\chi}.$$

Putting these together, we see that Artin's conjecture implies that $\zeta_L(s)/\zeta_K(s)$ is entire, whether L/K is Galois or not. This special case of Artin's conjecture is called Dedekind's conjecture. Below, we shall discuss it in several cases. In particular, it is known to hold in the case L/K is Galois (Aramata-Brauer) and in case $\tilde{L}/K$ is solvable (Uchida-van der Waall).

§3 The Aramata-Brauer Theorem

Let L/K be Galois with group G.

Theorem 3.1 *The quotient $\zeta_L(s)/\zeta_K(s)$ is entire.*

By the properties of Artin L-functions described in §2, the Theorem follows from the following result.

Proposition 3.2 *There are subgroups $\{H_i\}$, 1-dimensional character ψ_i of H_i and $0 \leq m_i \in \mathbb{Z}$ so that*

$$\mathrm{reg}_G - 1_G = \sum m_i \, \mathrm{Ind}_{H_i}^G \psi_i.$$

(Note that $(\mathrm{reg}_G, 1_G) = (\mathrm{Ind}_{\{e\}}^G 1, 1_G) = (1, 1_G|_{\{e\}}) = 1$ *by Frobenius reciprocity).*

For any cyclic subgroup A define $\theta_A : A \to \mathbb{C}$ by

$$\theta_A(\sigma) = \begin{cases} |A| & \text{if } \sigma \text{ generates } A \\ 0 & \text{else} \end{cases}$$

and

$$\lambda_A = \phi(|A|) \, \mathrm{reg}_A - \theta_A,$$

where ϕ denotes Euler's function.

Thus,

$$\lambda_A(\sigma) = \begin{cases} \phi(|A|)|A| & \text{if } \sigma = 1 \\ -\theta_A(\sigma) & \text{if } \sigma \neq 1 \end{cases}$$

Proposition 3.2 will be proved in two steps.

Step 1. $\lambda_A = \sum m_\chi \chi$ with $m_\chi \geq 0$, $m_\chi \in \mathbb{Z}$ and χ ranges over the characters of A.

Step 2. $\mathrm{reg}_G - 1_G = \frac{1}{|G|} \sum_A \mathrm{Ind}_A^G \lambda_A$ where the sum is over all cyclic subgroups A of G.

To prove Step 1, it is enough to show that $(\lambda_A, \chi) \geq 0$ for any irreducible χ of A. But

$$\begin{aligned}(\lambda_A, \chi) &= \phi(|A|) - (\theta_A, \chi) \\ &= \phi(|A|) - \sum_{\substack{\sigma \in A \\ <\sigma>=A}} \chi(\sigma) = \sum_{\substack{\sigma \in A \\ <\sigma>=A}} (1 - \chi(\sigma)) \\ &= Tr(1 - \chi(\sigma)) \in \mathbb{Z} \text{ (for any generator } \sigma \text{ of } A)\end{aligned}$$

Now for $\chi \neq 1, \mathrm{Re}(1 - \chi(\sigma)) > 0$ if $\sigma \neq e$ and $= 0$ if $\sigma = e$. Then, if $A \neq \{1\}$, (λ_A, χ) is positive for all $\chi \neq 1$ and $= 0$ if $\chi = 1$. If $A = \{1\}$ then $\lambda_A = 0$. This proves Step 1.

To prove the equality of Step 2, it is enough to show that for any irreducible character ψ of G, both sides have the same inner product with ψ. Now

$$\begin{aligned}(|G|(\mathrm{reg}_G - 1_G), \psi) &= \sum (\mathrm{reg}_G - 1_G)(g)\overline{\psi(g)} \\ &= |G|\psi(1) - \sum_{g \epsilon G} \psi(g)\end{aligned}$$

Also, by Frobenius reciprocity,

$$\begin{aligned}\sum_A (\mathrm{Ind}_A^G \lambda_A, \psi) &= \sum_A (\lambda_A, \psi|_A) \\ &= \sum_A \{\phi(|A|)\psi(1) - \sum_{\substack{\sigma \in A \\ <\sigma>=A}} \psi(\sigma)\} \\ &= \psi(1) \sum_A \phi(|A|) - \sum_{\sigma \epsilon G} \psi(\sigma).\end{aligned}$$

Now

$$\sum_A \phi(|A|) = \sum_A \sum_{\substack{\sigma \in A \\ <\sigma>=A}} 1 = \sum_{\sigma \epsilon G} 1 = |G|.$$

This completes Step 2 and the proof of Proposition 3.2.

We illustrate the equality of Step 2 above with an example. Let $L/\mathbb{Q}$ be a biquadratic extension (Galois). Then the identity is

$$\begin{tikzcd}[column sep=small] & L \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ K_1 \arrow[dr, dash] & K_2 \arrow[d, dash] & K_3 \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

$$\left(\frac{\zeta_L(s)}{\zeta(s)}\right)^4 = \left(\frac{\zeta_L(s)}{\zeta_{K_1}(s)}\right)^2 \left(\frac{\zeta_L(s)}{\zeta_{K}2(s)}\right)^2 \left(\frac{\zeta_L(s)}{\zeta_{K_3}(s)}\right)^2$$

which when unwound, gives the usual factorization

$$\zeta_L(s) = \zeta(s)L(s,\chi_1)L(s,\chi_2)L(s,\chi_3).$$

§4 Dedekind's conjecture in the non-Galois case

As explained in §2, Artin's holomorphy conjecture implies that the quotient $\zeta_K(s)/\zeta_F(s)$ is entire even when K/F is *not* normal. This latter assertion, called Dedekind's conjecture, is still an open problem in general.

Dedekind's conjecture has been settled in a few cases, notably for extensions K/F whose normal closure has solvable Galois group. This is due to Uchida [Uc] and van der Waall [vdW]. In fact, their method allows us to prove the following.

Theorem 4.1 *Let K/F be a finite extension of number fields and suppose that the normal closure $\tilde{K}/F$ has Galois group G which is the semidirect product of $H = \mathrm{Gal}(\tilde{K}/K)$ by an abelian normal subgroup A of G. Then Dedekind's conjecture is true for K/F. That is,*

$$\zeta_K(s)/\zeta_F(s)$$

is entire.

Proof. Let us write

$$\mathrm{Ind}_H^G(1_H) = \sum m_\chi \chi$$

where $0 \le m_\chi \in \mathbb{Z}$, $m_1 = 1$ and χ ranges over the irreducible characters of G. Consider

$$\mathrm{Ind}_H^G(1_H)|_A = \sum m_\chi \chi|_A.$$

By Mackey's theorem,

$$\mathrm{Ind}_H^G(1_H)|_A = \mathrm{Ind}_{H\cap A}^A(1_H|_{H\cap A}) = \mathrm{Ind}_{\{1\}}^A 1 = \mathrm{reg}_A\,.$$

Thus,

$$\operatorname{Ind}_H^G(1_H)|_A = \sum \epsilon$$

where ϵ ranges over all the irreducible characters of A. Thus, for all χ,

$$m_\chi = 0 \text{ or } 1 \text{ and } (\chi|_A, \epsilon) = 0 \text{ or } 1 \text{ for any } \epsilon \in Irr(A).$$

Now, take an $\epsilon \in Irr(A)$ such that there is a $\chi \in Irr(G)$ with $m_\chi \neq 0$ and $(\chi|_A, \epsilon) = 1$. Let T_ϵ be the inertia group of ϵ :

$$T_\epsilon = \{\sigma \in G : \epsilon^\sigma = \epsilon\}.$$

(Here, ϵ^σ is the character $a \mapsto \epsilon(\sigma a \sigma^{-1})$.) Of course, $T_\epsilon \supseteq A$ and we can write it as $T_\epsilon = H_\epsilon A$ where $H_\epsilon \subseteq H$. We can extend ϵ to a character $\tilde{\epsilon}$ of T_ϵ by setting

$$\tilde{\epsilon}(ha) = \epsilon(a) \text{ for any } h \in H_\epsilon, a \in A.$$

Let us write

$$\operatorname{Ind}_A^{T_\epsilon} \epsilon = \operatorname{Ind}_A^{T_\epsilon} \tilde{\epsilon}|_A = \sum_{\psi \in Irr(T_\epsilon)} m_\psi \psi.$$

Notice that

$$\operatorname{Ind}_A^{T_\epsilon} \epsilon(g) = \begin{cases} [T_\epsilon : A]\epsilon(g) & \text{if } g \in A \\ 0 & \text{otherwise} \end{cases}.$$

Thus,

$$[T_\epsilon : A]\epsilon = (\operatorname{Ind}_A^{T_\epsilon} \epsilon)|_A = \sum m_\psi \psi|_A.$$

Thus for every $\psi \in Irr(T_\epsilon)$, with $m_\psi \neq 0$, $\psi|_A$ is a multiple of ϵ. In fact,

$$m_\psi = (\psi, \operatorname{Ind}_A^{T_\epsilon} \epsilon) = (\psi|_A, \epsilon),$$

and so $\psi|_A = m_\psi \epsilon$. It follows that

$$\sum m_\psi^2 = [T_\epsilon : A].$$

From this, we deduce that the characters $\{\operatorname{Ind}_{T_\epsilon}^G \psi\}$ are distinct and irreducible. Indeed, we have

$$[T_\epsilon : A] = \sum m_\psi^2 \leq (\operatorname{Ind}_A^G \epsilon, \operatorname{Ind}_A^G \epsilon) = (\epsilon, (\operatorname{Ind}_A^G \epsilon)|_A)$$

and

$$\operatorname{Ind}_A^G \epsilon|_A = [T_\epsilon : A] \sum \epsilon^g$$

where the sum on the right is over a set of coset representatives for T_ϵ in G. By definition of T_ϵ, the conjugates ϵ^g are distinct and our claim follows. Now,

$$1 = (\chi|_A, \epsilon) = (\chi, \operatorname{Ind}_A^G \epsilon) = \sum_{\psi \in Irr(T_\epsilon)} m_\psi (\chi, \operatorname{Ind}_{T_\epsilon}^G \psi).$$

Thus, there is a unique $\phi = \phi(\chi) \in Irr(T_\epsilon)$ with $m_\phi = 1$ and $(\chi, \operatorname{Ind}_{T_\epsilon}^G \phi) = 1$. By the irreducibility of both characters, it follows that $\chi = \operatorname{Ind}_{T_\epsilon}^G \phi$. Also, as $\psi|_A = m_\psi \epsilon$, we have $\phi(1) = m_\phi = 1$. Hence, χ is the induction of a linear character. This proves that $\operatorname{Ind}_H^G 1_H$ is a sum of monomial characters and the proposition follows.

Corollary 4.2 (Uchida, van der Waall) *Let K/F be an extension of number fields and $\tilde{K}$ a normal closure of K/F. Suppose that* $\mathrm{Gal}(\tilde{K}/F)$ *is solvable. Then $\zeta_K(s)/\zeta_F(s)$ is entire.*

Proof. As above, we set $G = \mathrm{Gal}(\tilde{K}/F)$ and $H = \mathrm{Gal}(\tilde{K}/K)$, We proceed by induction on the order of $|G|$. We may assume that H is a maximal subgroup of G. For if J is a maximal subgroup of G with $H \subset J \subset G$, and M is the fixed field of J, then

$$\zeta_K(s)/\zeta_F(s) = (\zeta_K(s)/\zeta_M(s))\,(\zeta_M(s)/\zeta_F(s))$$

where the first factor on the right is entire by the induction hypothesis and the second by the maximality of J.

Also, since G corresponds to the normal closure of K/F, we may assume that H does not contain any proper non-trivial normal subgroup of G. Now let A be a minimal normal subgroup of G. As G is solvable, such an A exists and is (elementary) abelian. Moreover, A is not contained in H. Then $HA = G$ and $H \cap A = \{1\}$. Indeed, the first equality is just the maximality of H and the second follows from the minimality of A and the observation that $H \cap A$ is again a normal subgroup. Thus, G is the semidirect product of A by H and Theorem 4.1 applies.

Finally in this section, we can ask the following variant of Dedekind's conjecture. Let L/K be an extension with group G, and let H be a subgroup. Let ρ be an irreducible representation of G. Then, is the quotient

$$L(s, \mathrm{Ind}_H^G(\rho|_H), K)/L(s, \rho, K) \tag{‡}$$

entire? This includes the general case of Dedekind's conjecture (if we take $\rho = 1_G$). (‡) can be proved by the method of the Proposition above, if G is solvable and ρ is an abelian character. Indeed, we need only make two observations. First, if we write

$$\mathrm{Ind}_H^G(\rho|_H) - \rho = \sum m_\chi \chi$$

then restricting to A shows that

$$\sum m_\chi \chi|_A = \rho(1) \sum \epsilon.$$

Moreover, if G is any group and A is an abelian normal subgroup, and ϵ is an (irreducible) character of A, then

$$\mathrm{Ind}_A^G \epsilon = \sum m_i \,\mathrm{Ind}_{T_\epsilon}^G \psi_i$$

where $\psi_i(1) = m_i$ and T_ϵ is the inertia subgroup of ϵ. Thus, if $\rho(1) = 1$, and $(\chi|_A, \epsilon) \neq 0$, then

$$1 = (\chi|_A, \epsilon) = (\chi, \mathrm{Ind}_A^G \epsilon) = \sum m_i (\chi, \mathrm{Ind}_{T_\epsilon}^G \psi_i)$$

and as before, this implies that there is an i with $m_i = 1$ and $\chi = \mathrm{Ind}_{T_\epsilon}^G \psi_i$. Even without assuming $\rho(1) = 1$, we get $\chi = \mathrm{Ind}_{T_\epsilon}^G \psi_i$ for some ϵ and i. But we may not know the holomorphy of $L(s, \psi_i)$. (Notice also, that we can restrict to the case H is a maximal subgroup. For if $J \supseteq H$ is a maximal subgroup, (M = fixed field of J)

$$L(s, \mathrm{Ind}_H^G(\rho|_H), K)/L(s, \mathrm{Ind}_J^G(\rho|_J), K) = L(s, \mathrm{Ind}_H^J(\rho|_H), M)/L(s, \rho|_J, M).$$

and so

$$\frac{L(s, \mathrm{Ind}_H^G(\rho|_H), K)}{L(s, \rho, K)} = \frac{L(s, \mathrm{Ind}_H^J(\rho|_H), M)}{L(s, \rho|_J, M)} \cdot \frac{L(s, \mathrm{Ind}_J^G(\rho|_J), K)}{L(s, \rho, K)}.$$

§5 Zeros and poles of Artin L-functions

There is another approach to the Aramata-Brauer theorem which does not explicitly use the decomposition of $\mathrm{reg}_G - \chi$ into monomial characters. To describe it, let us set

$$n_\chi = n_\chi(s_0) = ord_{s=s_0} L(s, \chi, F).$$

Then, in [St], the inequality

$$\sum_{\chi \in Irr(G)} n_\chi^2 \le r^2, \quad r = ord_{s=s_0} \zeta_K(s)$$

is proved. From this, it follows for example that $\zeta_K(s)/L(s, \chi, F)$ is entire except possibly at $s = 1$, and that the same holds for the product $\zeta_K(s)L(s, \chi, F)$. This raises the question of whether $\mathrm{reg}_G - \chi$ can be decomposed as a non-negative sum of monomial characters. This was answered in the affirmative by Rhoades [R]. Some special cases were computed in [Mu1].

Our approach applies in a wider context of an L-function formalism which is satisfied by a variety of objects in number theory and algebraic geometry. Let G be a finite group. For every subgroup H of G and complex character ψ of H, we attach a complex number $n(H, \psi)$ satisfying the following properties:

(1) Additivity: $n(H, \psi + \psi') = n(H, \psi) + n(H, \psi')$,
(2) Invariance under induction: $n(G, \mathrm{Ind}_H^G \psi) = n(H, \psi)$.

The formalism can be applied to the above case when G is the Galois group of a normal extension K/k and $n(H, \psi)$ is the order of the zero at $s = s_0$ of the Artin L-series attached to ψ corresponding to the Galois extension K/K^H. It can also be applied to the situation when E is an elliptic curve over k and $n(H, \psi)$ corresponds to the order of the zero at $s = s_0$ of the "twist" by ψ of the L-function of E over K^H (see [MM] for definitions and details).

We consider the following generalized character introduced by Heilbronn:

$$\theta_H = \sum_{\psi} n(H, \psi)\psi$$

where the sum is over all irreducible characters ψ of H. Our first step is to show that

Proposition 5.1 $\theta_G|_H = \theta_H$.

Proof.

$$\begin{aligned}\theta_G|_H &= \sum_{\chi} n(G, \chi)\chi|_H \\ &= \sum_{\chi} n(G, \chi)\left(\sum_{\psi} (\chi|_H, \psi)\psi\right)\end{aligned}$$

where the inner sum is over all irreducible characters of H and the outer sum is over all irreducible characters of G. By Frobenius reciprocity, $(\chi|_H, \psi) = (\chi, \operatorname{Ind}_H^G \psi)$ and so

$$\theta_G|_H = \sum_{\psi}\left(\sum_{\chi} n(G, \chi)(\chi, \operatorname{Ind}_H^G \psi)\right)\psi.$$

But now, by property (1), the inner sum is $n(G, \operatorname{Ind}_H^G \psi)$ which equals $n(H, \psi)$ by property (2). Thus, $\theta_G|_H = \theta_H$.

This immediately implies:

Proposition 5.2 *Let* reg *denote the regular representation of G. Suppose for every cyclic subgroup H of G, we have $n(H, \psi) \geq 0$. Then $n(G, \chi)$ is real for every irreducible character χ of G and*

$$\sum_{\chi} n(G, \chi)^2 \leq n(G, \mathrm{reg})^2.$$

Proof. By Artin's theorem, every character can be written as a rational linear combination of characters induced from cyclic subgroups and so $n(G, \chi)$ is real. By the orthogonality relations,

$$(\theta_G, \theta_G) = \sum_{\chi} n(G, \chi)^2.$$

On the other hand,

$$(\theta_G, \theta_G) = \frac{1}{|G|}\sum_{g \in G} |\theta_G(g)|^2.$$

By Proposition 5.1,

$$\theta_G(g) = \theta_{\langle g \rangle}(g) = \sum_{\psi} n(\langle g \rangle, \psi)\psi(g)$$

which is bounded by $n(G, \mathrm{reg})$ in absolute value by our hypothesis and property (1). This completes the proof.

Similar reasoning implies

Proposition 5.3 *Let ρ be an arbitrary character of G. Suppose for every cyclic subgroup H of G, and irreducible character ψ of H, we have $n(H, \rho|_H \otimes \psi) \geq 0$, then $n(G, \rho \otimes \chi)$ is real for every irreducible character χ of G and*

$$\sum_{\chi} n(G, \rho \otimes \chi)^2 \leq n(G, \rho \otimes \mathrm{reg})^2.$$

These results can also be generalized to the context of automorphic forms. Some preliminary work in this direction can be found in [MM].

§6 Low order zeros of Dedekind zeta functions

By analogy with the conjecture that the zeros of the Riemann zeta function are simple, one expects that the n_χ are bounded. One might ask whether

$$n_\chi \ll \chi(1)$$

or even the stronger

$$n_\chi \ll 1$$

holds.

We begin by establishing a zero-free region for Dedekind zeta functions. This is due to Stark [St]. This in turn gives a region where Artin L-functions are zero-free except possibly for a simple exceptional zero.

Proposition 6.1 *Let M be an algebraic number field of degree $n = r_1 + 2r_2$ where M has r_1 real embeddings and $2r_2$ complex conjugate embeddings. For $\sigma > 1$ we have*

$$-\frac{\zeta_M'}{\zeta_M}(\sigma) < \frac{1}{\sigma} + \frac{1}{\sigma - 1} + \frac{1}{2}\log\left(\frac{|d_m|}{2^{2r_2}\pi^n}\right) + \frac{r_1}{2}\frac{\Gamma'}{\Gamma}(\sigma/2) + r_2\frac{\Gamma'}{\Gamma}(\sigma).$$

Also, if $M \neq \mathbb{Q}$, ζ_M has at most one zero in the region

$$\sigma \geq 1 - \frac{1}{4\log|d_m|}, \quad |t| \leq \frac{1}{4\log|d_m|}.$$

Proof. Consider $f(s) = s(s-1)\zeta_M(s)$. By logarithmically differentiating the Hadamard factorization, we get the relation

$$\sum_\rho \frac{1}{s-\rho} = \frac{1}{s-1} + \frac{1}{2}\log|d_m| + \left(\frac{1}{s} - \frac{n}{2}\log\pi\right) + \frac{r_1}{2}\frac{\Gamma'}{\Gamma}(\frac{s}{2}) + r_2\left(\frac{\Gamma'}{\Gamma}(s) - \log 2\right) + \frac{\zeta_M'}{\zeta_M}(s).$$

The sum on the left runs over zeros ρ of $\zeta_M(s)$ in the strip $o < \sigma < 1$ and the terms with ρ and $\bar{\rho}$ are grouped together.

For $s = \sigma > 1$ we have

$$\frac{1}{\sigma-\rho} + \frac{1}{\sigma-\bar{\rho}} > 0.$$

Thus for $\sigma > 1$ we have

$$\sum_\rho{}' \frac{1}{\sigma-\rho} \leq \sum_\rho \frac{1}{\sigma-\rho}$$

where the sum on the left denotes summation over any convenient subset of the zeros ρ which is closed under complex conjugation. In particular, the sum

$$\sum \frac{1}{\sigma-\rho}$$

is positive and we deduce the inequality of the Proposition.

Now take $s = \sigma$ with $1 < \sigma < 2$. All the terms on the right of the above inequality after $\frac{1}{2}\log|d_m|$ are negative and thus

$$\sum_\rho{}' \frac{1}{\sigma-\rho} < \frac{1}{\sigma-1} + \frac{1}{2}\log|d_m|.$$

If $\rho = \beta + i\gamma$ is in the rectangle specified in the statement, (with $\gamma \neq 0$) then $\bar{\rho}$ is also in the same rectangle and taking the contribution from ρ and $\bar{\rho}$ only, we get the inequality

$$\frac{2(\sigma-\beta)}{(\sigma-\beta)^2+\gamma^2} < \frac{1}{\sigma-1} + \frac{1}{2}\log|d_m|.$$

But this is false for $M \neq \mathbb{Q}$ at $\sigma = 1 + \frac{1}{\log|d_m|} < 2$. The same value of σ gives a contradiction if there are two real zeroes in this rectangle (or a single real multiple zero). This completes the proof of the Proposition.

The following consequence is also due to Stark [St].

Corollary 6.2 *Let K/F be a Galois extension. For any Artin L-function $L(s,\chi,F)$ of this extension, the region*

$$\sigma \geq 1 - \frac{1}{4\log|d_k|}, \quad |t| \leq \frac{1}{4\log|d_k|}.$$

is free of zeros except possibly for a simple zero. This zero exists only if χ is a real Abelian character of a quadratic subfield of K.

Next, we examine the case when the Dedekind zeta function may in fact vanish, but the order of zero is small. We shall study this under the assumption that K/F itself is a solvable Galois extension. If we are at a point $s = s_0$ where $\zeta_K(s)$ has a "small" order zero, then it is possible to show more than just the analyticity of $\zeta_K(s)/\zeta_F(s)$ at s_0. We have the following result due to Foote and K. Murty [FM].

Theorem 6.3 *Let K/F be a solvable extension and write*

$$[K : F] = p_1^{\alpha_1} \cdots p_t^{\alpha_t}, \quad p_1 < p_2 < \cdots < p_t$$

for the prime power decomposition of the degree. Suppose that at $s = s_0$, we have

$$r = ord_{s=s_0}\zeta_K(s) \leq p_2 - 2.$$

Then for each $\chi \in Irr(G)$, the Artin L-series $L(s,\chi,F)$ is analytic at $s = s_0$.

This has the following immediate corollary.

Corollary 6.4 *If K/F is a Galois extension of odd degree and $\zeta_K(s)$ has a zero of order ≤ 3 at a point s_0 then all Artin L-functions of K/F are analytic at s_0.*

This represents a partial generalization of the result Corollary 6.2 of Stark. Of course, Stark's result makes no assumption on the Galois group of K/F.

We give a brief outline of the proof. Assume the theorem is false, and take G to be a minimal counterexample for which Artin's conjecture fails, at a point $s = s_0$ where the order of $\zeta_K(s)$ is small as explained in the statement. We want to prove that the generalized character θ_G defined above is an actual character. We repeatedly use the two key properties of θ_G namely,

$$\theta_G|_H = \theta_H \text{ for any subgroup } H \text{ of } G$$

and

$$\theta_G(1) = ord_{s=s_0}\zeta_K(s).$$

The first follows from Proposition 5.1 and the second follows from the factorization of ζ_K into the $L(s,\chi,F)$. Moreover, by our assumption of minimality, we may suppose that θ_H is a character for every proper subgroup H of G. In addition, the induction hypothesis and the invariance of L-functions under induction allow us to assume that χ is not induced from any proper subgroup of G. Also, we may assume that χ is faithful. For if $\operatorname{Ker}\chi$ is non-trivial and M (say) denotes its fixed field, then by the Aramata-Brauer theorem (Theorem 3.1), $\zeta_M(s)$ divides $\zeta_K(s)$. In particular, $ord_{s=s_0}\zeta_M(s) \leq r$ and the second smallest prime divisor of $[M : F]$ is $\geq p_2$. Since $L(s, \chi, F)$ is the same whether viewed as an L-function of K or M, the analyticity of this L-function at s_0 would follow from the induction hypothesis.

We now decompose θ_G into three parts $\theta_1, \theta_2, \theta_3$ as follows. Let θ_3 be the sum of all terms $n_\lambda \lambda$ such that λ is *not* a faithful character of G. Let $-\theta_2$ be the sum of all terms $n_\chi \chi$ for which n_χ is *negative*. Finally, let θ_1 be the sum of all terms $n_\psi \psi$ where ψ is a faithful character with $n_\psi > 0$. Again by the assumption of minimality, we see that $(\theta_2, \theta_3) = 0$ and by definition, θ_1 is orthogonal to θ_2 and θ_3. Thus, we get the decomposition

$$\theta_G = \theta_1 - \theta_2 + \theta_3.$$

We will now get further information about the constituents of θ_2 by restricting to an appropriate subgroup. As we shall see, a key tool in this is Clifford's theorem. It provides us with two pieces of information.

Firstly, since G is solvable and non-abelian, it has a normal subgroup N of prime index, p say, which contains the center $Z(G)$ of G. Clifford's theorem tells us that for any $\chi \in Irr(G)$, $\chi|_N$ is either irreducible or χ is the induction of a character from N. In particular, if we take for χ a summand of θ_2, it follows that $\chi|_N$ is irreducible.

Secondly, it tells us that any abelian normal subgroup must be central (that is, contained in the center), for otherwise every $\chi \in Irr(G)$ would be induced from a proper subgroup contradicting the non-triviality of θ_2.

Now, *every* non-trivial normal subgroup of a solvable group contains a non-trivial abelian subgroup which is normal in G. Thus, no irreducible constituent λ of θ_3 is faithful on the center. We must therefore have

$$(\theta_2|_N, \theta_3|_N) = 0.$$

Since

$$\theta_G|_N = \theta_1|_N - \theta_2|_N + \theta_3|_N$$

is a character of N, it follows that

$$\text{either } \theta_1|_N = \theta_2|_N \text{ or } \theta_1|_N = \theta_2|_N + \phi$$

for some character ϕ of N. A further argument using Clifford's theorem in fact eliminates the second possibility. Indeed, choose an irreducible component α of $\phi = \theta_1|_N - \theta_2|_N$ and let ψ be an irreducible component of $\theta_1 - \theta_2$ such that $\psi|_N$ contains α. Notice that the G conjugates of α are also contained in $\theta_1|_N - \theta_2|_N$

and hence also in $\psi|_N$. It follows that the sum of the distinct conjugates form a character of degree $\leq \phi(1)$. Clifford's theorem tells us that $\psi|_N$ is equal to this sum and so $\psi(1) \leq \phi(1) \leq r$. Also, ψ is a constituent of θ_1 and so it is faithful by definition.

Now, a theorem of Ito tells us that in a solvable group, a p-Sylow subgroup is abelian and normal if there is a faithful character of degree smaller than $p-1$. Thus, the conclusion of the previous paragraph and our assumption that $r \leq p_2 - 2$ imply that G has an abelian normal subgroup of order $n/p_1^{\alpha_1}$. This would force G to be nilpotent and Artin's conjecture is known to hold for such groups as every irreducible character is monomial. This again contradicts the nontriviality of θ_2. We conclude that $\theta_1|_N = \theta_2|_N$. This is the only step in which the assumed bound on r is used.

The final contradiction now comes by showing that $\theta_1 = \theta_2$. To do this, take $x \in G\backslash N$. Denote by H the subgroup generated by x and the center of G. As H is abelian, it is a proper subgroup of G. As we observed earlier, every irreducible component λ of θ_3 has the property that its kernel $\mathrm{Ker}\,\lambda$ meets the center non-trivially. Thus, the same holds for $\mathrm{Ind}_H^G(\lambda|_H)$. Now, taking an irreducible component χ of θ_2, we know that χ is faithful and so

$$(\chi, \mathrm{Ind}_H^G(\lambda|_H)) = 0.$$

By Frobenius reciprocity, $(\chi|_H, \lambda|_H) = 0$ and so

$$(\theta_2|_H, \theta_3|_H) = 0.$$

Now,

$$\theta_G|_H = \theta_1|_H - \theta_2|_H + \theta_3|_H$$

and again $\theta_G|_H$ is a character of H. Thus, $\theta_1|_H - \theta_2|_H$ is either zero or a character. By our earlier argument, we know that $\theta_1(1) = \theta_2(1)$ and so we must have $\theta_1|_H = \theta_2|_H$. Combined with our earlier result for N it follows that

$$\theta_1 = \theta_2.$$

This contradiction completes the proof.

The argument suggests that the condition $r \leq p_2 - 2$ be replaced by a bound on r involving the least degree of a faithful character. Results in this direction have in fact now been obtained by Foote [Fo] and by Foote and Wales [FW].

§7 Chebotarev density theorem

Let K/F be a finite Galois extension of number fields with group G. Let C be a subset of G which is stable under conjugation. Thus C is a union of conjugacy classes. Define

$$\pi_C(x) = \#\{\nu \text{ a place of } F \text{ unramified in } K,\ \mathbf{N}_{F/\mathbb{Q}}(\mathfrak{p}_\nu) \leq x \text{ and } \sigma_\nu \subset C\}.$$

The Chebotarev density theorem asserts that

$$\pi_C(x) \sim \frac{|C|}{|G|}\pi_F(x)$$

where $\pi_F(x)$ denotes the number of primes of F of norm $\leq x$. Effective versions of this theorem were given by Lagarias and Odlyzko [LO]. We state two of their results. The first of these assumes the Riemann Hypothesis for Dedekind zeta functions. The second is unconditional.

Theorem 7.1 *Suppose the Dedekind zeta function $\zeta_K(s)$ satisfies the Riemann hypothesis. Then*

$$\pi_C(x) = \frac{|C|}{|G|}\pi_F(x) + \mathbf{O}(\frac{|C|}{|G|} \cdot x^{\frac{1}{2}}(\log d_L + n_L \log x)).$$

This version of their result is only slightly more refined than the statement given in [LO] and is due to Serre [Se2, p. 133]. The proof of Theorem 7.1 is very analogous to the classical proof of the prime number theorem in arithmetic progressions, as presented, for example, in the monograph of Davenport [D]. However, there are some points of difference and we now briefly discuss them.

As in the classical case, the proof begins by expressing the characteristic function of the conjugacy class C in terms of characters of G. However, we have to deal with the fact that G is non-abelian and that we do not know the analytic properties of Artin L-functions. In particular, we do not know Artin's conjecture. We have

$$\delta_C = \frac{|C|}{|G|}\sum_{\chi}\overline{\chi(g_C)}\chi$$

where δ_C denotes the characteristic function of the class C and g_C is any element in this class. Hence

$$\pi(x, \delta_C) = \frac{|C|}{|G|}\sum_{\chi}\overline{\chi(g_C)}\pi(x, \chi)$$

where for any class function ϕ we set

$$\pi(x, \phi) = \sum_{\mathbf{N}\nu \leq x} \phi(\sigma_\nu).$$

Here the sum is over places ν of F unramified in K and of norm $\leq x$.

If we want to include ramified primes and also prime powers in the sums, we introduce the function

$$\tilde{\pi}(x, \phi) = \sum_{\mathbf{N}\nu^m \leq x} \phi(\sigma_\nu^m)$$

where in the case ν is a ramified prime, we define

$$\phi(\sigma_\nu^m) = \frac{1}{|I_w|}\sum \phi(g)$$

where I_w is the inertia group at a prime w of K dividing ν and the sum is over elements g in the decomposition group D_w whose image in the quotient D_w/I_w maps to σ_ν^m. The advantage in this sum $\tilde{\pi}$ is that it is closely related to the logarithmic derivative of the Artin L function.

At this point, we use some group theory to replace the Artin L-functions with Hecke L-functions. Indeed, let H be a subgroup of G and h an element of H. Let C_H denote its conjugacy class in H and C its conjugacy class in G. Let

$$\delta : H \longrightarrow \{0,1\}$$

denote the characteristic function of C_H. Now set

$$\phi = \operatorname{Ind}_H^G \delta.$$

By definition, we see that ϕ is supported only on the conjugacy class C and so $\phi = \lambda\delta_C$. The value of λ is easily computed by Frobenius reciprocity:

$$\lambda\frac{|C|}{|G|} = (\phi, 1_G) = (\delta, 1_H) = \frac{|C_H|}{|H|}.$$

Thus

$$\lambda = \frac{|C_H|\cdot|G|}{|H|\cdot|C|}.$$

From the inductive property of L-functions, it is not hard to see that

$$\tilde{\pi}(x,\phi) = \tilde{\pi}(x,\delta).$$

Now the right hand side is written as a sum involving the characters of H. In particular, if we are given C and we let H be the cyclic subgroup generated by g_C then we are able to express $\tilde{\pi}(x,\delta_C)$ in terms of Hecke L-functions. As we know the analytic properties of these L-functions, we are now able to follow rather closely the classical method as developed in [D] to prove Theorem 7.1.

Though the above technique has the advantage of replacing the non-abelian L-functions with abelian ones, it does so at some cost. The estimates will now involve the field constants (that is, degree, discriminant, etc.) of the fixed field M (say) of H. In general, as we do not have any information about M we are forced to majorize its field constants by those of K and this magnifies the error terms significantly.

This problem could be avoided if we were able to deal directly with the Artin L-functions. This theme is developed in the next section. We conclude this section by stating some unconditional results developed in [LO] and in [LMO].

Theorem 7.2 *If* $\log x \gg n_L(\log d_L)^2$, *then*

$$|\pi_C(x) - \frac{|C|}{|G|}\operatorname{Li}(x)| \le \frac{|C|}{|G|}\operatorname{Li}(x^\beta) + \mathbf{O}(|\tilde{C}|x\exp(-cn_L^{-\frac{1}{2}}(\log x)^{\frac{1}{2}}))$$

where $|\tilde{C}|$ *is the number of conjugacy classes contained in* C, β *is the exceptional zero of Proposition* 6.1, *and the term* $\frac{|C|}{|G|}\operatorname{Li}(x^\beta)$ *is to be suppressed if the exceptional zero* β *does not exist.*

Sometimes it is useful to have an inequality rather than an explicit error term. Such a bound is provided by the following result of Lagarias, Odlyzko and Montgomery [LMO].

Theorem 7.3 *We have*

$$\pi_C(x) \ll \frac{|C|}{|G|}\operatorname{Li}(x)$$

provided

$$\log x \gg (\log d_L)(\log\log d_L)(\log\log\log e^{20}d_L).$$

In applying these results, it is very useful to have some estimates for the discriminant of a field. These upper bounds are consequences of an inequality due to Hensel, and are developed in [Se2]. Let $\mathfrak{D}_{K/F}$ denote the different of K/F. It is an ideal of $\mathcal{O}_K$ and its norm $\mathfrak{d}_{K/F}$ from K to F is the discriminant of the extension. Let ν be a place of F and w a place of K dividing it. Let p_ν denote the residue characteristic of ν. Hensel's estimate states

$$w(\mathfrak{D}_{K/F}) = e_{w/\nu} - 1 + s_{w/\nu}$$

where

$$0 \le s_{w/\nu} \le w(e_{w/\nu}).$$

Here $e_{w/\nu}$ is the ramification index of $\mathfrak{p}_\nu$ in K. Using this, one can get an estimate for the norm of the relative discriminant. Let us set

$$n_K = [K:\mathbb{Q}], \quad n_F = [F:\mathbb{Q}]$$

and

$$n = [K:F] = n_K/n_F.$$

Let us also set $P(K/F)$ to be the set of rational primes p for which there is a prime $\mathfrak{p}$ of F with $\mathfrak{p}|p$ and $\mathfrak{p}$ is ramified in K. Then,

$$\log \mathbf{N}_{F/\mathbb{Q}}\mathfrak{d}_{K/F} \le (n_K - n_F)\sum_{p\in P(K/F)}\log p + n_K(\log n)|P(K/F)|.$$

This bound does not assume that K/F is Galois. If we know in addition that K/F is Galois, the following slightly stronger estimate holds:

$$\log \mathbf{N}_{F/\mathbb{Q}}\mathfrak{d}_{K/F} \le (n_K - n_F)\sum_{p\in P(K/F)}\log p + n_K(\log n).$$

There is an analogue of this for Artin conductors also. This analogue is needed in the proofs of the results of the next section.

Proposition 7.4 *Suppose that K/F is Galois with group G. Let χ denote an irreducible character of G and denote by $\mathfrak{f}_\chi$ its Artin conductor. Then*

$$\log \mathbf{N}_{F/\mathbb{Q}}\mathfrak{f}_\chi \leq 2\chi(1)n_F\{\sum_{p\in P(K/F)} \log p + \log n\}.$$

Proof. Firstly, we observe that for each $i \geq 0$,

$$\dim V^{G_i} = \frac{1}{|G_i|}\sum_{a\in G_i}\chi(a),$$

where G_i is as in Section 2.

Thus, for each finite ν,

$$n(\chi,\nu) = \sum_i \frac{|G_i|}{|G_0|}\left(\chi(1) - \frac{1}{|G_i|}\sum_{a\in G_i}\chi(a)\right).$$

Denote by $\mathcal{O}_\nu$ (respectively $\mathcal{O}_w$) the ring of integers of F_ν (resp. K_w). Define a function i_G on G by

$$i_G(g) = w(gx - x) = \max\{i : g \in G_{i-1}\}$$

where $\mathcal{O}_w = \mathcal{O}_\nu[x]$. Rearranging gives

$$n(\chi,\nu) = \frac{\chi(1)}{|G_0|}\sum_i(|G_i| - 1) - \frac{1}{|G_0|}\sum_{1\neq a\in G_0}\chi(a)i_G(a).$$

Applying this formula for χ the trivial character, and the character of the regular representation of G_0, we find that

$$\sum_{1\neq a\in G_0} i_G(a) = \sum_i(|G_i| - 1) = w(\mathfrak{D}_{K/F}).$$

Hence,

$$n(\chi,\nu) = \frac{1}{|G_0|}\sum_{1\neq a\in G_0} i_G(a)(\chi(1) - \chi(a)) \leq \frac{2\chi(1)w(\mathfrak{D}_{K/F})}{e_{w/\nu}}.$$

Now using the above stated estimate for $w(\mathfrak{D}_{K/F})$ we deduce that

$$\log \mathbf{N}\mathfrak{f}_\chi \leq 2\chi(1)\sum \frac{1}{e_{w/\nu}}(e_{w/\nu} - 1 + s_{w/\nu})f_\nu \log p_\nu$$

and this is

$$\leq 2\chi(1)\left\{\sum f_\nu\left(1-\frac{e_\nu}{e_w}\right)\log p_\nu + \sum f_\nu \frac{e_\nu}{e_w} w(e_{w/\nu})\log p_\nu\right\}$$

where e_ν (resp. e_w) denotes absolute ramification index at ν (resp. w) and we have used $e_{w/\nu} = e_w/e_\nu$. Also, as $w(e_{w/\nu}) = e_w \nu_p(e_{w/\nu})$ and as K/F is Galois, $e_{w/\nu}$ divides n. Thus

$$\log \mathbf{N}\mathfrak{f}_\chi \leq 2\chi(1)n_F\left\{\sum_{p\in P(K/F)} \log p + \log n\right\}.$$

This completes the proof.

We remark that there is no analogue of Hensel's estimate in the function field case. This is one source of difficulty in extending to this case the effective versions of the Chebotarev density theorem discussed in this and the next section. The reader is referred to [MS] and the references therein for the function field analogues.

§8 Consequences of Artin's conjecture

These estimates can be significantly improved if we know Artin's conjecture on the holomorphy of L-series. The improvement is in the dependence of the error term on C. The results of this section are from the paper [MMS]. We shall only discuss the conditional result Proposition 7.1.

Let χ be a character of G and denote by $\pi(x,\chi)$ the function

$$\pi(x,\chi) = \sum_{\mathbf{N}\nu\leq x} \chi(\sigma_\nu).$$

Let $\delta(\chi)$ denote the multiplicity of the trivial character in χ.

As before (see §2)

$$A_\chi = d_K^{\chi(1)}\mathbf{N}_{F/\mathbb{Q}}(\mathfrak{f}_\chi)$$

and

$$\Lambda(s,\chi) = \Lambda(s,\chi,F) = A_\chi^{s/2}\gamma(s,\chi,F)L(s,\chi)$$

Proposition 8.1 *Suppose that the Artin L-series $L(s,\chi)$ is analytic for all $s \neq 1$ and is nonzero for* $\mathrm{Re}(s) \neq \frac{1}{2}, 0 < \mathrm{Re}(s) < 1$. *Then*

$$\pi(x,\chi) = \delta(\chi)\,\mathrm{Li}(x) + \mathbf{O}(x^{\frac{1}{2}}((\log A_\chi) + \chi(1)n_F\log x)) + \mathbf{O}(\chi(1)n_F \log M(K/F))$$

where

$$M(K/F) = nd_F^{1/n_F}\prod_{p\in P(K/F)} p.$$

Proof. The argument proceeds along standard lines and so we just sketch it here. Artin proved the functional equation

$$\Lambda(s,\chi) = W(\chi)\Lambda(1-s,\bar{\chi})$$

where $W(\chi)$ is a complex number of absolute value 1 and $\bar{\chi}$ is the complex conjugate of χ. We know that

$$(s(s-1))^{\delta(\chi)}\Lambda(s,\chi)$$

is entire and we have the Hadamard factorization

$$\Lambda(s,\chi) = e^{a(\chi)+b(\chi)s}\prod(1-\frac{s}{\rho})e^{s/\rho}(s(s-1))^{-\delta(\chi)}$$

where $a(\chi), b(\chi) \in \mathbb{C}$ and the product runs over all zeroes ρ of $\Lambda(s,\chi)$ (ncecessarily $0 \le \mathrm{Re}(\rho) \le 1$.) From the equality

$$\overline{\Lambda(s,\chi)} = \Lambda(\bar{s},\bar{\chi})$$

we deduce the relation

$$\overline{\frac{\Lambda'}{\Lambda}(s,\chi)} = \frac{\Lambda'}{\Lambda}(\bar{s},\bar{\chi}).$$

Moreover, the functional equation implies the relation

$$\frac{\Lambda'}{\Lambda}(s,\chi) = -\frac{\Lambda'}{\Lambda}(1-s,\bar{\chi}).$$

From these two relations, we deduce that

$$\mathrm{Re}\,\frac{\Lambda'}{\Lambda}(\frac{1}{2},\chi) = 0.$$

Also, if ρ is a zero of $\Lambda(s,\chi)$ then so is $1-\bar{\rho}$. Hence,

$$\mathrm{Re}\sum(\frac{1}{2}-\rho)^{-1} = 0$$

as is seen by grouping together the terms corresponding to ρ and $1-\bar{\rho}$ in the absolutely convergent sum. Logarithmically differentiating the product formula at $s=\frac{1}{2}$ and taking real parts, we deduce that

$$\mathrm{Re}(b(\chi)+\sum\frac{1}{\rho}) = 0.$$

Hence,

$$\mathrm{Re}\,\frac{\Lambda'}{\Lambda}(s,\chi) = \sum_{\rho}\mathrm{Re}(\frac{1}{s-\rho}) - \delta(\chi)\,\mathrm{Re}(\frac{1}{s}+\frac{1}{s-1}).$$

Let $N(t,\chi)$ denote the number of zeros $\rho = \beta + i\gamma$ of $L(s,\chi)$ with $0 < \beta < 1$ and $|\gamma - t| \le 1$. Evaluating the above formula at $s = 2 + it$ and observing that

$$\mathrm{Re}(\frac{1}{2+it-\rho}) = \frac{2-\beta}{(2-\beta)^2 + (t-\gamma)^2}$$

is non-negative for all ρ and is atleast $1/5$ if $|t-\gamma| \le 1$ we deduce that

$$N(t,\chi) \ll \mathrm{Re}\,\frac{\Lambda'}{\Lambda}(2+it,\chi).$$

Since the Dirichlet series for $L(s,\chi)$ converges at $2+it$, the right hand side is easily estimated, the essential contribution coming from $\log A_\chi$ and the number of Γ factors. We get

$$N(t,\chi) \ll \log A_\chi + \chi(1) n_F \log(|t|+5).$$

By developing an explicit formula as in [LO] or [Mu2] we find that

$$\begin{aligned}\sum_{\mathbf{N}\nu \le x}{}' \, \chi(\sigma_\nu) \log \mathbf{N}\nu = \delta(\chi)x - \sum_{|\gamma|<x} \frac{x^\rho}{\rho} &+ \mathbf{O}(\chi(1) n_F \log M(K/F)) \\ &+ \mathbf{O}(x^{\frac{1}{2}}(\log x)(\log A_\chi + \chi(1) n_F \log x)),\end{aligned}$$

where the prime on the sum indicates that we only include places ν that are unramified in K. The sum over zeros can be estimated by observing that

$$\sum_{|\gamma|<x} \frac{1}{\rho} \ll \sum_{j<x} \frac{N(j,\chi)}{j}$$

and using the above estimate for $N(t,\chi)$. The estimate for $\pi(x,\chi)$ can be deduced by partial summation.

Proposition 8.2 *Suppose that all Artin L-series of the extension K/F are analytic at $s \ne 1$ and that GRH holds. Then*

$$\sum_C \frac{1}{|C|} \left(\pi_C(x) - \frac{|C|}{|G|} \operatorname{Li} x \right)^2 \ll x n_F^2 (\log M(K/F)x)^2.$$

Proof. We first observe that

$$\sum_C \frac{1}{|C|} \left(\frac{|C|}{|G|} \pi(x, 1_G) - \frac{|C|}{|G|} \operatorname{Li} x \right)^2 = \frac{1}{|G|} (\pi(x,1_G) - \operatorname{Li} x)^2.$$

Expressing $\pi(x, 1_G)$ in terms of characters, we see that this is

$$\leq \frac{1}{|G|}\left(\sum_{\chi\neq 1}|\pi(x,\chi)|^2 + (\pi(x,1_G) - \operatorname{Li} x)^2\right)$$

where the sum is over the non-trivial irreducible characters of G. By Propositions 7.4 and 8.1,

$$\pi(x,\chi) - \delta(\chi)\operatorname{Li} x \ll \chi(1) n_F x^{\frac{1}{2}}(\log(M(K/F)x).$$

The result follows on noting that

$$\sum_{\chi}\chi(1)^2 = |G|.$$

Proposition 8.3 *Let D be a union of conjugacy classes. Under the same hypotheses as in Proposition* 8.2*, we have*

$$\pi_D(x) = \frac{|D|}{|G|}\operatorname{Li} x + \mathbf{O}(|D|^{\frac{1}{2}} x^{\frac{1}{2}} n_F \log M(K/F)x).$$

Proof. We have

$$\pi_D(x) - \frac{|D|}{|G|}\operatorname{Li} x = \sum_C\left(\pi_C(x) - \frac{|C|}{|G|}\operatorname{Li} x\right)$$

where the sum is taken over all conjugacy classes C contained in D. Now applying the Cauchy-Schwarz inequality we deduce that

$$\sum_C\left|\pi_C(x) - \frac{|C|}{|G|}\operatorname{Li} x\right| \ll (\sum_C|C|)^{\frac{1}{2}}\left(\sum_C\frac{1}{|C|}\left|\pi_C(x) - \frac{|C|}{|G|}\operatorname{Li} x\right|^2\right)^{\frac{1}{2}}.$$

The result now follows from Proposition 8.2.

Remark. Using Hensel's estimate for the discriminant, it is possible to write the error term in Theorem 7.1 as

$$\mathbf{O}(|C| x^{\frac{1}{2}} n_F \log M(K/F)x).$$

Thus Artin's conjecture allows us to replace $|C|$ with $|C|^{\frac{1}{2}}$. In some cases, we can also improve Theorem 7.1 even without assuming Artin's conjecture. We give two such results below.

Proposition 8.4 *Let D be a union of conjugacy classes in G and let H be a subgroup of G satisfying*

(i) *Artin's conjecture is true for the irreducible characters of H*

(ii) *H meets every class in D.*

Suppose the GRH holds. Then

$$\pi_D(x) = \frac{|D|}{|G|}\operatorname{Li} x + \mathbf{O}\left(x^{\frac{1}{2}}\left(\sum_{C\subseteq D}\frac{|C|^2}{|C_H|}\right)^{\frac{1}{2}} n_F \log Mx\right)$$

where $M = M(K/F)$ and $C_H = C_H(\gamma)$ for some $\gamma \in H\cap C$.

Proof. Firstly, we have the relation

$$\pi_D(x) = \tilde{\pi}_D(x) + \mathbf{O}(\frac{1}{|G|}\log d_K + n_F x^{\frac{1}{2}}).$$

Using the estimate from Hensel's bound, we have

$$\frac{1}{|G|}\log d_K \ll n_F \log Mx.$$

Also,

$$\tilde{\pi}_D(x) = \sum_{C\subseteq D}\tilde{\pi}_C(x) = \sum_{C\subseteq D}\frac{|C|}{|G|}\cdot\frac{|H|}{|C_H|}\tilde{\pi}_{C_H}(x). \tag{8.1}$$

Now,

$$\begin{aligned}
&\sum_{C\subseteq D}\frac{|C|}{|G|}\cdot\frac{|H|}{|C_H|}(\tilde{\pi}_{C_H}(x) - \pi_{C_H}(x))\\
&\quad\leq \frac{|H|}{|G|}\sum_{C\subseteq D}\frac{|C|}{|C_H|}\left(\sum_{\substack{\mathrm{N}\nu^m\leq x\\ m\geq 2}}\delta_{C_H}(\sigma_\nu^m) + \sum_{\substack{\mathrm{N}\nu\leq x\\ \nu \text{ ramified in } L/K}}\delta_{C_H}(\sigma_\nu)\right)\\
&\quad\leq \frac{|H|}{|G|}\left(\max_{C\subseteq D}\frac{|C|}{|C_H|}\right)\cdot\left\{\frac{|G|}{|H|}n_F x^{\frac{1}{2}} + \frac{2}{\log 2}\frac{1}{|H|}\log d_K\right\}\\
&\quad\leq \left(\max\frac{|C|}{|C_H|}\right)(n_F x^{\frac{1}{2}} + n_F\log Mx)
\end{aligned}$$

and this can be absorbed into the error term. Therefore, we can replace $\tilde{\pi}_{C_H}$ by π_{C_H} in the equation (8.1). Now,

$$\begin{aligned}
&\sum_{C\subseteq D}\frac{|C|}{|G|}\cdot\frac{|H|}{|C_H|}\pi_{C_H}(x)\\
&= \frac{|D|}{|G|}\operatorname{Li} x + \mathbf{O}\left(\frac{|H|}{|G|}\cdot\sum_{C\subseteq D}\frac{|C|}{|C_H|^{\frac{1}{2}}}\frac{1}{|C_H|^{\frac{1}{2}}}\left|\pi_{C_H}(x) - \frac{|C_H|}{|H|}\operatorname{Li} x\right|\right).
\end{aligned}$$

Now applying the Cauchy-Schwarz inequality and using Proposition 8.2, we find that the error term above is

$$\ll \frac{|H|}{|G|} \cdot \left(\sum_{C \subseteq D} \frac{|C|^2}{|C_H|} \right)^{\frac{1}{2}} x^{\frac{1}{2}} n_F \frac{|G|}{|H|} \log M(K/F')x$$

where F' is the fixed field of H. This proves the proposition since $M(K/F') \ll M(K/F)$.

We state one immediate corollary of this result.

Corollary 8.5 *Under the same hypotheses as above,*

$$\pi_D(x) = \frac{|D|}{|G|} \operatorname{Li} x + \mathbf{O}\left(|D|^{\frac{1}{2}} x^{\frac{1}{2}} \left(\frac{|G|}{|H|} \right)^{\frac{1}{2}} n_F \log Mx \right).$$

The corollary follows immediately on noting that

$$\frac{|C|}{|C_H|} \leq \frac{|G|}{|H|}.$$

We now present one further result in this direction. This estimate has the feature that in some cases, it gives a better result than what one deduces from Artin's conjecture.

Proposition 8.6 *Suppose the GRH holds. Let D be a nonempty union of conjugacy classes in G and let H be a normal subgroup of G such that Artin's conjecture is true for the irreducible characters of G/H and $HD \subseteq D$. Then*

$$\pi_D(x) = \frac{|D|}{|G|} \operatorname{Li} x + \mathbf{O}\left(\left(\frac{|D|}{|H|} \right)^{\frac{1}{2}} x^{\frac{1}{2}} n_F \log Mx \right)$$

where M is as in the previous proposition.

Proof. Let $\bar{D}$ be the image of D in G/H. It is a union of conjugacy classes in G/H and

$$\pi_{\bar{D}}(x) = \frac{|\bar{D}| \cdot |H|}{|G|} \operatorname{Li} x + \mathbf{O}(|\bar{D}|^{\frac{1}{2}} x^{\frac{1}{2}} n_F \log M(F'/F)x)$$

where F' is the fixed field of H. As $HD \subseteq D$,

$$|\bar{D}| \cdot |H| = |D|$$

and

$$\pi_D(x) = \pi_{\bar{D}}(x) + \mathbf{O}((\log d_K)/|G|).$$

Also, $M(F'/F) \ll M(K/F)$. The result follows.

Finally, we can ask what the true order of the error term in the Chebotarev theorem should be. Let $\alpha(G)$ denote the number of conjugacy classes of G.

Question. Is it true that for any conjugacy set $D \subseteq G$,

$$\pi_D(x) = \frac{|D|}{|G|} \operatorname{Li} x + \mathbf{O}\left(\left(\frac{|D|}{\alpha(G)}\right)^{\frac{1}{2}} x^{\frac{1}{2}} n_F \log Mx\right)?$$

This would be implied by the Proposition 8.2 if all the terms are of the same order. In the case $F = \mathbb{Q}$ and K/F is Abelian, our question is a well-known conjecture of Montgomery.

§9 The least prime in a conjugacy class

Let L/K be a finite non-trivial Galois extension of number fields with group G. Our main result is an estimate, assuming the Riemann Hypothesis for Dedekind zeta functions (GRH), for the least norm of a prime ideal of K which is unramified in L and which does not split completely. The results of this section are from [Mu3].

If C is any subset of G stable under conjugation, Lagarias and Odlyzko [LO, pp. 461–462] showed, assuming (GRH) that there is a prime ideal $\mathfrak{p}$ with

$$N_{K/\mathbb{Q}}\mathfrak{p} \ll (\log |d_L|)^2 \tag{9.1}$$

for which the Frobenius conjugacy class $\sigma_{\mathfrak{p}}$ of $\mathfrak{p}$ lies in C. Here, d_L (resp. d_K) denotes the (absolute) discriminant of L (resp. K). In this estimate, an important tool was the effective version of the Chebotarev density theorem proved in [LO]. By the results of the previous section, it follows that the assumption of Artin's conjecture (AC) on the holomorphy of Artin L- series allows one to prove a sharper version of this theorem. In particular, the assumption of AC implies that the estimate (9.1) may be improved to

$$\mathbf{N}_{K/\mathbb{Q}}\mathfrak{p} \ll \frac{(\log |d_L|)^2 (\log |G|)^2}{|C|}. \tag{9.2}$$

In fact, the term $(\log |G|)^2$ may also be removed by using a more detailed argument. The purpose of this section is to show, assuming the GRH, that in the special case $C = G - \{1\}$, there is a prime ideal $\mathfrak{p}$ of K of degree 1 which is unramified in L which does not split completely and which satisfies

$$\mathbf{N}_{K/\mathbb{Q}}\mathfrak{p} \ll \left(\frac{\log |d_L|}{|G| - 1}\right)^2 \ll \left(\frac{n_K}{n_L} \log |d_L|\right)^2. \tag{9.3}$$

where $n_K = [K : \mathbb{Q}]$ and $n_L = [L : \mathbb{Q}]$. Thus, the estimate (9.3) shows that for the special set $C = G - \{1\}$, one can do substantially better than (9.1).

Next, we shall show that for certain subgroups H of G the bound (9.3) may be extended for the least norm of a prime ideal $\mathfrak{p}$ for which $\sigma_{\mathfrak{p}}$ does not intersect H. The precise statement is given in Theorem 9.3.

We apply these last results to the group of points on an elliptic curve over a finite field. Let E be an elliptic curve without complex multiplication and defined over $\mathbb{Q}$. Denote by $\mathcal{N}$ the conductor of E.

Let us set

$$T = \mathrm{lcm}_{E'} |E'(\mathbb{Q})_{\mathrm{tors}}|$$

where the lcm ranges over elliptic curves E' which are defined over $\mathbb{Q}$ and are $\mathbb{Q}$-isogenous to E. In [K, Th. 2] Katz proved that

$$\gcd |E(\mathbb{F}_p)| = T$$

where the *gcd* is taken over primes p of good reduction. It is well known and easily proved that both sides are divisible by the same primes. Using our results, we can make this effective in the following sense. Let $l \geq 5$ be a prime and assume the *GRH*. If l does not divide T then we show (Theorem 9.4) that there is a prime p so that

$$p \ll (\ell \log \mathcal{N} \ell)^2$$

and $E(\mathbb{F}_p)$ does not have a point of order ℓ.

We begin by proving the estimate (9.3). We recall that L/K is a *non-trivial* Galois extension.

Theorem 9.1 *Assume the GRH. Then, there exists a prime ideal* $\mathfrak{p}$ *of* K

(i) $\mathfrak{p}$ *is of degree* 1 *over* $\mathbb{Q}$ *and unramified in* L

(ii) $\mathfrak{p}$ *does not split completely in* L
and

$$\mathbf{N}_{K/\mathbb{Q}}\mathfrak{p} \ll \left(\frac{n_K}{n_L} \log |d_L|\right)^2$$

where $n_K = [K : \mathbb{Q}]$ *and* $n_L = [L : \mathbb{Q}]$.

Proof. We consider the kernel function of [LMO, §2], namely

$$k(s) = k(s; x, y) = \left(\frac{y^{s-1} - x^{s-1}}{s-1}\right)^2.$$

For $y > x > 1$ and $u > 0$, it has the property that the inverse Mellin transform

$$\hat{k}(u) = \frac{1}{2\pi i} \int_{(2)} k(s) u^{-s} ds$$

is given by the formulae

$$\hat{k}(u; x, y) = \begin{cases} 0 & \text{if} \quad u > y^2 \\ \frac{1}{u} \log \frac{y^2}{u} & \text{if} \quad xy < u < y^2 \\ \frac{1}{u} \log \frac{u}{x^2} & \text{if} \quad x^2 < u < xy \\ 0 & \text{if} \quad u < x^2. \end{cases}$$

Now consider the integral

$$J_K = \frac{1}{2\pi i}\int_{(2)} \left(-\frac{\zeta_K'}{\zeta_K}(s)\right) k(s;x,y)ds.$$

On the one hand, it is equal to

$$(\log y/x)^2 - \sum_\rho k(\rho;x,y)$$

where ρ runs over all zeroes of $\zeta_K(s)$. Write $\rho = \beta + i\gamma$. If $N_K(r;s_0)$ denotes the number of zeroes ρ of $\zeta_K(s)$ with $|\rho - s_0| \le r$ then ([LMO, Lemma 2.2])

$$N_K(r;s_0) \ll 1 + r(\log|d_K| + n_K \log(|s_0|+2)).$$

Since

$$|k(\rho;x,y)| \le \frac{x^{-2(1-\beta)}}{|\rho-1|^2}$$

it follows that

$$\sum_{\beta\le 1-\delta} k(\rho;x,y) \ll x^{-2\delta}\int_\delta^\infty \frac{1}{r^2}dN_K(r;1)$$
$$\ll x^{-2\delta}(\delta^{-2} + \delta^{-1}\log|d_K|).$$

As we are assuming the GRH, we may take $\delta = \frac{1}{2}$ and we see that

$$J_K = (\log\frac{y}{x})^2 + \mathbf{O}(x^{-1}\log|d_K|).$$

On the other hand, the integral is equal to the sum

$$\sum_{\mathfrak{p},m} \Lambda((N\mathfrak{p})^n)\hat{k}((N\mathfrak{p})^n;x,y).$$

The contribution to this sum of ideals $\mathfrak{p}^n$ for which $N\mathfrak{p}^n$ is not a rational prime is

$$\ll \frac{n_K(\log y)(\log y/x)}{x\log x}$$

as in [LMO, (2.6)]. Moreover, the contribution of primes $\mathfrak{p}$ which ramify in L is

$$\ll \sum_{\mathfrak{p}|d_{L/K}} (\log N\mathfrak{p})x^{-2}\log\frac{y}{x}$$

as in [LMO, (2.27)]. (Recall that $d_{L/K}$ is the norm to $\mathbb{Q}$ of the discriminant of the extension L/K.) Since [Se2, p. 129]

$$\sum_{\mathfrak{p}|d_{L/K}} \log N\mathfrak{p} \le \frac{2}{n}\log|d_L|,$$

the contribution of primes $\mathfrak{p}$ which ramify in L is

$$\ll \frac{1}{n}(\log |d_L|)x^{-2} \log \frac{y}{x}.$$

Let us set

$$\tilde{J_K} = \sum{}^*(\log N\mathfrak{p})\hat{k}(N\mathfrak{p}; x, y)$$

where the sum ranges over primes $\mathfrak{p}$ of K of degree 1 which are unramified in L. Then the above estimates imply that

$$\tilde{J_K} = (\log \frac{y}{x})^2 + \mathbf{O}\big(x^{-1} \log |d_K| + n_K(\log y)(\log \frac{y}{x})\frac{1}{x \log x} + (\frac{1}{n} \log |d_L|)x^{-2}(\log \frac{y}{x})\big).$$

On the other hand, by an argument similar to that given above,

$$J_L = (\log \frac{y}{x})^2 + \mathbf{O}(x^{-1} \log |d_L|).$$

Now if we suppose that *every* prime ideal $\mathfrak{p}$ of K with $N\mathfrak{p} \leq y^2$ either ramifies or splits completely in L, then

$$J_L \geq n\tilde{J_K}.$$

Putting this together with the above estimates, and choosing

$$x = (\frac{\alpha}{n} \log |d_L|)$$

and

$$y = bx$$

for some $b > 1$ and $\alpha > (\log b)^2$ we deduce the inequality

$$(n-1)(\log b)^2 \ll \frac{n}{\alpha} + \frac{n n_L (\log bx)(\log b)}{\alpha(\log |d_L|)(\log x)} + \frac{n^2(\log b)}{\alpha^2(\log |d_L|)} \ll n.$$

For a sufficiently large value of b, we get a contradiction. This completes the proof.

Remarks. 1. This method can also be used to produce an unconditional bound. In terms of its dependence on L the main term is $|d_L|^{1/2(n-1)}$.

2. Note that we used the normality of the extension L/K in asserting that a prime of K which splits completely in L has $[L : K]$ prime divisors in L.

3. We note an interesting consequence of the above. Assume the *GRH*. Suppose the class number h of K is larger than 1. There exists a non-principal prime ideal $\mathfrak{p}$ of K of degree 1 over $\mathbb{Q}$ with

$$N_{K/\mathbb{Q}}\mathfrak{p} \ll (\log |d_K|)^2.$$

Indeed, choose for L the Hilbert class field of K, and use the fact that $d_L = d_K^h$.

We describe two variants of Theorem 9.1.

(A) Consider the following diagram of fields.

$$\begin{array}{c} F \\ / \; / \quad \backslash \\ L_1 L_2 \ \dots \ L_r \\ \backslash \; \backslash \quad / \\ K \\ | \\ M \\ | \\ \mathbb{Q} \end{array}$$

Theorem 9.2 *Assume the GRH. Let $L_1, \dots, L_r$ be distinct non-trivial Galois extensions of K. Let F be an extension of K containing all the L_i and M a subfield of K so that F/M is Galois. Set*

$$m = \min[L_i : K]$$
$$f = [F : K]$$

and assume that

$$r < m.$$

Then, there exists a prime ideal $\mathfrak{p}$ of K satisfying

(i′) $\mathfrak{p}$ *is of degree 1 over $\mathbb{Q}$ and $N_{K/M}\mathfrak{p}$ does not ramify in F*

(ii′) $\mathfrak{p}$ *does not split completely in any of the L_i, $1 \le 1 \le r$ with*

$$N_{K/\mathbb{Q}}\mathfrak{p} \ll B^2$$

where

$$B = \max\left(\frac{\sum_{i=1}^{r} (\log |d_{L_i}|)}{m - r}, \sqrt{\frac{m}{f(m-r)} \log |d_F|} \right).$$

Proof. Let $\mathcal{S}$ denote the set of degree 1 prime ideals $\mathfrak{p}$ of K with $N\mathfrak{p} \le y^2$ for which $\mathfrak{p} \cap \mathcal{O}_M$ does not ramify in F. Suppose that every element of $\mathcal{S}$ splits completely in *some* L_i. Then, with notation as in the proof of Theorem 9.1, we have

$$\sum J_{L_i} \ge m \sum_{\mathfrak{p} \in \mathcal{S}} (\log N\mathfrak{p}) \hat{k}(N\mathfrak{p}; x, y).$$

Using the estimate for J_L and $\tilde{J}_K$ given in the proof of Theorem 9.1, we deduce that

$$r(\log\frac{y}{x})^2 + \mathbf{O}(\frac{1}{x}\sum_i \log|d_{L_i}|)$$

$$\geq m(\log\frac{y}{x})^2 + \mathbf{O}(\frac{m}{x}\log|d_K|) + \mathbf{O}(\frac{mn_K(\log y)(\log y/x)}{x\log x})$$

$$+ \mathbf{O}(\frac{m}{f}(\log|d_F|)\frac{1}{x^2}\log y/x).$$

Simplifying, and choosing $x = \alpha B$ and $y = \beta x$ with some $\beta > 1$ and $\alpha > (\log\beta)^2$, we get the inequality

$$(m-r)(\log\beta)^2 \leq \mathbf{O}((m-r)(\log\beta))$$

which is a contradiction if β is sufficiently large.

(B) With L/K a normal extension and $G = \mathrm{Gal}(L/K)$ as before, we take a subgroup H of G. We want to find a prime $\mathfrak{p}$ of K so that $\sigma_{\mathfrak{p}}$ is disjoint from H. Theorem 9.1 had to do with $H = \{1\}$.

Theorem 9.3. *Assume the GRH. Denote by $N = N_G(H)$ the normalizer of H in G and let R be the fixed field of N. Let $H_1, \ldots, H_r$ be a set of normal subgroups of N and $L_1, \ldots, L_r$ their respective fixed fields. Suppose that*
(1) *for each $g \in G$, $gHg^{-1} \cap N$ is contained in some $H_i (1 \leq i \leq r)$.*
(2) *if $m = \min[L_i : R]$ then $r < m$.*
Then, there exists a prime ideal $\mathfrak{p}$ of K with

$$N_{K/\mathbb{Q}}\mathfrak{p} \ll B_H^2$$

and satisfying
(a) *$\mathfrak{p}$ is of degree one and does not ramify in L*
(b) *$\sigma_{\mathfrak{p}}$ is disjoint from H.*
Here,

$$B_H = \max\left\{\frac{1}{m-r}\left(\sum\frac{1}{|H_i|}\right)\log|d_L|, \sqrt{\frac{m}{|N|(m-r)}(\log|d_L|)}\right\}.$$

Proof. Each L_i is a Galois extension of R and L is a Galois extension of R containing all the L_i. By Theorem 9.2, we can find a prime ideal $\mathfrak{P}$ of R of degree one (over $\mathbb{Q}$) so that $\mathfrak{p} = N_{R/K}\mathfrak{P}$ does not ramify in L, $\mathfrak{P}$ does not split completely in any of the L_i and

$$N_{R/\mathbb{Q}}\mathfrak{P} \ll B^2$$

where

$$B = \max\left\{\frac{1}{m-r}\sum_{i=1}^{r}\log|d_{L_i}|, \sqrt{\frac{m}{[L:R](m-r)}(\log|d_L|)}\right\}.$$

The splitting completely condition means that

$$\sigma_{\mathfrak{P}} \cap H_i = \phi \qquad 1 \leq i \leq r.$$

Now

$$\sigma_{\mathfrak{p}} = \cup_\tau \tau \sigma_{\mathfrak{P}} \tau^{-1}$$

where the union is over a set of coset representatives $\{\tau\}$ for N in G. It follows that

$$\sigma_{\mathfrak{p}} \cap H = \phi.$$

Hence $\mathfrak{p}$ satisfies (a) and (b). Now as

$$|d_{L_i}| \leq |d_L|^{1/|H_i|},$$

we deduce the stated bound.

Remarks. 1. In the case $r = 1$, the assumptions (1) and (2) may be stated as
(1′) for any $g \in G$, $gHg^{-1} \cap N$ is nonempty $\Rightarrow g \in N$
(2′) H is a proper subgroup of N.
2. If we are only interested in finding a prime $\mathfrak{p}$ so that $\sigma_{\mathfrak{p}} = (\mathfrak{p}, L/K)$ is not *contained* in H, then we do not need to consider the conjugates of H at all. Rather, it suffices to take a degree one prime $\mathfrak{P}$ of R such that $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ does not ramify in L and $(\mathfrak{P}, L/R)$ is not contained in H. But as H is normal in N, this just means that $\mathfrak{P}$ does not split completely in $M =$ the fixed field of H. We can find such a $\mathfrak{P}$ with

$$N_{R/\mathbb{Q}}\mathfrak{P} \ll \left(\frac{\log |d_L|}{|N| - |H|} \right)^2.$$

Corollary 9.4. *Let the notation and hypotheses be as in Theorem* 9.3. *If C is a subset of G stable under conjugation and H intersects every conjugacy class in C nontrivially, then there is a prime $\mathfrak{p}$ of K satisfying*

$$N_{K/\mathbb{Q}}\mathfrak{p} \ll B_H^2$$

as well as (a) *and*
(b′) *$\sigma_{\mathfrak{p}}$ is not contained in C.*

Let E be an elliptic curve defined over $\mathbb{Q}$ and let $\mathcal{N}$ denote its conductor. For $p \nmid \mathcal{N}$, we may consider the group $|E(\mathbb{F}_p)|$ of $\mathbb{F}_p$-rational points on E. Its cardinality is given by $|E(\mathbb{F}_p)| = p + 1 - a(p)$ for some integer $a(p)$.

The action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on points of $E(\bar{\mathbb{Q}})$ which are in the kernel of multiplication by ℓ gives a representation

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}_\ell).$$

It has the property that for $p \nmid \ell\mathcal{N}$, $\rho_\ell(\sigma_p)$ has trace $a(p)$ and determinant p modulo ℓ.

Recall that we have set

$$T = \mathrm{lcm}_{E'} |E'(\mathbb{Q})_{\mathrm{tors}}|$$

where the lcm ranges over elliptic curves E' which are $\mathbb{Q}$-isogenous to E.

Theorem 9.5 *Suppose that E does not have complex multiplication and let $\ell \geq 5$ be a prime which does not divide T. Denote by $\mathcal{N}$ the conductor of E. Assume the GRH. Then, there is a prime*

$$p \ll (\ell \log \ell\mathcal{N})^2$$

such that $E(\mathbb{F}_p)$ does not have a point of order ℓ.

Proof. Let us denote by G the image of ρ_ℓ. It is known that the fixed field of the kernel of ρ_ℓ contains the field of ℓ-th roots of unity. Let PG denote the image of G under the natural map $GL_2(\mathbb{F}_\ell) \to PGL_2(\mathbb{F}_\ell)$. It is well known (See [Se2, p. 197]) that one of the following holds:

(i) PG contains $PSL_2(\mathbb{F}_\ell)$
(ii) G is contained in a Borel subgroup of $GL_2(\mathbb{F}_\ell)$
(iii) G is contained in a non-split Cartan subgroup of $GL_2(\mathbb{F}_\ell)$
(iv) $PG \simeq A_4$, S_4 or A_5
(v) G is contained in the normalizer of a Cartan subgroup C but is not contained in C.

We shall consider each in turn.

(i): Consider the Borel subgroup (see [Se2, p. 197])

$$B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subseteq G = GL_2(\mathbb{F}_\ell)$$

and the subgroups

$$H = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\}, \quad H' = \left\{ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \right\}$$

of B. A simple calculation shows that

$$N_G(H) = N_G(H') = B.$$

We also have that for any $g \in G$,

$$gHg^{-1} \cap B \subseteq H' \text{ or } H.$$

We apply Theorem 9.3 to get a prime p which is unramified in L, the fixed field of the kernel of ρ_ℓ and which has the property that $\sigma_p \cap H = \phi$ and

$$p \ll x^2$$

where

$$x = \left\{ \frac{1}{\ell - 1 - 2} \; \frac{2}{\ell(\ell-1)} (\log |d_L|), \sqrt{\frac{\ell - 1}{\ell^4} (\log |d_L|)} \right\}.$$

Now by Hensel's inequality,

$$\log |d_L| \ll n_L \log \ell\mathcal{N} \ll \ell^4 \log \ell\mathcal{N}$$

and so

$$p \ll (\ell \log \ell\mathcal{N})^2.$$

Now consider

$$D = \{g \in G : \mathrm{tr} g = 1 + \det g\}.$$

Clearly, every conjugacy class in D intersects H non-trivially. Hence σ_p is not contained in D, or in other words $\sigma_p \cap D = \phi$. Thus

$$a(p) \not\equiv 1 + p (\mathrm{mod}\, \ell)$$

and this means that

$$|E(\mathbb{F}_p)| = p + 1 - a(p) \not\equiv 0 (\mathrm{mod}\, \ell).$$

(**ii**): We may suppose (after a suitable choice of basis) that $G \subseteq B$ (with B as above).

We are again looking for a prime p such that $\sigma_p \cap H = \phi$ where

$$H = G \cap \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\}.$$

If $G = H$, then it is clear that ℓ divides T and this is excluded by assumption. Thus, we may suppose that $G \neq H$.

Since H is a normal subgroup of G, it follows from Theorem 9.1 that there exists a prime p with the desired property and

$$p \ll \Big(\frac{1}{[G:H]} \log d_F\Big)^2$$

where F is the fixed field of H. Since F is a Galois extension of $\mathbb{Q}$ ramified only at primes dividing $\ell\mathcal{N}$, we have

$$p \ll (\log \ell\mathcal{N})^2.$$

(**iii**): This is impossible if $\ell > 2$ since G contains the image of complex conjugation, a matrix with distinct $\mathbb{F}_\ell$-rational eigenvalues (namely $+1$, -1), whereas the eigenvalues of every element of a nonsplit Cartan subgroup are either equal or lie in $\mathbb{F}_{\ell^2} \backslash \mathbb{F}_\ell$.

(**iv**): In this case $|G| \ll \ell$. By the result of Lagarias and Odlyzko , quoted as (9.1) at the beginning of this section, there exists a prime p whose σ_p is $\left\{\begin{pmatrix} 2 & \\ & 2 \end{pmatrix}\right\}$ (say) and

$$p < (|G| \log \ell\mathcal{N})^2 \ll (\ell \log \ell\mathcal{N})^2.$$

Such a prime has

$$a(p) \equiv 4 \not\equiv 1 + 4 \equiv 1 + p \pmod{\ell}.$$

(**v**): In this case, there is a quadratic character ϵ with the property that

$$p \nmid \mathcal{N} \text{ and } \epsilon(p) = -1 \Rightarrow a(p) \equiv 0 (\operatorname{mod} \ell).$$

Let K be the quadratic extension of $\mathbb{Q}$ corresponding to ϵ. This field has the property [Se2, p. 198] that it is unramified at ℓ and can only ramify at primes dividing $\mathcal{N}$. Hence, we can find a prime p such that $p \equiv 1 (\operatorname{mod} \ell)$ and $\epsilon(p) = -1$ with

$$p \ll (\log |d_{K(\zeta_\ell)}|)^2 \ll (\ell \log \ell\mathcal{N})^2$$

where ζ_ℓ is a primitive ℓ-th root of unity. For such a prime, $a(p) \equiv 0 \not\equiv 2 \equiv 1 + p (\operatorname{mod} \ell)$. This proves the theorem.

Exercises

1. Let χ be an irreducible character of a finite group G. If χ is a linear combination with positive real coefficients of monomial characters, then $m\chi$ is monomial for some integer $m \geq 1$.

2. Let A be a normal subgroup of the group G and let χ be an irreducible character of G. Then either the restriction of χ to A is isotypic (that is, a multiple of one character) or there is a subgroup H containing A and an irreducible character σ of H such that $\chi = \operatorname{Ind}_H^G \sigma$. (See [Se1, Prop. 24]).

3. A finite group G is called *supersolvable* if there is a sequence of subgroups

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots G_n = G$$

with each G_i normal in G and with successive quotients G_i/G_{i-1} cyclic.

(a) Prove that a nonabelian supersolvable group has a normal abelian subgroup which is not contained in the center.

(b) Use (a) and Exercise 2 to prove that an irreducible character of a supersolvable group is monomial (that is, the induction of a one-dimensional character of some subgroup).

Exercises 4–7 are based on the paper [R] of Rhoades.

4. Let $\mathcal{F}$ be a set of characters of the finite group G. We say that a class function θ is *semi-orthogonal* to $\mathcal{F}$ if $(\theta, \phi) \geq 0$ for all $\phi \in \mathcal{F}$.
   (a) If $\mathcal{F}$ is the set of all characters of G, then a generalized character θ is semi-orthogonal to $\mathcal{F}$ if and only if θ is a character.
   (b) Let
   $$\tilde{\mathcal{F}} = \{\sum x_\phi \phi : 0 < x_\phi \in \mathbb{R}, \phi \in \mathcal{F}\}.$$
   Then a class function θ is semi-orthogonal to $\mathcal{F}$ if and only if it is semi-orthogonal to $\tilde{\mathcal{F}}$.

5. If
   $$\mathcal{F} = \{\mathrm{Ind}_H^G \psi : H \text{ an Abelian subgroup of } G\}$$
   then
   (a) the generalized character θ_G is semi-orthogonal to $\mathcal{F}$.
   (b) if a generalized character $\theta = \sum m_\chi \chi$ is semi-orthogonal to $\mathcal{F}$ then $|m_\chi| \leq |\theta(1)|$.

6. Let F be a subset of $\mathbb{R}^k$ and define
   $$\mathcal{H}(F) = \{x \in \mathbb{R}^k : (f, x) \geq 0 \text{ for all } f \in F\}$$
   and
   $$\mathcal{C}(F) = \{\sum x_i f_i : 0 < x_i \in \mathbb{R}, f_i \in F\}$$
   where (,) denotes the standard inner product.
   (a) If F is a subspace, then $\mathcal{H}(F)$ is the subspace of $\mathbb{R}^k$ orthogonal to F and $\mathcal{H}(\mathcal{H}(F)) = F$ and $\mathcal{C}(F) \subset F$.
   *(b) [R, Lemma 1] If F does not contain the zero vector and all elements of F have non-negative coordinates, then $\mathcal{H}(\mathcal{H}(F)) = \mathcal{C}(F)$.

7. Let G be a finite group and $\mathcal{F}$ a subset of characters of G. Expressing the elements of $\mathcal{F}$ as a sum of irreducible characters of G, identify $\mathcal{F}$ as a subset of $\mathbb{R}^k$ for some k. Using Exercise 6(b), show that a generalized character ψ of G can be written as a positive rational linear combination of characters in $\mathcal{F}$ if and only if $(\psi, \theta) \geq 0$ for all θ semi-orthogonal to $\mathcal{F}$. Deduce that for any irreducible character χ of G, $\mathrm{reg}_G \pm \chi$ can be written as a positive rational linear combination of monomial characters.

8. Let L/K be a finite Galois extension with group G. Show that the Artin L-functions $L(s, \chi, K)$ (as χ ranges over the irreducible characters of G) are multiplicatively independent over $\mathbb{Q}$. That is, if
   $$\prod_\chi L(s, \chi, K)^{c_\chi} = 1$$
   for some rational numbers c_χ then $c_\chi = 0$ for all χ.

9. Let $F/\mathbb{Q}$ be a finite Galois extension with group G and let H, H' be two subgroups. Denote by K and K' the corresponding fixed fields.
   (a) Show that $\zeta_K(s) = \zeta_{K'}(s)$ if and only if for every conjugacy class C of G, we have $\#(H \cap C) = \#(H' \cap C)$.
   (b) Let $G = S_6$ (the symmetric group on 6 letters) and consider the subgroups
   $$H = \{(1), (12)(34), (12)(56), (34)(56)\}$$
   and
   $$H' = \{(1), (12)(34), (13)(24), (14)(23)\}.$$
   Prove that the above condition is satisfied and deduce that the Dedekind zeta functions of the corresponding fixed fields coincide. (This is due to Gassman, 1926.)

10. Let $1 < a \in \mathbb{Z}$ be a squarefree integer and q a prime. Set $K = \mathbb{Q}(a^{1/q})$ and prove directly that $\zeta_K(s)/\zeta(s)$ is entire.

11. Let $f(T) \in \mathbb{Z}[T]$ be an irreducible polynomial of degree larger than 1. Show that the set
$$\{p : f(T) \equiv 0 (\operatorname{mod} p) \text{ has a solution}\}$$
has positive density.

12. Let E be a biquadratic extension of $\mathbb{Q}$ and let K_1, K_2, K_3 be the three quadratic subfields. Show that
$$\zeta(s)^2 \zeta_E(s) = \zeta_{K_1}(s)\zeta_{K_2}(s)\zeta_{K_3}(s).$$
Deduce a relation amongst the class numbers of the K_i.

References

[CF] J. Cassels and A. Fröhlich, Algebraic Number Theory, Academic Press, 1967.

[D] H. Davenport, Multiplicative Number Theory, Springer-Verlag, 1980.

[Fo] R. Foote, Non-monomial characters and Artin's conjecture, *Trans. Amer. Math. Soc.*, **321** (1990), 261–272.

[FM] R. Foote and V. Kumar Murty, Zeros and poles of Artin L-series, *Math. Proc. Camb. Phil. Soc.*, **105** (1989), 5–11.

[FW] R. Foote and D. Wales, Zeros of order 2 of Dedekind zeta functions and Artin's conjecture, *J. Algebra*, **131** (1990), 226–257.

[Fr] A. Fröhlich, Galois Module Structure of algebraic integers, Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, 1983.

[K] N. Katz, Galois properties of torsion points of abelian varieties, *Invent. Math.*, **62** (1981), 481–502.

[La] S. Lang, Algebraic Number Theory, Springer-Verlag, 1986.

[LO] J. Lagarias and A. M. Odlyzko, Effective versions of the Chebotarev Density Theorem, *Algebraic Number Fields*, ed. A. Fröhlich, 409–464, Academic Press, New York, 1977.

[LMO] J. Lagarias, H. Montgomery and A. M. Odlyzko, A bound for the least prime ideal in the Chebotarev Density Theorem, *Invent. Math.*, **54** (1979), 271–296.

[Mu1] V. Kumar Murty, Holomorphy of Artin L-functions, in: Proc. Ramanujan Centennial Conference, pp. 55–66, Ramanujan Mathematical Society, Chidambaram, 1987.

[Mu2] V. Kumar Murty, Explicit formulae and the Lang-Trotter conjecture, *Rocky Mountain J. Math.*, **15** (1985), 535–551.

[Mu3] V. Kumar Murty, The least prime which does not split completely, *Forum Math.*, **6** (1994), 555–565.

[MM] M. Ram Murty and V. Kumar Murty, Base change and the Birch and Swinnerton-Dyer conjecture, in: A tribute to Emil Grosswald: number theory and analysis, *Contemp. Math.*, **143** (1993), 481–494.

[MMS] M. Ram Murty, V. Kumar Murty and N. Saradha, Modular forms and the Chebotarev Density Theorem, *Amer. J. Math.*, **110** (1988), 253–281.

[MS] V. Kumar Murty and J. Scherk, Effective versions of the Chebotarev Density Theorem in the function field case, *C.R. Acad. Sci. Paris*, **319** (1994), 523–528.

[R] S. Rhoades, A generalization of the Aramata-Brauer theorem, *Proc. Amer. Math. Soc.*, **119** (1993), 357–364.

[Se1] J.-P. Serre, Linear representations of finite groups, Springer-Verlag, New York, 1977.

[Se2] J.-P. Serre, Quelques applications du Théorème de Densité de Chebotarev, *Publ. Math. IHES*, **54** (1981), 123–201.

[St] H. M. Stark, Some effective cases of the Brauer-Siegel theorem, *Invent. Math.*, **23** (1974), 135–152.

[Uc] K. Uchida, On Artin L-functions, *Tohoku Math. J.*, **27** (1975), 75–81.

[vdW] R. W. van der Waall, On a conjecture of Dedekind on zeta functions, *Indag. Math.*, **37** (1975), 83–86.

http://www.springer.com/978-3-0348-0273-4

Non-vanishing of L-Functions and Applications
Murty, M.R.; Murty, V.K.
1997, XI, 196 p. 1 illus., Softcover
ISBN: 978-3-0348-0273-4
A product of Birkhäuser Basel