74. On the Divisibility of Dedekind's Zeta-Functions

By Makoto ISHIDA
Mathematical Institute, University of Tokyo
(Comm. by Z. SUETUNA, M.J.A., June 12, 1957)

Let k be an algebraic number field of finite degree and K a finite extension over k. Then it was conjectured by E. Artin [2] that the Dedekind's zeta-function $\zeta_k(s)$ of k divides the Dedekind's zeta-function $\zeta_K(s)$ of K, in the sense that the quotient $\zeta_K(s)/\zeta_k(s)$ is an integral function of the complex variable s. Already R. Dedekind [4] has proved that $\zeta_k(s)$ divides $\zeta_K(s)$, if K is a "rein" cubic extension of the rational field k. E. Artin [2], H. Aramata [1] and R. Brauer [3] have made contributions to this conjecture and obtained indeed affirmative answers in several special cases.

In this paper, using Artin's L-series and Brauer's group-theoretical lemma, I shall prove a theorem which includes all those former results as special cases. And here I wish to express my hearty gratitude to Prof. Z. Suetuna for his encouragement.

In the following, for sake of simplicity, we shall use the following notation: If U is a finite group, θ the character of the regular representation of U and λ_0 the principal character of U, then we shall denote the character $\theta-\lambda_0$ by $X(U)$.

Lemma 1 (R. Brauer [3]). Let G be a group of finite order g. Then the character $X(G)$ of G can be expressed as follows:

$$X(G)=\sum_{H_\sigma}\sum_j c_j^{(\sigma)}\,\Xi_{\psi_j^{(\sigma)}}, \tag{1}$$

where H_σ ranges over all the cyclic subgroups of order $h_\sigma>1$ of G and $\Xi_{\psi_j^{(\sigma)}}$ over the characters of G induced by all the irreducible characters $\psi_j^{(\sigma)}$ of H_σ. Furthermore, the coefficients $c_j^{(\sigma)}$ of $\Xi_{\psi_j^{(\sigma)}}$ in (1) are non-negative rational numbers with denominators g, and given by

$$c_j^{(\sigma)}=\frac{1}{g}\{\varphi(h_\sigma)-\sum_{\sigma^*}\psi_j^{(\sigma)}(\sigma^*)\}, \tag{2}$$

where σ^* ranges over all the generators of H_σ.

Remarking that the numerator of $c_j^{(\sigma)}$ depends only on H_σ and $\psi_j^{(\sigma)}$, we have the following important

Lemma 2. Let G and g be the same as in Lemma 1. Let H be an arbitrary subgroup of order $h>1$ of G. Then we can rewrite (1) as follows:

$$X(G)=\frac{h}{g}\,\Xi_{X(H)}+\sum\nolimits'_{H_{\sigma'}\not\subseteq H}\sum_j c_j^{(\sigma')}\,\Xi_{\psi_j^{(\sigma')}}, \tag{3}$$

where $\Xi_{X(H)}$ is the character of G induced by $X(H)$ and $H_{\sigma'}$ ranges over all the cyclic subgroups of order $h_{\sigma'}>1$ of G which are not contained in H.

Proof. If we consider Lemma 1 with regard to the finite group H, we have

$$(4) \qquad X(H)=\sum_{H_\tau}\sum_j \tilde{c}_j^{(\tau)}\chi_{\psi_j^{(\tau)}},$$

where H_τ and $\chi_{\psi_j^{(\tau)}}$ have the similar meaning as H_σ and $\Xi_{\psi_j^{(\sigma)}}$ in Lemma 1, but the coefficients $\tilde{c}_j^{(\tau)}$ are given by

$$\tilde{c}_j^{(\tau)}=\frac{1}{h}\{\varphi(h_\tau)-\sum_{\tau^*}\psi_j^{(\tau)}(\tau^*)\}$$

Then, according to the remark stated above, we have $\tilde{c}_j^{(\tau)}=\dfrac{g}{h}c_j^{(\tau)}$, and consequently

$$(4') \qquad \frac{h}{g}X(H)=\sum_{H_\tau}\sum_j c_j^{(\tau)}\chi_{\psi_j^{(\tau)}}.$$

If we substitute the character of G induced by the character (4′) of H in (1), then we have (3) easily.

Lemma 3. Let G and H be the same as in Lemmas 1 and 2. Let $\sigma H\sigma^{-1}$ be a conjugate of H in G. Then we have

$$(5) \qquad \Xi_{X(H)}=\Xi_{X(\sigma H\sigma^{-1})},$$

where $\Xi_{X(H)}$ and $\Xi_{X(\sigma H\sigma^{-1})}$ are the characters of G induced by $X(H)$ and $X(\sigma H\sigma^{-1})$ respectively.

Proof. Any element of $\sigma H\sigma^{-1}$ can be uniquely represented in the form $\sigma\tau\sigma^{-1}$ where τ is an element of H. If we define a character χ^σ of $\sigma H\sigma^{-1}$ by $\chi^\sigma(\sigma\tau\sigma^{-1})=\chi(\tau)$ where χ is a character of H, we have a one-to-one correspondence between the characters of H and those of $\sigma H\sigma^{-1}$. By this correspondence, it is clear that Lemma 3 is true.

Main Theorem. Let k be an algebraic number field of finite degree, K a finite extension over k and K^* the smallest Galois extension over k which contains K. The Galois groups of K^*/k and K^*/K are denoted by G and H respectively. If H satisfies the following condition:

(I) if an element σ of G does not belong to H, then the intersection of H and $\sigma H\sigma^{-1}$ contains only the identity element,

then the quotient $\zeta_K(s)/\zeta_k(s)$ is an integral function.

Furthermore, by a theorem of Frobenius [6], all the elements of G which do not belong to any conjugate of H in G form with the identity element a normal subgroup M of G under the condition (I). If K_0 is the intermediate field corresponding to M, then we have the following equality:

$$(6) \qquad \left\{\frac{\zeta_K(s)}{\zeta_k(s)}\right\}^{[K_0:k]}=\frac{\zeta_{K^*}(s)}{\zeta_{K_0}(s)}$$

Before proving the main theorem, we shall transform the condition (I) into the conditions (II) and (III). The proof of the equivalence of the three conditions is trivial.

Theorem 1. Let k, K and K^* be the same as in the above theorem. Let α be an element of K such that $K=k(\alpha)$ and $\alpha^{(1)}=\alpha, \alpha^{(2)}, \cdots, \alpha^{(n)}$ its conjugates over k. Accordingly $K^*=k(\alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(n)})$. If α satisfies the following condition:

(II) *if $\alpha^{(i)}\neq\alpha$ (i.e. $i\neq 1$), then K^* coincides with $k(\alpha, \alpha^{(i)})$,*

then the same results as in the main theorem hold.

Theorem 2. Let $k, K, K^*, \alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(n)}$ and G be the same as in the above two theorems. If G satisfies the following condition:

(III) *if an element σ of G leaves two of $\alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(n)}$ invariant, then σ is the identity element,*

then the same results as in the main theorem hold.

As a corollary of Theorems 1 and 2, we can easily show the results proved by R. Dedekind [4] and by E. Artin [2].

Proof of the Main Theorem. H is assumed to satisfy the condition (I).

First case: The order of H is equal to 1. Then K is a Galois extension over k, and this is the case proved by H. Aramata [1] and by R. Brauer [3]. In this case, by the method of R. Brauer with Lemma 1, we can easily prove the theorem. Here the equality (6) is trivial.

Second case: The order of H is larger than 1. First we shall show that the normalizer $N(H)$ of H coincides with H. In fact, if σ is any element of $N(H)$, then $\sigma H\sigma^{-1}$ coincides with H; and consequently, by the condition (I), σ must belong to H. Thus clearly $N(H)$ coincides with H. Accordingly there are exactly $\frac{g}{h}$ different conjugates of H in G where g and h are the orders of G and H respectively. Furthermore any two of those different conjugates intersect only with the identity element each other.

Now remembering the definition of the normal subgroup M, we can divide the sum $\sum_{H_\sigma}$ in (1) as follows:

$$\sum_{H_\sigma} = \sum_{H_{\sigma_0}\subseteq H}+\sum_{H_{\sigma_1}\subseteq\tau_1 H\tau_1^{-1}}+\cdots +\sum_{H_{\sigma_{n-1}}\subseteq\tau_{n-1}H\tau_{n-1}^{-1}}+\sum_{H_\rho\subseteq M}, \tag{7}$$

where $\tau_0=1$ (identity element), $\tau_1,\cdots,\tau_{n-1}$ are the complete system of the representatives of the cosets of G by $H=N(H)$, and H_{σ_i} and H_ρ range over all the cyclic subgroups of order $h_{\sigma_i}>1$ and $h_\rho>1$ of G which are contained in $\tau_i H\tau_i^{-1}$ and M respectively. Then by (7) and Lemma 2 with (3) we can rewrite (1) as follows:

$$X(G)=\frac{h}{g}\Xi_{X(H)}+\frac{h}{g}\Xi_{X(\tau_1H\tau_1^{-1})}\cdots \tag{8}$$
$$+\frac{h}{g}\Xi_{X(\tau_{n-1}H\tau_{n-1}^{-1})}+\frac{m}{g}\Xi_{X(M)},$$

where m is the order of M. Furthermore, Lemma 3 shows

$$\Xi_{X(H)}=\Xi_{X(\tau_1H\tau_1^{-1})}=\cdots=\Xi_{X(\tau_{n-1}H\tau_{n-1}^{-1})}. \tag{9}$$

Since n is equal to $\frac{g}{h}$ exactly, we have combining (8) and (9)

$$\frac{g}{m}X(G)=\frac{g}{m}\Xi_{X(H)}+\Xi_{X(M)}. \tag{10}$$

If we consider then the Artin's L-series with the character (10) of G in the Galois extension K^*/k, we have the equality (6) easily, as $\frac{g}{m}$ is equal to $[K_0:k]$. Since K^* is a Galois extension over K_0, the right side of the equality (6) is an integral function (cf. the first case of the proof). Consequently the suitable power of the quotient $\zeta_K(s)/\zeta_k(s)$ is integral. Since this quotient is meromorphic, it must be integral. Thus the proof is completed.

Considering the residue of Dedekind's zeta-function at $s=1$, we can show, by (6), a relation between the class numbers of the four fields k, K, K_0 and K^*.

Finally I should like to remark that the main theorem proved above is the true extension of the former results, in the sense that there exist infinitely many extensions K over k such that the integrality of the quotient $\zeta_K(s)/\zeta_k(s)$ can be proved by the main theorem but not by all the former results. The Galois group G where the assumption of Theorem 2 holds is characterized by the following two conditions, if we consider G as a finite permutation group:

1) G is transitive;

2) an element of G which leaves two objects invariant is only the identity element.

Then, in order to obtain the above remark, the following three theorems are sufficient.

Theorem 3 (H. Zassenhaus [7]). A finite permutation group G satisfies the above two conditions 1) and 2) if and only if G is represented as a linear transformation group in a finite "Fastkörper".

Theorem 4 (H. Zassenhaus [7]). There exist infinitely many finite "Fastkörper" which are not finite fields $GF(p^n)$ such that the linear transformation groups in them are solvable. Furthermore, in such a group, the subgroup of all the transformations which leave a fixed object invariant is maximal.

Theorem 5 (I. R. Šafarevič [5]). Let k be an algebraic number field and G a finite solvable group. Then there exists a Galois extension K^* over k with a Galois group isomorphic to G.

References

[1] H. Aramata: Proc. Imp. Acad., **9**, 31–34 (1933).
[2] E. Artin: Math. Ann., **89**, 147–156 (1923).
[3] R. Brauer: Amer. J. Math., **121**, 243–250 (1947).
[4] R. Dedekind: Crelles J., **121**, 40–123 (1900). Collected Papers, II, 148–235.
[5] I. R. Šafarevič: Izv. Akad. Nauk, SSSR, Ser. Math., **18**, 525–578 (1954).
[6] A. Speiser: Theorie der Gruppen von endlicher Ordnung, p. 144.
[7] H. Zassenhaus: Abh. Math. Sem. Univ. Hamburg, **11**, 187–220 (1936).