J. Fac. Sci. Univ. Tokyo
Sect. IA, Math.
35 (1988), 177-197.

On the values of abelian L-functions at s=0

By Benedict H. GROSS

"En m'occupant ⋯ à prouver que toute progression arithmétique indéfinie ⋯ renferme une infinité de nombres premiers⋯, j'ai été conduit à envisager un grand nombre de questions relatives aux nombres, sous un point de vue entièrement nouveau, et qui les rattache aux principes de l'analyse infinitésimale et aux propriétés remarquables d'une classe de séries et de produits infinis qui ont beaucoup d'analogie avec les expressions que l'illustre EULER a considérées⋯". So begins Dirichlet's great memoire [4] on the zeta functions of quadratic fields. Dedekind generalized the arithmetic formula for the residue at $s=1$ to the zeta function of an arbitrary number field:

$$\lim_{s\to 1}(s-1)\zeta(s)=\frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|d|}}\cdot\frac{hR}{w}$$

in his eleventh supplement to Dirichlet's lectures [2, § 183-184]. Combining this formula with the functional equation relating $\zeta(s)$ to $\zeta(1-s)$, one obtains the first term in the Taylor expansion at $s=0$:

$$\zeta(s)\equiv -\frac{hR}{w}\cdot s^{r_1+r_2-1} \pmod{s^{r_1+r_2}}. \tag{0.1}$$

In this paper I will present a conjecture, which bears an interesting resemblance to (0.1), relating the values of abelian L-series at $s=0$ to a simple generalization of the unit regulator. This conjecture, which both generalizes and simplifies a conjecture I made on p-adic L-series at $s=0$ [5], was suggested by the recent work of Barry Mazur and John Tate [7] on the arithmetic of modular curves. Its precise formulation was suggested by the work of David Hayes [6] in the function field case. I would like to thank all of them for their help.

The contents of this paper are as follows. In § 1 we review the class-number formula (0.1) for zeta-functions, and in § 2 we present a generalization of the regulator. In § 3 we review the results known on the integrality of partial zeta functions at $s=0$, and in § 4 state our conjecture. In § 5 we give a proof in the archimedean case, using the 2-adic congruences of Deligne and Ribet [3], and in § 6 we prove the conjecture (up to a unit) when the abelian extension in question is cyclic of prime order. The last two sections are devoted to various generalizations: in § 6 we discuss a refinement of Stark's conjecture for the first derivative [11], and in § 7 we discuss the L-functions of quadratic characters.

It is a pleasure to thank the Japan Society for the Promotion of Science, and my host scientist Y. Ihara, for giving me the opportunity to visit the University of Tokyo, where this paper was written.

§ 1. The class-number formula (cf. [12, ch.1]).

Let k be a global field, and let S be a finite set of places of k which is non-empty and contains all archimedean places. Since S is fixed we will usually drop it from our notation. Let A denote the S-integers of k and let $U=A^*$ be the group of S-units. The class group $\mathrm{Pic}(A)$ is finite of order h, and the unit group U is finitely generated of rank $n=\#S-1$. The torsion subgroup of U is equal to the group of roots of unity μ in k^*; it is cyclic of order w.

Let Y be the free abelian group generated by the places $v\in S$ and $X=\{\sum a_v\cdot v\colon \sum a_v=0\}$ the subgroup of elements of degree zero in Y. The S-regulator R is defined as the absolute value of the determinant of the map

$$(1.1)\qquad \begin{aligned} \lambda_{\boldsymbol{R}}\colon U &\longrightarrow \boldsymbol{R}\otimes X \\ \varepsilon &\longmapsto \sum_S \log\|\varepsilon\|_v\cdot v, \end{aligned}$$

taken with respect to $\boldsymbol{Z}$-bases of the free abelian groups U/μ and X.

The zeta-function of A is given by

$$(1.2)\qquad \zeta(s)=\sum_{\mathfrak{A}\subseteq A} N\mathfrak{A}^{-s}=\prod_{\mathfrak{p}\notin S}\frac{1}{1-N\mathfrak{p}^{-s}}$$

in the half-plane $\mathrm{Re}(s)>1$. It has a meromorphic continuation to the s-plane, with a simple pole at $s=1$ and no other singularities. At $s=0$ the Taylor expansion begins:

$$(1.3)\qquad \zeta(s)\equiv\frac{-hR}{w}\cdot s^n \pmod{s^{n+1}}.$$

The presence of w in the denominator of (1.3) reflects the fact that the group U is not free. To achieve an integral formula, we let T be a finite set of places of k which is disjoint from S, and define

$$\zeta_T(s) = \prod_{\mathfrak{p} \in T} (1 - N\mathfrak{p}^{1-s}) \cdot \zeta(s). \tag{1.4}$$

Let U_T denote the subgroup of units which are $\equiv 1 \pmod{T}$ and let $\mathrm{Pic}(A)_T$ be the group of invertible A-modules together with a trivialization at T. We have an exact sequence

$$1 \longrightarrow U_T \longrightarrow U \longrightarrow \prod_{\mathfrak{p} \in T} F_{\mathfrak{p}}^* \longrightarrow \mathrm{Pic}(A)_T \longrightarrow \mathrm{Pic}(A) \longrightarrow 1. \tag{1.5}$$

Letting h_T be the order of $\mathrm{Pic}(A)_T$, R_T the determinant of λ with respect to bases of U_T/μ_T and X, and w_T the order of the roots of unity μ_T which are $\equiv 1 \pmod{T}$, we find

$$\zeta_T(s) \equiv \frac{-h_T R_T}{w_T} \cdot s^n \pmod{s^{n+1}}. \tag{1.6}$$

We shall henceforth assume that T is non-empty; then $\zeta_T(s)$ is entire and, in the function field case, $w_T = 1$. In the number field case we will assume that T either contains primes of different residue characteristics, or contains a prime $\mathfrak{p}$ whose absolute ramification index $e_{\mathfrak{p}}$ is strictly less than $(p-1)$, where p is the characteristic of $\boldsymbol{F}_{\mathfrak{p}}$. Then $w_T = 1$ for any abelian extension of k which is unramified outside S. In particular, U_T is a free abelian group.

Let $\langle \varepsilon_1, \cdots, \varepsilon_n \rangle$ and $\langle x_1, \cdots, x_n \rangle$ be $\boldsymbol{Z}$-bases of U_T and X respectively, and let $\det_R \lambda$ be the determinant of the matrix for λ_R with respect to these bases. By (1.6) we have

$$\zeta_T(s) \equiv m \cdot \det_R(\lambda) \cdot s^n \pmod{s^{n+1}} \tag{1.7}$$

where $m = \pm h_T$ is a non-zero integer (whose sign depends on the orientations of the bases chosen).

§ 2. The regulator.

Let $\boldsymbol{A}$ denote the ring of adèles of k. Let G be a locally compact abelian group and $f\colon \boldsymbol{A}^* \to G$ a continuous homomorphism whose kernel contains the subgroup $k^* \cdot \prod_{\mathfrak{p} \notin S} A_{\mathfrak{p}}^*$. For $\mathfrak{p} \notin S$ we let $g(\mathfrak{p})$ be the image $f(1, 1, \cdots, \pi_{\mathfrak{p}}, \cdots, 1)$, where $\pi_{\mathfrak{p}}$ is a uniformizing parameter in $k_{\mathfrak{p}}$.

Let λ_G be the homomorphism

$$\text{(2.1)} \qquad \begin{aligned} \lambda_G\colon U &\longrightarrow G\otimes X \\ \varepsilon &\longmapsto \sum_S f(1, 1, \cdots, \varepsilon_v, \cdots, 1)\cdot v. \end{aligned}$$

If $G=\boldsymbol{R}$ and $f=\log\|\ \ \|$, we obtain the homomorphism $\lambda_{\boldsymbol{R}}$ of § 1. Using the bases $\langle\varepsilon_1, \cdots, \varepsilon_n\rangle$ and $\langle x_1, \cdots, x_n\rangle$ chosen above for U_T and X, we obtain an $n\times n$ matrix $((g_{ij}))$ for λ_G with entries in G, and we would like to define its determinant (whose sign will depend on the orientations chosen).

Let $\boldsymbol{Z}[G]$ be the integral group ring of G and $I=\{\sum_G m(g)g\colon \sum m(g)=0\}$ be the augmentation ideal. Then the map $g\mapsto g-1$ gives an isomorphism $G\xrightarrow{\sim} I/I^2$ of abelian groups. We may therefore consider our matrix for λ_G as having entries $\eta_{ij}=g_{ij}-1$ in I/I^2. We define

$$\text{(2.2)} \qquad \begin{aligned} \det_G\lambda &= \sum_{\sigma\in\mathrm{Sym}(n)} \mathrm{sign}(\sigma)\eta_{1\sigma(1)}\eta_{2\sigma(2)}\cdots\eta_{n\sigma(n)} \\ &\in I^n/I^{n+1}. \end{aligned}$$

When $n=0$ we have $\det_G\lambda=1$ in $\boldsymbol{Z}[G]/I\cong\boldsymbol{Z}$.

§ 3. The L-function.

Consider the formal product

$$\text{(3.1)} \qquad F_G=\prod_{\mathfrak{p}\in T}(1-g(\mathfrak{p})N\mathfrak{p})\prod_{\mathfrak{p}\notin S}(1-g(\mathfrak{p}))^{-1}.$$

We view this as a function (complex-valued) on the complex quasi-characters of G by setting $F_G(\chi)=L_T(\chi)$, the value of the Hecke-Tate L-function of χ (relative to S, and modified at T) considered as a quasi-character of $\boldsymbol{A}^*/k^*$. When $\mathrm{Re}(\chi)>1$ we have:

$$\text{(3.2)} \qquad F_G(\chi)=\prod_{\mathfrak{p}\in T}(1-\chi(\mathfrak{p})N\mathfrak{p})\prod_{\mathfrak{p}\notin S}(1-\chi(\mathfrak{p}))^{-1}.$$

If $G=\boldsymbol{R}_+^*$ and $\chi=\|\ \ \|^s$, we have $F_G(\chi)=\zeta_T(s)$ by (1.4).

Restricting F_G to the characters of G gives a complex valued function on the dual group $\hat{G}$. We henceforth assume that G is *finite*, and (for simplicity) that the map $f\colon \boldsymbol{A}^\times\to G$ is surjective. Then $F_G(\chi)$ is the value, at $s=0$, of the abelian L-function $L_T(\chi, s)$. Let $\hat{F}$ be the Fourier transform of F_G, with respect to the Haar measure of volume 1 on $\hat{G}$, and define

(3.3) $$\theta_G=\sum_G \hat{F}(g)[g] \quad \text{in} \quad \boldsymbol{C}[G].$$

By Fourier inversion, θ_G is the unique element of $\boldsymbol{C}[G]$ such that

(3.4) $$\theta_G(\chi)=\sum_G \hat{F}(g)\chi(g)=L_T(\chi, 0)$$

for all characters χ.

When k is a function field with field of constants $\boldsymbol{F}_q$, the results of Weil (cf. [12, ch. V]) show that the product:

(3.5) $$\theta(s)=\prod_{\mathfrak{p}\in T}(1-g(\mathfrak{p})\boldsymbol{N}\mathfrak{p}^{1-s})\prod_{\mathfrak{p}\notin S}(1-g(\mathfrak{p})\boldsymbol{N}\mathfrak{p}^{-s})^{-1}$$

is a polynomial in q^{-s} with coefficients in $\boldsymbol{Z}[G]$. Hence $\theta_G=\theta(0)$ is an element of $\boldsymbol{Z}[G]$. We will now show that our hypotheses on T force $\theta_G\in\boldsymbol{Z}[G]$ in general. Indeed, when $T=\{\mathfrak{p}\}$ consists of a single place, the coefficient of $g'=g\cdot g(\mathfrak{p})$ in θ_G is equal to

(3.6) $$\zeta(g', 0)-\boldsymbol{N}\mathfrak{p}\cdot\zeta(g, 0).$$

Here $\zeta(g, s)$ is the partial zeta function relative to the set S. Results of Siegel [10] show that $\zeta(g, 0)$ is rational for all $g\in G$, and the combinations in (3.6) were shown to be integral, except perhaps at the characteristic p of $\mathfrak{p}$, by Deligne-Ribet [3] and Cassou-Noguès [1]. To see that they are integral at p, we observe that $W\zeta(g, 0)$ is integral for any integer W annihilating the roots of unity in the classfield L of k corresponding to G [12, ch. IV, §1]. Since L/k is unramified outside S, the order of $\mu(L)$ is prime to p (by our hypothesis that $e_{\mathfrak{p}}<(p-1)$). This shows θ_G is integral when $T=\{\mathfrak{p}\}$. If T contains two places of unequal residue characteristics p and q, then θ_G lies in $\boldsymbol{Z}[1/p][G]$, but also in $\boldsymbol{Z}[1/q][G]$. Hence we have established

PROPOSITION 3.7. *Assume G is finite, and let θ_G be the unique element of $\boldsymbol{C}[G]$ such that $\theta_G(\chi)=L_T(\chi, 0)$ for all characters $\chi\in\hat{G}$. Then θ_G lies in the integral group ring $\boldsymbol{Z}[G]$.*

§ 4. The conjecture.

We now present a conjectural refinement of the class number formula, as a congruence for θ_G in $\boldsymbol{Z}[G]$. Recall that $I\subset\boldsymbol{Z}[G]$ is the augmentation ideal.

CONJECTURE 4.1. *Assume G is finite, and define θ_G in $\boldsymbol{Z}[G]$ by (3.7). Let m be the non-zero integer defined by (1.7) and $\det_G \lambda$ the element of I^n/I^{n+1} defined by (2.2). Then*

$$\theta_G \equiv m \cdot \det_G \lambda \quad (mod\ I^{n+1}).$$

In particular, Conjecture 4.1 implies the weaker congruence

$$\theta_G \equiv 0 \quad (\text{mod } I^n). \tag{4.2?}$$

Note that the definition of m and $\det_G \lambda$ require the choice of bases for U_T and X. However a change of bases either leaves both m and $\det_G \lambda$ fixed, or takes $m \mapsto -m$ and $\det_G \lambda \mapsto -\det_G \lambda$. Hence conjecture 4.1 is independent of the bases chosen.

If $n=0$ then $\det_R \lambda = 1$ and hence $m = \zeta_T(0)$. Since $\det_G \lambda = 1$ and

$$\theta_G \equiv \sum_G \hat{F}(g) = \zeta_T(0) \quad (\text{mod } I) \tag{4.3}$$

we see that Conjecture 4.1 is true. We will henceforth assume that $n \geqq 1$, which implies by (4.3) that $\theta_G \equiv 0$ (mod I).

If $S' = S \cup \{\mathfrak{p}\}$, then $\theta'_G = (1 - g(\mathfrak{p}))\theta_G$ and $m' \cdot \det_G \lambda' \equiv (1 - g(\mathfrak{p})) \cdot m \cdot \det_G \lambda$ (mod I^{n+2}). Hence if Conjecture 4.1 holds for G and S, it holds for G and any set S' containing S. Similarly, if $T' = T \cup \{\mathfrak{p}\}$ then $\theta'_G = (1 - g(\mathfrak{p})N\mathfrak{p})\theta_G$; if $\theta_G \equiv 0$ (mod I^n) we have $\theta'_G \equiv (1 - N\mathfrak{p})\theta_G$ (mod I^{n+1}). Since $m' \cdot \det_G \lambda' = (1 - N\mathfrak{p}) \cdot m \cdot \det_G \lambda$, if Conjecture 4.1 holds for the set T, it holds for any set T' containing T.

Finally, suppose $G = \varprojlim G/H$ is a profinite abelian group and $f: A^*/k^* \prod_{v \notin S} A_v^\times \to G$ has dense image. We may define $\theta_{G/H} \in \boldsymbol{Z}[G/H]$ for each finite quotient via (3.7), and the limit

$$\underline{\theta}_G = \varprojlim \theta_{G/H} \tag{4.4}$$

exists in the ring $\boldsymbol{Z}[[G]] = \varprojlim \boldsymbol{Z}[G/H]$ of integral measures on G. Let $\underline{I}$ be the ideal of measures of volume zero. Since $\underline{I}/\underline{I}^2 = \varprojlim (I_{G/H}/I^2_{G/H}) \cong \varprojlim G/H = G$, we may define $\underline{\det}_G \lambda$ in $\underline{I}^n/\underline{I}^{n+1}$ as in (2.2). Conjecture 4.1 then predicts that

$$\underline{\theta}_G \equiv m \cdot \underline{\det}_G \lambda \quad (\text{mod } \underline{I}^{n+1}). \tag{4.5?}$$

Taking G to be the Galois group of the maximal abelian extension of k which is unramified outside S and f the reciprocity map of global class field theory, we obtain one conjecture which implies all the others. Note however that the results of class field theory, are *not* necessary for the statement of conjecture 4.1.

§ 5. Archimedean considerations.

In this § we will consider Conjecture 4.1 in the case when k is a number field. Using the 2-adic congruences of Deligne and Ribet [3, § 8] and [9, § 3] we will prove the conjecture in the special case when S contains *only* the archimedean places of k. In this case, we will assume that G is the quotient of $A^*/k^* \prod_{v \notin S} A_v^*$ by its connected component, which is a finite group, isomorphic to the strict class group of A. For other S, we will let G be any finite quotient of $A^*/k^* \prod_{v \notin S} A_v^*$. We will also assume throughout that $n \geqq 1$, that $n \geqq 1$, and that the primes in T have odd residual characteristic.

If k has a complex place v, then the idèle $(1, \cdots, \varepsilon_v, \cdots, 1)$ has trivial image in G for any $\varepsilon \in U$. Hence the v^{th} row of the matrix of λ is zero, and $\det_G \lambda \equiv 0 \pmod{I^{n+1}}$. But we also have $\theta_G = 0$ in $\boldsymbol{Z}[G]$: the pole of the local L-factor $(2\pi)^{-s}\Gamma(s)$ at $s=0$ forces the function $L_T(\chi, s)$ to vanish at $s=0$ for all $\chi \in \hat{G}$. Hence Conjecture 4.1 is true (both sides are zero).

We henceforth assume that k is totally real, and let Σ denote the set of real places of k. For $v \in \Sigma$ we let g_v be the image of the idèle $(1, \cdots, -1_v, \cdots, 1)$ in G. If $g_v = 1$ for any $v \in \Sigma$, the argument in the previous paragraph shows that $\det_G \lambda \equiv 0 \pmod{I^{n+1}}$ and $\theta_G = 0$ in $\boldsymbol{Z}[G]$. In any case, $2 \cdot \det_G \lambda \equiv 0 \pmod{I^{n+1}}$, as the row corresponding to any $v \in \Sigma$ is killed by 2. Hence only the parity of m is relevant in Conjecture 4.1, and the determination of its sign is not necessary.

Since $L_T(\chi) = 0$ unless $\chi(g_v) \neq 1$ for all $v \in \Sigma$, we find that the Fourier transform $\hat{F}$ satisfies

$$\hat{F}(g) + \hat{F}(gg_v) = 0 \tag{5.1}$$

for all $g \in G$, $v \in \Sigma$. Hence θ_G is divisible by $(1-g_v)$ in $\boldsymbol{Z}[G]$, for each place $v \in \Sigma$. The more difficult question of whether θ_G is divisible by the product $\prod_{\Sigma}(1-g_v)$ was addressed by Deligne and Ribet. To translate into their language, we need an algebraic lemma.

Let G be a finite abelian group, and let $g_1, \cdots, g_r$ be elements of G satisfying $g_i^2 = 1$. Let H be the subgroup generated by the elements g_i and let H' be the subgroup generated by the products $g_i g_j$. Then

H has order 2^s with $0 \leqq s \leqq r$ and H' has index 1 or 2 in H.

We say a function $f: G \to \boldsymbol{Z}$ is odd iff

$$f(g)+f(gg_i)=0 \tag{5.2}$$

for all $g \in G$ and $i=1, 2, \cdots, r$. When $H=H'$ any odd function is equal to 0. When $H \neq H'$ we may prescribe an odd function f by its values on a set T of coset representatives for H, and these values may be arbitrary. The algebraic result we need is the following.

LEMMA 5.3. *The element* $\theta=\sum F(g)[g]$ *of* $\boldsymbol{Z}[G]$ *is divisible by* $\prod_{i=1}^r(1-g_i)$ *if and only if*

a) F *is an odd function on* G

b) *For all odd functions* f *on* G *we have* $\sum_G F(g)f(g) \equiv 0 \pmod{2^r}$.

PROOF. If $\theta=\prod_{i=1}^r(1-g_i)\cdot\eta$, one checks immediately that conditions a) and b) are satisfied using induction on r. To prove the converse, we may assume $H \neq H'$, for otherwise a) implies $F=0$. Since f odd implies that $f\cdot F$ is even, we have

$$\sum_G F(g)f(g)=2^s\cdot\sum_T F(g)f(g)$$

where $2^s=|H|$ and T is a set of coset representatives for H. Since f may be specified arbitrarily on T, taking the characteristic function of each element shows that

$$F(g) \equiv 0 \pmod{2^{r-s}}$$

for all $g \in T$. The element $\eta=(1/2^{r-s})\sum_T F(g)[g]$ then lies in $\boldsymbol{Z}[G]$ and

$$\theta=\prod_{i=1}^r(1-g_i)\cdot\eta.$$

PROPOSITION 5.4 (Deligne-Ribet). *The element* θ_G *is divisible by* $\prod_\Sigma(1-g_v)$ *in* $\boldsymbol{Z}[G]$, *except in the special case to be described below.*

Indeed, [9, (3.1)] shows that the conditions a) and b) of Lemma 5.3 hold (with $g_i=g_v$ and $r=\#\Sigma$), except when

$$\begin{cases} S=\Sigma. \\ \text{All units } \varepsilon \in U \text{ satisfy } N\varepsilon=+1. \\ \text{The extension } L \text{ obtained by taking the square-roots of all} \\ \quad \text{totally positive units in } U \text{ has degree 2 over } k. \\ T=\{\mathfrak{p}\} \text{ with } \mathfrak{p} \text{ inert in } L/k. \end{cases} \tag{5.5}$$

This will be referred to as the special case. Together the second and third hypotheses imply that k has units of all possible real signatures satisfying $N\varepsilon=+1$. Hence all g_v are equal to a single non-trivial involution τ in G.

In the special case, Deligne and Ribet show that θ_G is divisible by $(1-\tau)^n$, but not by $\prod_\Sigma(1-g_v)=(1-\tau)^{n+1}$. In fact,

PROPOSITION 5.6. *In the special case,* $\theta_G\equiv h(1-\tau)^n \pmod{I^{n+1}}$, *where* $h=\#\,\mathrm{Pic}(A)$.

PROOF. Let $\theta_G=\sum F(g)[g]$. The subgroup $H=\langle\tau\rangle$ of Lemma 5.3 has order 2 and index $h=\#T$. The "negative congruence" of [9, (3.2)] states that for odd f

$$\begin{cases}\sum_G F(g)f(g)=2^n\cdot\alpha_f, & \text{with}\\ \alpha_f\equiv\sum_T f(g) \pmod 2. & \end{cases}$$

Taking f to be the characteristic function of an element of T, oddly extended to G, we find that $\mathrm{ord}_2 F(g)=n-1$ for all $g\in G$. The element

$$\eta=\frac{1}{2^{n-1}}\sum_T F(g)[g]=\sum_T m(g)[g]$$

in Lemma 5.3 has odd coefficients $m(g)$, so

$$\eta\equiv\sum_T m(g)\equiv h \quad \mathrm{mod}(I,\,2).$$

Hence

$$\begin{aligned}\theta_G&=(1-\tau)^n\eta\\ &\equiv h(1-\tau)^n \pmod{I^{n+1}}.\end{aligned}$$

We end this analysis of θ_G by giving an example, in the special case, when $\theta_G\not\equiv 0 \pmod{I^{n+1}}$. Take $k=\boldsymbol{Q}(\sqrt{12})$ and $S=\Sigma$. Then $n=1$ and $h=1$; the group $G=\langle 1,\tau\rangle$ has order 2 and is the Galois group of the classfield $k(\mu_{12})$. The field L is equal to $k(\sqrt{2})$. Let $T=\{\mathfrak{p}\}$ where $\mathfrak{p}$ is a prime of degree one in k with $N\mathfrak{p}\equiv 11$ or $13 \pmod{24}$. Then $\theta_G=(1/12)(1-g(\mathfrak{p})N\mathfrak{p})(1-\tau)\equiv(1-\tau) \pmod{I^2}$.

We now turn to the calculation of $m\cdot\det_G\lambda$ when $S=\Sigma$ and $n\geqq 1$. In this case, $m=\pm h_T=\pm h\cdot c_T$ where

$$c_T=\#\,\mathrm{coker}\Big(U\longrightarrow\prod_{\mathfrak{p}\in T}\boldsymbol{F}_{\mathfrak{p}}^*\Big). \tag{5.7}$$

PROPOSITION 5.8. $c_T \cdot \det_G \lambda \equiv 0 \pmod{I^{n+1}}$ *except in the special case, when*

$$c_T \det_G \lambda \equiv (1-\tau)^n \pmod{I^{n+1}}.$$

PROOF. Each unit ε gives a relation on the elements $g_v \in G$: $\prod_{\varepsilon_v<0} g_v = 1$. If units exist with all possible signs, then $g_v=1$ for all v and $\det_G \lambda \equiv 0 \pmod{I^{n+1}}$.

Assume that there is a relation $\sum a_v[v]$ on the signs of global units, with $a_v \in \boldsymbol{Z}/2$ and not all $a_v=0$. To exclude the special case, we assume that not all $a_v=1$. We view this relation as a homomorphism $X \to \boldsymbol{Z}/2$ taking $\sum b_v[v]$ to $\sum a_v b_v$. By our assumptions, this homomorphism is surjective. Let $X' \subseteq X$ be its kernel, and choose a basis $x_1, \cdots, x_n$ of X such that X' is spanned by $2x_1, x_2, \cdots, x_n$.

Let H be the subgroup, of exponent 2, in G generated by the g_v for $v \in \Sigma$. The map λ_G gives a homomorphism $\lambda: U \to X \otimes H$, whose image, by our hypothesis, is contained in $X' \otimes H$. Hence the matrix of λ on U_T has first row divisible by 2. Since H has exponent 2, the first row is zero and $\det_G \lambda \equiv 0 \pmod{I^{n+1}}$.

We are therefore reduced to the case where the single relation on the signs of units in k is given by $N\varepsilon = +1$. Let $\tilde{U}$ be the subgroup of $\prod_T F_\mathfrak{p}^*$ generated by the image of U, and let $\tilde{U}^+$ be the subgroup generated by the images of totally positive units. Then U_T has units of all signs, with the single restriction that $N\varepsilon = +1$, precisely when the index of $\tilde{U}^+$ in $\tilde{U}$ is odd. In this case, $\det_G \lambda \equiv (1-\tau)^n \pmod{I^{n+1}}$; otherwise $\det_G \lambda \equiv 0 \pmod{I^{n+1}}$ by the argument above. Since c_T is the index of $\tilde{U}$ in $\prod_T F_\mathfrak{p}^*$, and $2(1-\tau) = (1-\tau)^2$ we see that $c_T \cdot \det_G \lambda \equiv 0 \pmod{I^{n+1}}$ unless the index of $\tilde{U}^+$ in $\prod_T F_\mathfrak{p}^*$ is odd, in which case $c_T \cdot \det_G \lambda \equiv (1-\tau)^n \pmod{I^{n+1}}$. Since U^+/U^2 has order 2, the index of $\tilde{U}^+$ is odd only when $T = \{\mathfrak{p}\}$ and $\mathfrak{p}$ is inert in $k(\sqrt{U^+})$. Since this is exactly the special case (5.5), we are done.

Combining (5.4), (5.6) and (5.8) we obtain a proof of conjecture 4.1 when $S = \Sigma$.

§ 6. Cyclic groups of prime order.

In this § we will consider Conjecture 4.1 in the case when $G \cong \boldsymbol{Z}/l\boldsymbol{Z}$ is cyclic of prime order l. We will show that θ_G lies in I^n, and vanishes $\pmod{I^{n+1}}$ if and only if $m \det_G \lambda \equiv 0$. This proves the conjecture when $G \cong \boldsymbol{Z}/2\boldsymbol{Z}$, which is the relevant case for number fields, and shows it is true up to an element of $(\boldsymbol{Z}/l\boldsymbol{Z})^*$ when $G\cong\boldsymbol{Z}/l\boldsymbol{Z}$. It would be interesting to prove the full result when $l\geqq 3$; this seems to involve a refinement of the techniques of classical genus theory.

We assume, as usual, that $n\geqq 1$ and that G is cyclic of order l, with a generator σ. Then I is a principle ideal in $\boldsymbol{Z}[G]$, generated by $\sigma-1$. Hence $I^k=(\sigma-1)^k$ and $I^k/I^{k+1}\cong G$ for all $k\geqq 1$. Using the fact that σ has prime order, we can give a simple criterion for membership in I^k.

LEMMA 6.1. *Assume $\theta\in I$. Then $\theta\in I^k$ if and only if*

$$\mathrm{ord}_l\Big(\prod_{\substack{\chi\in\hat{G}\\ \chi\neq 1}}\chi(\theta)\Big)\geqq k.$$

PROOF. We note that when $\chi\neq 1$, $\zeta=\chi(\sigma)$ is a primitive l^{th} root of unity and $\chi(\theta)$ is an algebraic integer in the cyclotomic field $\boldsymbol{Q}(\zeta)$. The product occuring in Lemma 6.1 is the norm of $\chi(\theta)$ from $\boldsymbol{Q}(\zeta)$ to $\boldsymbol{Q}$, as the different non-trivial characters of G and all obtained by conjugating χ over $\boldsymbol{Q}$. Hence the product is an integer, which is non-zero if and only if $\theta\neq 0$ in $\boldsymbol{Z}[G]$.

Since the rational prime l is totally ramified in $\boldsymbol{Q}(\zeta)$: $(l)=(\zeta-1)^{l-1}$, the l-valuation of the norm is equal to the $(\zeta-1)$-valuation of $\chi(\theta)$. If $\theta\in I^k$ then $\theta=(\sigma-1)^k\eta$ with $\eta\in\boldsymbol{Z}[G]$, so $\chi(\theta)=(\zeta-1)^k\chi(\eta)$ has valuation $\geqq k$. Conversely, if $\chi(\theta)=(\zeta-1)^k(\sum_{i=1}^{l-1}a_i\zeta^i)$ has valuation $\geqq k$ in $\boldsymbol{Z}[\zeta]$, let $\eta=\sum_{i=1}^{l-1}a_i\sigma^i$ in $\boldsymbol{Z}[G]$. Then $\theta=(\sigma-1)^k\eta$ in $\boldsymbol{Z}[G]$, as $\psi(\theta)=\psi((\sigma-1)^k\eta)$ for *all* characters ψ of G (here is where we use the hypothesis that $\theta\in I$, which is equivalent to $\psi(\theta)=0$ for the trivial character). Hence $\theta\in I^k$.

When $\theta=\theta_G$, the product $\prod_{\chi\neq 1}\chi(\theta_G)$ which occurs in Lemma 6.1 can be evaluated by the class-number formula. By global classfield theory, the group G corresponds to the Galois group of a unique cyclic extension L of degree l over k. Furthermore,

$$\zeta_{T(L)}(s)=\zeta_T(s)\prod_{\chi\neq 1}L_T(\chi,s) \tag{6.2}$$

where the zeta-function of L, on the left-hand side of (6.2), is taken relative to the sets $S(L)$ and $T(L)$ of primes dividing S and T respectively. Since for $\chi\neq 1$ we have $\chi(\theta_G)=L_T(\chi,0)$, we find

$$\prod_{\chi\neq 1}\chi(\theta_G)=\lim_{s\to 0}\left\{\frac{\zeta_{T(L)}(s)}{\zeta_T(s)}\right\}. \tag{6.3}$$

By (1.6), the above limit is zero if any place $v \in S$ is split in L. In this case $\theta_G = 0$ and, since λ has a trivial row, Conjecture 4.1 is true. When all places in S are either ramified or inert in L, the limit is non-zero and equal to

$$M_L = h_{T(L)} \cdot R_{T(L)} / h_T \cdot R_T \tag{6.4}$$

by (1.6), as $w_T = w_{T(L)} = 1$. By Lemma 6.1, M_L is an integer, and $\theta_G \in I^k$ if and only if $\mathrm{ord}_l(M_L) \geqq k$. We wish to use this criterion to show that $\theta_G \equiv 0 \pmod{I^n}$, where $n = \sharp S - 1 = \sharp S(L) - 1$.

To verify this congruence for θ_G (or even to test Conjecture 4.1 in its entirety), we may enlarge S by adding a finite number of places which are inert in L. Indeed, if $\mathfrak{p}$ is such a place and $S' = S \cup \{\mathfrak{p}\}$, then $\theta'_G = (1 - g(\mathfrak{p})) \cdot \theta_G$ with $g(\mathfrak{p}) \neq 1$. Hence $I = (1 - g(\mathfrak{p}))$ and θ'_G lies in I^{k+1} if and only if θ_G lies in I^k. Since the inert primes $\mathfrak{p}$ have density $(l-1)/l > 0$, they generate the class group of k. By enlarging S if necessary, we may, and will, assume that $h = h(A_S)$ is prime to l. (This simplifies some of the calculations below.) Let H be the class-number of the $S(L)$-integers in L.

The definition (1.1) of the regulator homomorphism and the fact that $\|\varepsilon\|_w = \|\varepsilon\|_v^l$ for every unit $\varepsilon \in U$, where $v \in S$ and w is the unique place dividing v in $S(L)$, shows that

$$\begin{aligned} R_{T(L)}/R_T &= l^n / (U_{T(L)} \colon U_T) \\ &= l^n \cdot (U_L \colon U_{T(L)}) / (U_L \colon U) \cdot (U \colon U_T). \end{aligned} \tag{6.5}$$

On the other hand, the T-class numbers are given by

$$\begin{cases} h_T = h \cdot \prod_{\mathfrak{p} \in T} (N\mathfrak{p} - 1) / (U \colon U_T). \\ h_{T(L)} = H \cdot \prod_{\mathfrak{P} \in T(L)} (N\mathfrak{P} - 1) / (U_L \colon U_{T(L)}). \end{cases} \tag{6.6}$$

Consequently, we obtain the following formula for M_L

$$M_L = l^n H \prod_T \frac{\prod_{\mathfrak{P} | \mathfrak{p}} (N\mathfrak{P} - 1)}{N\mathfrak{p} - 1} \Big/ (U_L \colon U) h. \tag{6.7}$$

Call the local factor at each place $\mathfrak{p} \in T$ of this product $m_L(\mathfrak{p})$. Then

$$m_L(\mathfrak{p}) = \begin{cases} (N\mathfrak{p} - 1)^{l-1} & \text{if } \mathfrak{p} \text{ is split in } L \\ \dfrac{(N\mathfrak{p}^l - 1)}{(N\mathfrak{p} - 1)} & \text{if } \mathfrak{p} \text{ is inert in } L. \end{cases} \tag{6.8}$$

In either case, $m_L(\mathfrak{p})$ is a positive integer which is divisible by l if and only if $N\mathfrak{p}\equiv 1 \pmod{l}$. By (6.7) and our hypothesis that h is prime to l, we have

$$\text{(6.9)} \qquad \operatorname{ord}_l(M_L)=n+\operatorname{ord}_l(H)+\sum_T \operatorname{ord}_l(m_L(\mathfrak{p}))-\operatorname{ord}_l(U_L\colon U).$$

Now consider the Sylow l-subgroup of the finite abelian group U_L/U. If it is non-trivial, we may find $\alpha\in U_L-U$ with $\alpha^l\in U$. This is impossible when k has characteristic l, for then $L=k(\alpha)$ would be an inseparable extension. More generally, if σ is a generator of G, we must have $\alpha^{\sigma-1}=\zeta$ equal to a primitive l^{th} root of unity. Hence if $\operatorname{ord}_l(U_L\colon U)>0$, L^* contains the group μ_l; since the degree of $k(\mu_l)$ over k divides $(l-1)$, k^* must also contain μ_l, so $w\equiv 0 \pmod{l}$. In this case, Kummer theory shows that the subgroup killed by l in U_L/U is isomorphic to $\boldsymbol{Z}/l\boldsymbol{Z}$, so the Sylow l-subgroup is cyclic. If U_L/U contains an element β of order l^2, then $\beta^{\sigma-1}=\zeta'$ is a primitive l^2-root of unity. Since $N_{L/k}\zeta'=1$, $\zeta'\in L-k$ and $L=k(\zeta')=k(\mu_{l^2})$. Furthermore, $\beta^l=(\zeta')^a\cdot u$ with $u\in U$ and $a\in(\boldsymbol{Z}/l\boldsymbol{Z})^*$; this follows from the cyclicity of the Sylow l-subgroup. Hence $L(\sqrt[l]{\zeta'})=k(\mu_{l^3})$ is the compositum of L with the cyclic extension $k(\sqrt[l]{u})$. Since $(1+l\boldsymbol{Z})/(1+l^3\boldsymbol{Z})$ is cyclic for $l\geqq 3$, this can only occur in the case when $l=2$. Summarizing the above paragraph, we have shown

LEMMA 6.10. *If* $w\not\equiv 0 \pmod{l}$ *then* $\operatorname{ord}_l(U_L\colon U)=0$. *If* $w\equiv 0 \pmod{l}$ *then* $\operatorname{ord}_l(U_L\colon U)=1$, *except in the special case when* $l=2$ *and* $L=k(\mu_4)$.

Leaving aside the special case for the moment, we may combine this lemma with formula (6.9) to show $\operatorname{ord}_l(M_L)\geqq n$, and hence that $\theta_G\equiv 0 \pmod{I^n}$. Indeed, when $w\equiv 0 \pmod{l}$ we have $\operatorname{ord}_l m_L(\mathfrak{p})\geqq 1$ for all $\mathfrak{p}\in T$ which do not have residual characteristic l, and T must contain at least one such place. Hence $\sum_T \operatorname{ord}_l m_L(\mathfrak{p})-\operatorname{ord}_l(U_L\colon U)\geqq 0$. We will have $\theta_G\not\equiv 0 \pmod{I^{n+1}}$ if and only if $\operatorname{ord}_l(M_L)=n$. This forces $\operatorname{ord}_l(H)=0$ and $\sum_T \operatorname{ord}_l m_L(\mathfrak{p})=\operatorname{ord}_l(U_L\colon U)$. When $w\not\equiv 0 \pmod{l}$ the latter condition is just $N\mathfrak{p}\not\equiv 1 \pmod{l}$ for any $\mathfrak{p}\in T$. When $w\equiv 0 \pmod{l}$ it means that T contains a *single* place $\mathfrak{p}$ of residue characteristic $\neq l$ and $m_L(\mathfrak{p})\not\equiv 0 \pmod{l^2}$. Referring to (6.8) we see that for $l>2$, this condition is simply that $\mathfrak{p}$ is inert in L. If $l=2$ and $L=k(\sqrt{\alpha})$, $\mathfrak{p}$ must be inert in the extension $L'=k(\sqrt{-\alpha})$ (which is quadratic, as we are not in the special case). Hence we have shown the following.

PROPOSITION 6.11. *Assume* $G\cong \boldsymbol{Z}/l\boldsymbol{Z}$ *and, when* $l=2$ *that* $L\neq k(\mu_4)$. *Then* $\theta_G\equiv 0 \pmod{I^n}$. *Assume further that no prime* $\mathfrak{p}\in S$ *is split in* L *and that* h *is prime to* l. *Then* $\theta_G\not\equiv 0 \pmod{I^{n+1}}$ *if and only if* H *is prime to* l *and*

a) [*When* $w\not\equiv 0 \pmod{l}$] *no prime* $\mathfrak{p}\in T$ *satisfies* $N\mathfrak{p}\equiv 1 \pmod{l}$,

b) [*When* $w\equiv 0 \pmod{l}$ *and* $L=k(\sqrt[l]{\alpha})$] T *contains exactly one place* $\mathfrak{p}$ *which is not of residual characteristic* l, *and* $\mathfrak{p}$ *is inert in the cyclic extension* $L'=k(\sqrt[l]{\alpha'})$, *with* $\alpha'=(-1)^{l-1}\alpha$.

We now consider the exceptional case when $l=2$ and $L=k(\mu_4)$. When $k=\boldsymbol{F}_q(X)$ is the function field of the curve X over the finite field with q elements, this forces $q\equiv 3 \pmod 4$ and $L=\boldsymbol{F}_{q^2}(X)$, the constant field extension. The group U_L/U is isomorphic to $\boldsymbol{F}_{q^2}^*/\boldsymbol{F}_q^*$, which is cyclic of order $(q+1)$. Furthermore

$$m_L(\mathfrak{p})=\begin{cases} q^{\deg \mathfrak{p}}-1 & \text{if} \quad \deg \mathfrak{p}\equiv 0 \ (2) \\ q^{\deg \mathfrak{p}}+1 & \text{if} \quad \deg \mathfrak{p}\equiv 1 \ (2). \end{cases}$$

In the first case $m_L(\mathfrak{p})\equiv 0 \pmod{(q^2-1)}$, so $\operatorname{ord}_2 m_L(\mathfrak{p})-\operatorname{ord}_2(U_L\colon U)\geqq 1$ and $\operatorname{ord}(M_L)\geqq n+1$. In the second case, $\operatorname{ord}_2 m_L(\mathfrak{p})=\operatorname{ord}_2(U_L\colon U)$. Consequently, $\theta_G\equiv 0 \pmod{I^n}$, and $\theta_G\not\equiv 0 \pmod{I^{n+1}}$ if and only if H is odd and $T=\{\mathfrak{p}\}$ consists of a single place which is inert in L. Now assume k is a number field and, for simplicity, that S contains all places dividing 2. If $\operatorname{ord}_2(w_L)=t\geqq 2$, let ζ denote an element of order 2^t in $\mu(L)$; since k must be the totally real subfield of the CM field L (so no archimedean places are split in L/k), the element $\eta=\zeta+\zeta^{-1}=\zeta+\bar{\zeta}$ lies in k. Let $\alpha'=2+\eta$, which is an element in U. If $(\zeta')^2=\zeta$, then $\zeta'\notin L$ and $\eta'=\zeta'+(\zeta')^{-1}\notin k$. Since $(\eta')^2=\alpha'$, this shows that α' is not a square in k^* and hence that the extension $L'=k(\sqrt{\alpha'})=k(\eta')$ is quadratic.

In this case, the element $(1+\zeta)$ generates the 2-Sylow subgroup of U_L/U, which has order 2^t. We also have

$$m_L(\mathfrak{p})=\begin{cases} N\mathfrak{p}-1 & \text{if} \quad N\mathfrak{p}\equiv 1 \pmod{2^t} \\ N\mathfrak{p}+1 & \text{if} \quad N\mathfrak{p}\equiv -1 \pmod{2^t}. \end{cases}$$

The fact that $N\mathfrak{p}\equiv \pm 1 \pmod{2^t}$ is equivalent to the fact that k contains the field $\boldsymbol{Q}(\zeta+\zeta^{-1})=\boldsymbol{Q}(\eta)$. Hence $m_L(\mathfrak{p})\equiv 0 \pmod{2^t}$ and $\operatorname{ord}_2(M_L)\geqq n$. We have $\theta_G\not\equiv 0 \pmod{I^{n+1}}$ if and only if H is odd and $T=\{\mathfrak{p}\}$ consists of a single place with $\operatorname{ord}_2 m_L(\mathfrak{p})=t$. This is equivalent to assuming that $\mathfrak{p}$ is inert in the quadratic extension L'. Hence we have proved

PROPOSITION 6.12. *Assume* $L=k(\mu_4)$. *Then* $\theta_G\equiv 0$ (*mod* I^n). *Assume further that no prime* $\mathfrak{p}\in S$ *is split in* L *and that* h *is odd. Then* $\theta_G\not\equiv 0$ (*mod* I^{n+1}) *if and only if* H *is odd and*

a) [*When* char$(k)>0$] $T=\{\mathfrak{p}\}$ *with* $\mathfrak{p}$ *inert in* L.

b) [*When* char$(k)=0$] $T=\{\mathfrak{p}\}$ *with* $\mathfrak{p}$ *inert in the quadratic extension* $L'=k(\sqrt{2+\zeta+\zeta^{-1}})$, *where* ζ *generates the* 2*-Sylow subgroup of* $\mu(L)$.

We conclude with some examples in case b). If $w_L\equiv 4\pmod 8$ then $\zeta=i$ and $L'=k(\sqrt{2})$; this is the case in the example discussed after Proposition 5.6. If $w_L\equiv 8\pmod{16}$ then $\zeta+\zeta^{-1}=\sqrt{2}\subset k$ and $L'=k(\sqrt{2+\sqrt{2}})$.

We now turn to an analysis of the term $m\cdot\det_G\lambda$, under the usual assumptions that $n\geqq 1$, S contains no prime which is split in L, and that h is prime to l. Since $I^n/I^{n+1}\cong \boldsymbol{Z}/l\boldsymbol{Z}$ and $m=\pm h(\prod_T \boldsymbol{F}_{\mathfrak{p}}^*:\tilde{U})$, we have $m\cdot\det_G\lambda\not\equiv 0\pmod{I^{n+1}}$ if and only if

$$(6.13)\qquad \begin{cases}\det_G\lambda\not\equiv 0 & \pmod{I^{n+1}}\\ \left(\prod_T \boldsymbol{F}_{\mathfrak{p}}^*:\tilde{U}\right) & \text{is prime to } l.\end{cases}$$

Consider the homomorphism $f\colon U\to G^S\cong(\boldsymbol{Z}/l\boldsymbol{Z})^{n+1}$, where the v^{th} component of $f(\varepsilon)$ is the image of the idèle $(1, 1, \cdots, \varepsilon_v, \cdots, 1)$ in G. Since G is a quotient of $A^*/k^*\prod_{v\notin S}A_v^*$ the image of f lies in the hyperplane $V\subseteq G^S$ where the sum of the coordinates is zero. Let U^+ denote the kernel of f; by local class field theory, we have $\varepsilon\in U^+$ if and only if ε_v is a norm in L_v/k_v for all places $v\in S$. Since L/k is unramified outside S, any $\varepsilon\in U$ is a norm at all places $v\notin S$, so $\varepsilon\in U^+$ if and only if ε is a local norm at all places. Since L/k is cyclic, the set of $\varepsilon\in k^*$ which are local norms everywhere coincides with the set of norms from L^*. Hence $U^+=U\cap(NL^*)$.

On the other hand, the quotient U/NU_L is isomorphic to $(\boldsymbol{Z}/l\boldsymbol{Z})^n$, so $f(U)=V$ if and only if $U\cap(NL^*)=NU_L$. I claim the latter condition is equivalent to the hypothesis that H is prime to l; this is the content of classical genus theory, and we sketch a proof. If $H\equiv 0\pmod l$, there is an element in $\mathrm{Pic}(A_{S(L)})$ of order l which is fixed by the l-group G. If $\mathfrak{A}$ is a representative ideal, then $\mathfrak{A}^{\sigma-1}=(\gamma)$ for $\gamma\in L^*$. Then $\varepsilon=N\gamma$ is an element of $U\cap(NL^*)-NU_L$. Conversely, any such ε gives a principal ideal (γ) of norm 1; since the Galois module of ideals prime to $S(L)$ has trivial cohomology: $(\gamma)=\mathfrak{A}^{\sigma-1}$. The class of $\mathfrak{A}$ has order l in $\mathrm{Pic}(A_{S(L)})$. Thus we have shown

LEMMA 6.14. *The map $f\colon U\to V\subseteq G^S$ is surjective if and only if H is prime to l.*

This condition is necessary for the non-vanishing of the determinant of λ, as $\det_G\lambda\not\equiv 0 \pmod{I^{n+1}}$ if and only if $f(U^T)=V$. Any further relation on the image of U^T would give a zero column in the matrix of λ, as in the proof of 5.8.

When $w\not\equiv 0 \pmod l$ the $\boldsymbol{Z}_l$-module $U\otimes\boldsymbol{Z}_l$ is free and $f(U)=V$ if and only if $U^+=U^l$. The condition $f(U^T)=V$ then implies that $U^T\cap U^l=(U^T)^l$, so $(U\colon U^T)$ is prime to l. Since $(U\colon U^T)\cdot(\prod_T \boldsymbol{F}_{\mathfrak{p}}^*\colon \tilde{U})=\prod_T(\boldsymbol{N}\mathfrak{p}-1)$, we see that the two conditions of (6.13) are equivalent, by Lemma 6.14, to the fact that the integer $H\cdot\prod_T(\boldsymbol{N}\mathfrak{p}-1)$ is prime to l. Since this agrees with the hypothesis in part a) of Proposition 6.11, we have shown that θ_G is a unit times $m\cdot\det_G\lambda$ in I^n/I^{n+1}.

When $w\equiv 0 \pmod l$ we have $f(U)=V$ if and only if U^l has index l in U^+. In this case, the quotient U^+/U^l is generated by an element α' which is a global norm from U_L. Writing $L=k(\sqrt[l]{\alpha})$ with $\alpha\in U_L$, we have $\alpha'=\alpha$ when $l>2$. When $l=2$ and $L\neq k(\mu_4)$ we have $\alpha'=-\alpha$. When $L=k(\mu_4)$ and $\mathrm{char}(k)>0$ we have $\alpha'=\alpha\equiv -1 \pmod{U^2}$; when $L=k(\mu_4)$ and $\mathrm{char}(k)=0$ we have $\alpha'=2+\zeta+\zeta^{-1}=\boldsymbol{N}(1+\zeta)$ in the notation of 6.12. To insure that $f(U^T)=V$ we must have $f(U)=V$ and the further condition that the index $(\prod_T \boldsymbol{F}_{\mathfrak{p}}^*\colon\langle\tilde{\alpha}'\rangle)$ is prime to l. Hence the first condition of (6.13) implies the second. Since the subgroup generated by α' is cyclic, there is exactly one $\mathfrak{p}\in T$ of characteristic $\neq l$, and this prime is inert in the field $L'=k(\sqrt[l]{\alpha'})$. These are exactly the hypotheses in part b) of 6.11 and in 6.12. Hence we have proved the following general result.

PROPOSITION 6.15. *If $G\cong\boldsymbol{Z}/l\boldsymbol{Z}$ then $\theta_G\equiv u\cdot m\cdot\det_G\lambda \pmod{I^{n+1}}$ with $u\in(\boldsymbol{Z}/l\boldsymbol{Z})^*$.*

§ 7. A refinement of Stark's conjecture.

Stark [11] has proposed several interesting conjectures which give the leading term in the expansion of Artin L-functions at $s=0$ in terms of a unit regulator. We will describe his conjecture on the first derivatives of abelian L-functions, and give a refinement along the lines of Conjecture 4.1.

First consider Conjecture 4.1 when $n=1$, so $S=\{v, v'\}$. Let ε be a generator of U^T, which is free of rank 1, and let $x=v-v'$ be a generator of $X=\mathrm{Div}_S^0$. Then $\det_R \lambda=\log|\varepsilon|_v$, and the class number formula gives:

$$\zeta_T'(0)=m\cdot\log|\varepsilon|_v=\log|u|_v, \tag{7.1}$$

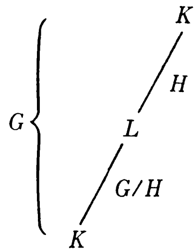
where $u=\varepsilon^m$ is *uniquely* determined in U^T by $\zeta'(0)$ and the choice of v. Conjecture 4.1 then predicts that for any abelian extension K/k which is unramified outside S and has Galois group G, we have $\theta_G\equiv m\cdot\det_G\lambda \pmod{I^2}$ where $\det_G\lambda\equiv r_v(\varepsilon)-1$ in I/I^2. Here $r_v\colon k_v^*\to A^*\to G$ is the Artin map of local classfield theory. If we use the isomorphism $I/I^2\xrightarrow{\sim}G$ which maps $\theta_G=\sum m(g)g$ to $\prod g^{m(g)}$, we see that Conjecture 4.1 is equivalent to the identity:

$$\prod_G g^{m(g)}\stackrel{?}{=}r_v(\varepsilon)^m=r_v(u) \tag{7.2}$$

in G. The unit u in (7.2) is determined by (7.1), and the integers $m(g)$ are the coefficients of g in $\prod_{\mathfrak{p}\in T}(1-g(\mathfrak{p})N\mathfrak{p})\sum_G\zeta_S(g, 0)\cdot g=\theta_G$. When v is ramified in K/k, the identity (7.2) gives more information on the unit u than is furnished by (7.1). We note that if u is defined by (7.1) then (7.2) should hold even when $\#S>2$. Since $\zeta'(0)=0$, we have $u=1$; but Conjecture 4.1 would imply that $\theta_G\equiv 0 \pmod{I^2}$, so $\prod g^{m(g)}=1$.

We now extend (7.1–7.2) by introducing an intermediate extension L of k, which is contained in K and fixed by the subgroup $H\subset G$:

(7.3)



We assume that $\#S\geqq 2$ and that S contains a place v which *splits completely* in L. Let w be a place of L which divides v. We say an element $u\in U_L$ is a v-unit if $|u|_{w'}=1$ for all $w'\nmid v$ when $\#S\geqq 3$. If $S=\{v, v'\}$ we say $u\in U_L$ is a v-unit if $|u|_{w'}=|u|_{\sigma w'}$ for all $\sigma\in\mathrm{Gal}(L/k)$, where w' is a place dividing v'. Then Stark has proposed the following [cf. 12, ch. IV]:

CONJECTURE 7.4 (Stark). *There is a unique element* $u=u(w)$ *in* L^* *satisfying*

1) u *is a v-unit.*
2) *For all* $\sigma \in G/H$: $\zeta_T'(\sigma, 0)=\log|u^\sigma|_w$.
3) $u \equiv 1$ (*mod* $\underline{T}$).

This conjecture is true when $L=k$, by (7.1). Using ratios of zeta functions, one can prove it when $[L:k]=2$. It is also known to be true when $k=\boldsymbol{Q}$ or $k=\boldsymbol{Q}(\sqrt{-D})$ is imaginary quadratic: this comprises the theory of circular and elliptic units, as well as that of Jacobi sums. Deligne [cf. 12, ch. V] and Hayes [6] have given different proofs of 7.4 when k is a function field.

To see that 7.4 is equivalent to the form of Stark's conjecture presented in Tate [12, pg. 89], which asserts the existence of $\varepsilon \in L^*$ satisfying 1), as well as

2′) $\forall \sigma \in G/H$, $\zeta'(\sigma, 0)=-(1/W)\log|\varepsilon^\sigma|_w$
3′) $\lambda=\sqrt[W]{\varepsilon}$ is abelian over k,

where $W=\#\mu(L)$, we put $u=\lambda^{\prod_T(g(\mathfrak{p})^{-1}N\mathfrak{p}-1)}$. Then $u \in L^*$ by Galois theory and u clearly satisfies 2) and 3).

To refine 7.4 using the further abelian extension K, we note that $L_w=k_v$, as v is split in K. The elements $r_w(u^\sigma)$ lie in the subgroup H, for all $\sigma \in G/H$. Since $\#S \geqq 2$ and $v \in S$ is split in K, the element $\theta_G \in \boldsymbol{Z}[G]$ lies in the kernel of the natural map from $\boldsymbol{Z}(G) \to \boldsymbol{Z}[G/H]$. Let us call this kernel I_H; when $H=G$, I_H is just the usual augmentation ideal. In particular, writing $\theta_G=\sum m(g)g$ we find

$$\sum_{g \in H\sigma} m(g)=0 \quad \text{for all } \sigma \in G/H. \tag{7.5}$$

CONJECTURE 7.6. *Let* $u \in L^*$ *be defined by Conjecture* 7.4. *Then*

$$r_w(u^\sigma)=\prod_{g \in H\sigma} g^{m(g)} \quad \textit{in } H, \textit{ for all } \sigma \in G/H.$$

When $L=K$ this is (7.2). In general, when L/K is ramified at w it gives more information on the v-unit u and its conjugates than Conjecture 7.4. If S contains 2 places which split in L (and at least 3 places), then Conjecture 7.4 is true with $u=1$. Conjecture 7.6 then predicts that $\prod_{H\sigma} g^{m(g)}=1$ for all $\sigma \in G/H$. This is precisely the statement that $\theta_G \in I_H^2$. In general, I would guess that $\theta_G \equiv 0 \bmod I_H^n$, where n is the number of $v \in S$ which are split in L (minus one, if all places in S are split).

Conjecture 7.6 is known to be true when $k=\boldsymbol{Q}$, where it gives the p-adic expansion of Jacobi sums, and Hayes [6, § 3–5] has recently proved it when k is a function field, using the theory of rank 1 Drinfeld modules. It would be interesting to find a proof when $L=k$ (formula 7.2) or, more generally, when $[L:k]=2$. In the quadratic case, we also have a more precise conjecture when $n>1$, which we will discuss in the next section.

§ 8. The L-functions of tori.

Another possible generalization of 4.1 is to the L-function of a torus τ defined over k. When $\tau \cong \boldsymbol{G}_m$ this gives the zeta-function; in general, one has an Artin L-function attached to the representation of the Galois group on the group $X(\tau)=\operatorname{Hom}(\tau, \boldsymbol{G}_m)$ of characters of τ. In this § we will treat the case when τ has dimension 1 but is not split over k. Then the representation on $X(\tau)$ gives a quadratic character χ of the Galois group, and hence a separable quadratic extension L/k which splits τ. We have an exact sequence of algebraic tori over k:

$$(8.1) \qquad 1 \longrightarrow \boldsymbol{G}_m \longrightarrow \operatorname{Res}_{L/k} \boldsymbol{G}_m \longrightarrow \tau \longrightarrow 1.$$

If σ denotes the non-trivial automorphism of L/k, then $\tau(k)=\{\alpha \in L^*: \alpha \cdot \alpha^\sigma = 1\}$.

As before, we fix a set S of places of k which is finite, non-empty, and contains all archimedean places as well as all places ramified in L/k. We fix a set T disjoint from S which is finite, non-empty, and separates the roots of unity in any abelian extension of k which is unramified outside S. Let A denote the S-integers of k and let $\mathcal{O}$ denote the $S(L)$ integers of L; since $\mathcal{O}/A$ is étale, we may define τ over A by the exact sequence (8.1), taking $\operatorname{Res}_{\mathcal{O}/A}\boldsymbol{G}_m$ as the middle term, or as the kernel of $\boldsymbol{N}\colon \operatorname{Res}_{\mathcal{O}/A} \boldsymbol{G}_m \to \boldsymbol{G}_m$. Then $\tau(A)=\{\varepsilon \in \mathcal{O}^*: \varepsilon \cdot \varepsilon^\sigma = 1\}$. Let $\tau(A)_T$ be the subgroup of units in $\tau(A)$ which are $\equiv 1$ (mod $T(L)$); then $\tau(A)_T$ is a free abelian group of rank n, the number of places $v \in S$ which are split in L/k.

The regulator homomorphism on the units of L $\lambda\colon U_L \to X_L \otimes \boldsymbol{R}$ is $\operatorname{Gal}(L/k)$ equivariant, so induces a map

$$(8.2) \qquad \lambda_\tau\colon \tau(A) \longrightarrow X_L^- \otimes \boldsymbol{R}$$

where $X_L^- \cong \boldsymbol{Z}^n$ is the minus eigenspace for the Galois action. Fix bases $\langle \varepsilon_1, \cdots, \varepsilon_n \rangle$ and $\langle x_1, \cdots, x_n \rangle$ for $\tau(A)_T$ and X_L^- respectively, and define $\det_R \lambda_\tau$ as the determinant of the matrix of this operator with respect to the bases chosen.

The L-function of τ, relative to S and T, is the abelian L-function $L_T(\chi, s)$ of the character χ. This has a zero of order n at $s=0$ and an expansion

$$(8.4) \qquad L_T(\chi, s) \equiv m_\tau \cdot \det_R \lambda_\tau \cdot s^n \pmod{s^{n+1}}$$

where m_τ is a non-zero integer (whose sign depends on the orientation of the bases chosen). In fact, using the formulae in [12, pg. 47–50] one can show that

$$(8.5) \qquad m_\tau = \pm \frac{h_{S(L)}}{h_S} \cdot (U_L^- : U_L^{1-\sigma}) \cdot \frac{\prod_{\mathfrak{p} \in T} (1 - \chi(\mathfrak{p}) N\mathfrak{p})}{(U_L^- : U_{L,T}^-)}$$

where $U_L^- = \tau(A)$ is the minus $S(L)$-units in L^*. A short calculation, using the cohomology sequence attached to (8.1), shows that the right hand side is $\pm \# H^1(A, \tau)^T$, the order of the group of principal homogeneous spaces for τ over A with trivialization at T. This shows m_τ is an integer.

Let K be an abelian extension of k, which is unramified outside S and does not contain L. Let G be the Galois group of K/k. Then $G = \mathrm{Gal}(KL/L)$ is a quotient of $A_L^*/L^* \prod_{v \notin S(L)} \mathcal{O}_v^*$ on which $\mathrm{Gal}(L/k)$ acts trivially. Hence the associated map $\lambda : U_L \to X_L \otimes G$ defined in § 2 is $\mathrm{Gal}(L/k)$-equivariant, and induces a homomorphism

$$(8.6) \qquad \lambda_\tau : \tau(A) \longrightarrow X_L^- \otimes G.$$

Let $\det_G \lambda_\tau \in I^n/I^{n+1}$ be the determinant of the matrix of λ_τ with respect to the bases chosen above for $\tau(A)_T$ and X_L^-.

As in § 3, define the Euler product

$$(8.7) \qquad \theta_T(\chi, s) = \prod_{\mathfrak{p} \in T} (1 - \chi(\mathfrak{p}) g(\mathfrak{p}) N\mathfrak{p}^{1-s}) \prod_{\mathfrak{p} \notin S} (1 - \chi(\mathfrak{p}) g(\mathfrak{p}) N\mathfrak{p}^{-s})^{-1}$$

with coefficients in $\boldsymbol{Z}[G]$. Then $\theta_G(\chi) = \theta_T(\chi, 0)$ lies in $\boldsymbol{Z}[G]$ by Proposition 3.7. Indeed, if $\theta_{G'} = \sum m(g') g'$ in $\boldsymbol{Z}[\mathrm{Gal}(LK/k)] = \boldsymbol{Z}[G']$, we have $\theta_G(\chi) = \sum_G \{m(g) - m(g^\sigma)\} g$.

The analog of Conjecture 4.1 for τ is then

CONJECTURE 8.8. $\theta_G(\chi) \equiv m_\tau \cdot \det_G(\lambda_\tau) \pmod{I^{n+1}}$.

It would be interesting to formulate this for a general torus over k; this is certainly connected to work of Ono [8] on Tamagawa numbers

Bibliography

[1] Cassou-Noguès, Pierrette, Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques, Invent. Math. **51** (1979), 29-59.

[2] Dedekind, R., Über die Theorie der algebraischen Zahlen: Supplement XI von Dirichlets Vorlesungen über Zahlentheorie, Gesammelte mathematische Werke Vol. 3, Brunschweig, 1932.

[3] Deligne, P. and K. Ribet, Values of abelian L-functions at negative integers over totally real fields, Invent. Math. **59** (1980), 227-286.

[4] Lejeune-Dirichlet, G., Recherches sur diverses applications de l'analyse infinitésimale a la théorie des nombres, Werke, tome 1, 411-496, Berlin, 1889.

[5] Gross, B., p-adic L-series at $s=0$, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), 979-994.

[6] Hayes, D., The refined $\mathfrak{p}$-adic abelian Stark conjecture in function fields, Invent. Math., to appear.

[7] Mazur, B. and J. Tate, Refined conjectures of the Birch and Swinnerton-Dyer type, Duke Math. J. **54** (1987), 711-750.

[8] Ono, T., On the Tamagawa number of algebraic tori, Ann. of Math. **78** (1963), 47-73.

[9] Ribet, K., Report on p-adic L-functions over totally real fields, Astérisque **61** (1979), 177-192.

[10] Siegel, C. L., Über die Fourierschen Koeffizienten von Modulformen, Nachr. Akad. Wiss. Göttingen Nr. 3, (1970), 15-56.

[11] Stark, H. M., L-functions at $s=1$ I-IV, Adv. in Math. **7** (1971) 301-343, **17** (1975) 60-92, **22** (1976) 64-84, **35** (1980) 197-235.

[12] Tate, J., Les Conjectures de Stark sur les Fonctions L d'Artin en $s=0$, Birkhäuser, Basel-Boston, 1984.

(Received July 3, 1987)

Department of Mathematics
Harvard University
Science Center
1 Oxford St.
Cambridge, MA 02138
U.S.A.