Appendix:
Ray class characters of bounded order and bounded conductor

David E. Rohrlich

We introduce a partial order on the set of formal Dirichlet series with non-negative real coefficients. Given two such series $A(s) = \sum_{q \geqslant 1} a(q)q^{-s}$ and $B(s) = \sum_{q \geqslant 1} b(q)q^{-s}$, write $A(s) \preccurlyeq B(s)$ to mean that $a(q) \leqslant b(q)$ for all $q \geqslant 1$. It is readily verified that if $A(s) \preccurlyeq B(s)$ and $C(s) \preccurlyeq D(s)$ then $A(s)C(s) \preccurlyeq B(s)D(s)$. Furthermore the implication holds at the level of Euler products: if $A(s) = \prod_p A_p(s)$ and $B(s) = \prod_p B_p(s)$ with $A_p(s) \preccurlyeq B_p(s)$ for all p then $A(s) \preccurlyeq B(s)$.

By way of illustration, let M be a number field, $\mathcal{O}_M$ its ring of integers, and $\zeta_M(s)$ the associated Dedekind zeta function. Then it is a standard remark that

$$(1) \qquad \qquad \zeta_M(s) \preccurlyeq \zeta(s)^m,$$

where $m = [M : \mathbb{Q}]$. Indeed let p be a rational prime and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_M$ above p, say of residue class degree f. The Euler factor of $\zeta_M(s)$ at $\mathfrak{p}$ satisfies

$$(1 - (\mathbf{N}\mathfrak{p})^{-s})^{-1} = \sum_{\nu \geqslant 0} p^{-\nu f s} \preccurlyeq \sum_{\nu \geqslant 0} p^{-\nu s} = (1 - p^{-s})^{-1}.$$

Hence if there are exactly r prime ideals $\mathfrak{p}$ above p then

$$\prod_{\mathfrak{p}|p} (1 - (\mathbf{N}\mathfrak{p})^{-s})^{-1} \preccurlyeq (1 - p^{-s})^{-r} \preccurlyeq (1 - p^{-s})^{-m}.$$

Passing to Euler products we obtain (1).

It follows from the definitions that if $A(s) \preccurlyeq B(s)$ then the associated summatory functions $\vartheta_A(x) = \sum_{n \leqslant x} a(n)$ and $\vartheta_B(x) = \sum_{n \leqslant x} b(n)$ satisfy $\vartheta_A(x) \leqslant \vartheta_B(x)$ for all x. For example, let $A(s)$ and $B(s)$ be the two sides of (1): Using Theorem 7.7 on p. 154 of [1] to estimate the summatory function of $\zeta(s)^m$, we obtain

$$(2) \qquad \qquad \sum_{\mathbf{N}\mathfrak{q} \leqslant x} 1 \ll x(\log x)^{m-1} \qquad \qquad (x \geqslant 2),$$

where $\mathfrak{q}$ denotes a nonzero ideal of $\mathcal{O}_M$ and the implicit constant depends only on m, not on M.

To illustrate the use of (2), let us deduce a standard bound for the class number h_M of M. Let r_1 and r_2 be the number of real embeddings and half the number of complex embeddings of M, so that $r_1 + 2r_2 = m$. Thus the Minkowski constant $(4/\pi)^{r_2} m!/m^m$ is bounded above by

$$\mu = (4/\pi)^{m/2} \frac{m!}{m^m},$$

and therefore Minkowski's theorem gives

$$(3) \qquad \qquad h_M \leqslant \sum_{\mathbf{N}\mathfrak{q} \leqslant \mu \sqrt{d_M}} 1,$$

where d_M is the absolute value of the discriminant of M (cf. [2], pp. 119-120). Combining (3) with (2), we recover the well-known bound

$$(4) \qquad \qquad h_M \ll \sqrt{d_M}(\log d_M)^{m-1} \qquad \qquad (\mu\sqrt{d_M} \geqslant 2),$$

where the implicit constant depends only on m. We shall regard m as a fixed integer $\geqslant 2$, and thus the condition $\mu\sqrt{d_M} \geqslant 2$ is satisfied for all but finitely many

d_M with $[M : \mathbb{Q}] = m$. Furthermore, since $m \geqslant 2$, we have $d_M \geqslant 2$. Therefore we can remove the condition $\mu\sqrt{d_M} \geqslant 2$ from (4) and still assert that the implicit constant in (4) depends only on m. Actually it is more useful to state (4) for h_M^{nar}, the narrow ray class number of M. Since $h_M^{\mathrm{nar}} \leqslant 2^{r_1} h_M$, we have

$$(5) \qquad h_M^{\mathrm{nar}} \ll \sqrt{d_M}(\log d_M)^{m-1},$$

where the implicit constant depends only on m.

It is convenient to refine the relation $\preccurlyeq$ slightly. Suppose that $A(s)$ and $B(s)$ are Dirichlet series over M in the sense that they are presented to us in the form $A(s) = \sum_{\mathfrak{q}} a(\mathfrak{q})(\mathbf{N}\mathfrak{q})^{-s}$ and $B(s) = \sum_{\mathfrak{q}} b(\mathfrak{q})(\mathbf{N}\mathfrak{q})^{-s}$, where $\mathfrak{q}$ denotes as before a nonzero ideal of $\mathcal{O}_M$. We write $A(s) \preccurlyeq_M B(s)$ to mean that $a(\mathfrak{q}) \leqslant b(\mathfrak{q})$ for all $\mathfrak{q}$. Thus $\preccurlyeq$ coincides with $\preccurlyeq_{\mathbb{Q}}$. Of course every Dirichlet series is a Dirichlet series over $\mathbb{Q}$, and one readily verifies that if $A(s) \preccurlyeq_M B(s)$ then $A(s) \preccurlyeq B(s)$.

Given a rational integer $c \geqslant 2$, let

$$R_{M,c}(s) = \sum_{\mathfrak{q}} h_{M,c}^*(\mathfrak{q})(\mathbf{N}\mathfrak{q})^{-s}$$

where $h_{M,c}^*(\mathfrak{q})$ is the number of idele class characters χ of M of conductor $\mathfrak{q}$ such that $\chi^c = 1$. Also put

$$E_{M,c}(s) = \prod_{p|c}\prod_{\mathfrak{p}|p}\Big(\sum_{\nu=0}^{e(\mathfrak{p})(v_p(c)+1)}(\mathbf{N}\mathfrak{p})^{\nu(1-s)}\Big),$$

where $e(\mathfrak{p})$ is the ramification index of $\mathfrak{p}$ over p and $v_p(c)$ the p-adic valuation of c.

Proposition 1. $R_{M,c}(s) \preccurlyeq_M h_M^{\mathrm{nar}} \cdot (\zeta_M(s)/\zeta_M(2s))^{c-1} \cdot E_{M,c}(s)$.

Define

$$E_{m,c} = \prod_{p|c}\prod_{e=1}^{m}\prod_{f=1}^{m}\Big(\sum_{\nu=0}^{e(v_p(c)+1)}p^{f\nu(1-s)}\Big)^m,$$

The following variant of Proposition 1 is weaker but actually more useful:

Proposition 2. $R_{M,c}(s) \preccurlyeq h_M^{\mathrm{nar}} \cdot \zeta(s)^{m(c-1)} \cdot E_{m,c}(s)$.

Proof. By inspection, $E_{M,c}(s) \preccurlyeq E_{m,c}(s)$. Also

$$\zeta_M(s)/\zeta_M(2s) = \prod_{\mathfrak{p}}(1 + (\mathbf{N}\mathfrak{p})^{-s}) \preccurlyeq \prod_{p}\Big(\sum_{\nu\geqslant 0}p^{-\nu s}\Big)^m = \zeta(s)^m,$$

where $\mathfrak{p}$ runs over all nonzero prime ideals of $\mathcal{O}_M$. $\qquad\square$

Let $\vartheta_{M,c}(x)$ and $\vartheta_{m,c}(x)$ denote the summatory function associated to $R_{M,c}(s)$ and $\zeta(s)^{m(c-1)} \cdot E_{m,c}(s)$ respectively. Then Proposition 2 gives

$$\vartheta_{M,c}(x) \leqslant h_M^{\mathrm{nar}}\vartheta_{m,c}(x),$$

which in conjunction with (5) becomes

$$(6) \qquad \vartheta_{M,c}(x) \ll \sqrt{d_M}(\log d_M)^{m-1}\vartheta_{m,c}(x).$$

Here the implicit constant depends only on m. Since $E_{m,c}(s)$ is entire while $\zeta(s)$ has a simple pole at $s = 1$, we obtain (cf. [1], *loc. cit.*):

Corollary. $\vartheta_{M,c}(x) \ll \sqrt{d_M}(\log d_M)^{m-1}x(\log x)^{m(c-1)-1}$, *the implicit constant depending only on c and $m = [M : \mathbb{Q}]$.*

We turn to the proof of Proposition 1. Put

$$\varphi_M(\mathfrak{q}) = |(\mathcal{O}_M/\mathfrak{q})^\times|,$$

and let $\mathbb{A}_M^\times$ be the group of ideles of M. As usual, we think of $\mathbb{A}_M^\times$ as the restricted direct product $\prod_v' M_v^\times$, where v runs over the places of M and M_v is the completion of M at v, and we identify $M^\times$ with its image in $\mathbb{A}_M^\times$ under the diagonal embedding. We also put

$$(7) \qquad\qquad \widehat{\mathcal{O}}_M = \prod_{v\nmid\infty} \mathcal{O}_v,$$

where v runs over the finite places of M and $\mathcal{O}_v$ is the ring of integers of M_v. By appending the coordinate 1 at the infinite places, we may view $\widehat{\mathcal{O}}_M^\times$ as a subgroup of $\mathbb{A}_M^\times$. Similarly, the product $M_\infty^\times = \prod_{v|\infty} M_v^\times$ and its identity component $(M_\infty^\times)^0$ are subgroups of $\mathbb{A}_M^\times$ with coordinate 1 at the finite places. With these conventions,

$$h_M^{\mathrm{nar}} = |\mathbb{A}_M^\times/(M^\times \cdot \widehat{\mathcal{O}}_M^\times \cdot (M_\infty^\times)^0)|$$

(cf. [2], pp. 146-147). As idele class characters are trivial on the principal ideles and idele class characters of finite order are trivial on the identity component at infinity, we deduce that there are at most h_M^{nar} extensions of a given character of $\widehat{\mathcal{O}}_M^\times$ to a finite-order idele class character of M. Let us write $\varphi_{M,c}^*(\mathfrak{q})$ for the number of characters χ of $\widehat{\mathcal{O}}_M^\times$ of order dividing c and conductor $\mathfrak{q}$, the conductor of a character of $\widehat{\mathcal{O}}_M^\times$ being defined in the same way as for idele class characters. Then the preceding discussion gives

$$h_{M,c}^*(\mathfrak{q}) \leqslant h_M^{\mathrm{nar}} \varphi_{M,c}^*(\mathfrak{q}).$$

Now $\varphi_{M,c}^*$ is multiplicative because $\widehat{\mathcal{O}}_M^\times = \prod_{v\nmid\infty} \mathcal{O}_v^\times$ by (7). Thus

$$(8) \qquad\qquad \sum_{\mathfrak{q}} h_{M,c}^*(\mathfrak{q})(\mathbf{N}\mathfrak{q})^{-s} \preccurlyeq_M h_M^{\mathrm{nar}} \prod_{\mathfrak{p}} \Big(\sum_{\nu\geqslant 0} \varphi_{M,c}^*(\mathfrak{p}^\nu)(\mathbf{N}\mathfrak{p})^{-\nu s}\Big),$$

where $\mathfrak{p}$ runs over the nonzero prime ideals of $\mathcal{O}_M$.

We now focus on the Euler factor in (8) corresponding to a particular prime ideal $\mathfrak{p}$. Let v be the corresponding place of M and p the residue characteristic of $\mathfrak{p}$. We consider cases according as $p|c$ or $p\nmid c$. In both cases we use the fact that if $\nu \geqslant 2$ then $\varphi_{K,c}^*(\mathfrak{p}^\nu)$ is the number of characters of $\mathcal{O}_v^\times$ of order dividing c which factor through $\mathcal{O}_v^\times/(1+\mathfrak{p}^\nu\mathcal{O}_v)$ but not through $\mathcal{O}_v^\times/(1+\mathfrak{p}^{\nu-1}\mathcal{O}_v)$.

Suppose first that $p\nmid c$. Then any character of $\mathcal{O}_v^\times$ of order dividing c is trivial on the pro-p-group $1+\mathfrak{p}\mathcal{O}_v$. Hence if $\nu \geqslant 2$ then $\varphi_{M,c}^*(\mathfrak{p}^\nu) = 0$. Furthermore

$$\varphi_{M,c}^*(\mathfrak{p}) = \gcd(c, \mathbf{N}\mathfrak{p}-1) - 1$$

because $\mathcal{O}_v^\times/(1+\mathfrak{p}\mathcal{O}_v)$ is cyclic and the trivial character of $\mathcal{O}_v^\times$ does not have conductor $\mathfrak{p}$. In particular we have $\varphi_{M,c}^*(\mathfrak{p}) \leqslant c-1$, whence

$$\sum_{\nu\geqslant 0} \varphi_{M,c}^*(\mathfrak{p}^\nu)(\mathbf{N}\mathfrak{p})^{-\nu s} \preccurlyeq_M 1 + (c-1)(\mathbf{N}\mathfrak{p})^{-s}.$$

Therefore

$$(9) \qquad\qquad \sum_{\nu\geqslant 0} \varphi_{M,c}^*(\mathfrak{p}^\nu)(\mathbf{N}\mathfrak{p})^{-\nu s} \preccurlyeq_M (1 + (\mathbf{N}\mathfrak{p})^{-s})^{c-1}$$

by the binomial theorem.

Next suppose that $p|c$. If $k \geqslant e(\mathfrak{p})/(p-1)+1$ then every element of $1+c\mathfrak{p}^k\mathcal{O}_v$ is a cth power (cf. [2], p. 186). In particular, every element of $1+c\mathfrak{p}^{e(\mathfrak{p})+1}\mathcal{O}_v$ is a cth power. It follows that $\varphi^*_{M,c}(\mathfrak{p}^\nu\mathcal{O}_v) = 0$ for $\nu \geqslant e(\mathfrak{p})(v_p(c)+1)+1$. Now for $1 \leqslant \nu \leqslant e(\mathfrak{p})(v_p(c)+1)$ we apply the trivial estimate

$$\varphi^*_{M,c}(\mathfrak{p}^\nu) \leqslant |\mathcal{O}_v^\times/(1+\mathfrak{p}^\nu\mathcal{O}_v)|.$$

Since $|\mathcal{O}_v^\times/(1+\mathfrak{p}^\nu\mathcal{O}_v)| = (\mathbf{N}\mathfrak{p})^{\nu-1}(\mathbf{N}\mathfrak{p}-1) \leqslant (\mathbf{N}\mathfrak{p})^\nu$, we obtain

$$(10) \qquad \sum_{\nu \geqslant 0} \varphi^*_{M,c}(\mathfrak{p}^\nu)(\mathbf{N}\mathfrak{p})^{-\nu s} \preccurlyeq_M \sum_{\nu=0}^{e(\mathfrak{p})(v_p(c)+1)} (\mathbf{N}\mathfrak{p})^{\nu(1-s)}.$$

This completes our discussion of the individual Euler factors in (8).

Now combine (8), (9), and (10). We obtain

$$(11) \qquad \sum_{\mathfrak{q}} h^*_{M,c}(\mathfrak{q})(\mathbf{N}\mathfrak{q})^{-s} \preccurlyeq_M h^{\mathrm{nar}}_M \cdot \prod_{p \nmid c}\prod_{\mathfrak{p}|p}(1+(\mathbf{N}\mathfrak{p})^{-s})^{c-1} \cdot E_{M,c}(s)$$

We may weaken the estimate in (11) by extending the product over $p \nmid c$ to a product over all p, and then we use the identity

$$\zeta_M(s)/\zeta_M(2s) = \prod_{\mathfrak{p}}(1+(\mathbf{N}\mathfrak{p})^{-s}).$$

Making this substitution in (11), we obtain Proposition 1.

References

[1] P. T. Bateman and H. G. Diamond, *Analytic Number Theory: An Introductory Course*. World Scientific (2004).
[2] S. Lang, *Algebraic Number Theory*, Addison-Wesley (1968).