ON POWER CHARACTERS IN CYCLOTOMIC FIELDS

BY H. S. VANDIVER

1. *Introduction.* In a previous paper,[*] I considered power characters in the field $K(\zeta)$; $\zeta = e^{2i\pi/l}$, where l is an odd prime. We write

$$\omega^{(N(\mathfrak{p})-1)/l} \equiv \zeta^a \pmod{\mathfrak{p}},$$

where ω is an integer in $K(\zeta)$; $\mathfrak{p}$ is an ideal in that field with ω and $\mathfrak{p}$ prime to l. Moreover,

$$\{\omega/\mathfrak{p}\} = \left\{\frac{\omega}{\mathfrak{p}}\right\} = \zeta^a$$

in the case where the field $K(\zeta)$ is properly irregular, that is, when the second factor of the class number of $K(\zeta)$ is prime to l. An explicit algebraic expression was found for a in the above relation provided ω was a unit in the field. This expression had been well known in the case where $\mathfrak{p}$ belonged to an exponent prime to l. In the same paper (pp. 400–401) an explicit expression was found for the symbol $\{\theta/\mathfrak{q}\}$, where θ is an integer and $\mathfrak{q}$ is a prime ideal in $K(\zeta)$ prime to l; also $\theta = \mathfrak{a}^l$, where $\mathfrak{a}$ is a prime ideal in the same field. These ideas appear quite novel in this connection and they possibly constitute the germs of an extension of the theory of relative abelian fields.

One aspect of the matter is the following. If $\theta = \alpha^l$, then we have the trivial conclusion that

$$\{\theta/\mathfrak{q}\} = 1.$$

The result we have been discussing is an extension of the one just mentioned since θ is the lth power of an ideal which is not necessarily principal. The value of the power characters involving θ depended upon those involving ω, where ω is a unit, and these in turn depended upon the following relation due to Kummer:

$$(1)\ \operatorname{ind} E_n \equiv \frac{r^{2n}-1}{2(1+a^{l-2n}-(a+1)^{l-2n})}\cdot\frac{d_0{}^{l-2n}\log\psi_a(e^v)}{dv^{l-2n}} \pmod{l},$$

[*] Transactions of this Society, vol. 32 (1930), pp. 391–408.

where

$$\left\{\frac{E_n}{\mathfrak{q}}\right\} = \zeta^{\operatorname{ind} E_n},$$

a is a rational integer, $0 < a < l-1$, r is a primitive root of l,

$$\psi_a(x) = \sum_h x^{-(a+1)h + \operatorname{ind}(g^h+1)},$$

x is arbitrary, $\mathfrak{q}$ is an ideal prime in $k(\zeta)$ whose norm is q^t, g is a primitive root of $\mathfrak{q}$, h ranges over the integers $0, 1, 2, \cdots, q^t-2$, excepting $(q^t-1)/2$ if q is odd and excepting zero if q is even. The primitive root g is selected so that

$$g^{(q^t-1)/l} \equiv \zeta \pmod{\mathfrak{q}}.$$

If

$$g^h + 1 \equiv g^k \pmod{\mathfrak{q}},$$

$0 < k < q^t - 1$, then we write

$$\operatorname{ind}(g^h + 1) = k.$$

The symbol

$$\frac{d_0{}^{l-2n} \log \psi_a(e^v)}{dv^{l-2n}}$$

means that the $(l-2n)$th derivative of log $\psi_a(e^v)$ is taken with respect to v and $v=0$ substituted in the result, e being the Napierian base. Further a is selected so that

$$1 + a^{l-2n} - (a+1)^{l-2n}$$

is prime to l. Also

$$E_n = \epsilon^R,$$

$$R = (1 + sr^{-2n} + s^2r^{-4n} + \cdots + s^{(l-3)/2}r^{-n(l-3)})r^l,$$

the symbol s representing the substitution (ζ/ζ^r) in the notation of the Kronecker-Hilbert symbolic powers, r is a primitive root of l, and

$$\epsilon = \left(\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}\right)^{1/2}.$$

The writer* extended (1) to the case of lth power characters in a field defined by (ln)th roots of unity, n prime to l.

In the present paper several different types of extensions of the above results will be considered. The proofs, in the main, will be indicated only.

2. *Power Characters.* In the first place, if n is an odd prime distinct from l and

$$\beta = e^{2i\pi/n},$$

then we may consider $\left\{\omega/\mathfrak{A}\right\}$, where

$$\omega = \frac{1-\beta^l}{1-\beta}\cdot$$

To find expressions involving this power character we employ the Lagrange resolvent form

$$\begin{aligned} F(u,\ x) &= \eta + u\eta_1 + u^2\eta_2 + \cdots + u^{\lambda-1}\eta_{\lambda-1}, \\ \lambda &= ln, \\ \eta_k &= x^{g^k} + x^{g^{\lambda+k}} + \cdots + x^{g^{(\nu-1)\lambda+k}}, \end{aligned}$$

where q is the norm of $\mathfrak{q}$ in $k(\alpha\beta)$ and a prime of the form $ln\nu+1$, $x^q=1$, $x\neq 1$, and g is a primitive root of q. Consider $F(u,\ x)F(u^{-1},\ x)$, where u is arbitrary. We find

$$F(u,\ x)\,F(u^{-1},\ x) = -\,V\frac{u^\lambda-1}{u-1} + q + X_1(u^\lambda - 1),$$

where X_1 is a polynomial in u with integral coefficients. We set $u=\beta e^v$ in the above expression. By a method analogous to that employed previously by the writer (loc. cit., p. 143), we have

$$\begin{aligned} \frac{d_0{}^l \log F(e^v\beta,\ x)}{dv^l} &\equiv f_l(\beta)f_0(\beta^{-1}) - (l-1)f_{l-1}(\beta)f_1(\beta^{-1}) \\ &\quad + \cdots + f_1(\beta)f_{l-1}(\beta^{-1}) \pmod{l}, \end{aligned}$$

where

$$f_s(\beta) = \eta_1\beta + 2^s\eta_2\beta^2 + \cdots + (\lambda-1)^s\eta_{\lambda-1}\beta^{\lambda-1}.$$

* American Journal of Mathematics, vol. 47 (1925), pp. 140–147.

The right-hand expression may then be written in the form

$$\sum_{i=0}^{\lambda-1}\sum_{k=0}^{\lambda-1}\beta^{i-k}i(k-1)^{l-1}\eta_i\eta_k.$$

Writing k for $k-1$, we obtain

$$\tag{2} \begin{aligned} s &= \sum_{s=1}^{n-1}\frac{d_0{}^l\log F(e^v,\beta^s x)}{dv^l} \\ &\equiv \sum_{s=1}^{n-1}\sum_{i=0}^{\lambda-1}\sum_{k=0}^{\lambda-1}\beta^{-ks}ik^{l-1}\eta_i\eta_{k+1}. \end{aligned}$$

By a method similar to that used by Kummer,* we find

$$\tag{3} s \equiv n(n-1)I(l) \pmod{l},$$

where

$$\left\{\frac{\theta}{\mathfrak{q}}\right\} = \zeta^{I(\theta)}.$$

From (2) we also have

$$\tag{4} \begin{aligned} s_1 &= \sum_{s=1}^{n-1}\beta^{cs}\frac{d_0{}^l\log F(e^v,\beta^s x)}{dv^l} \\ &\equiv \sum_{s}\sum_{i}\sum_{k}\beta^{(-k+c)s}ik^{l-1}\eta_i\eta_{k+1}, \end{aligned}$$

which gives, after some transformations,

$$\tag{5} s_1 \equiv I\left(\frac{1-\beta^{cl}}{1-\beta^c}\right) - \frac{1}{n}I(l) \pmod{l}.$$

From (2), (3), (4), and (5), we have the relations from which we can derive expressions involving σ, where $\mathfrak{q}^{l^s n} = (\sigma)$, by factoring the Lagrange resolvent into its prime factors, as did Kummer,† and proceeding as in the writer's paper. Similarly, by these methods we may find analogous expressions for the power characters of certain units with respect to $\mathfrak{p}$ from other relations given by the writer.

* Journal für Mathematik, vol. 44 (1851), p. 100.

† Loc. cit., p. 103.

3. *Extensions.* We shall now indicate how to obtain an extension of (1) for l^nth power characters. If θ is an integer in the field $K(\zeta_n)$, where

$$\zeta_n = e^{2i\pi/l^n},$$

which is prime to $1-\zeta_n$, and $\mathfrak{p}$ is an ideal in $K(\zeta_n)$ prime to θ, then

$$\theta^{(N(\mathfrak{p})-1)/l^n} \equiv \left\{\frac{\theta}{\mathfrak{p}}\right\}_n \pmod{\mathfrak{p}},$$

where $\{\theta/\mathfrak{p}\}_n$ is a power of (ζ_n) and $N(\mathfrak{p})$ is the norm of $\mathfrak{p}$ in $k(\zeta_n)$. To effect this we extend the methods of Kummer.* Set $\lambda = l^n$, and write

$$\psi_r(\zeta) = \sum \zeta^{-(n+1)h+\operatorname{ind}(g^h+1)},$$
$$r+1 \not\equiv 0 \pmod{\lambda}, \qquad r \not\equiv 0 \pmod{\lambda},$$

where the summation extends over the values $h=0, 1, 2, \cdots, q^t-2$, with the exception

$$\frac{q^t-1}{2}$$

if q is odd and zero if q is even, q being a prime such that q belongs to the exponent t modulo λ. Further, g is a primitive root of $\mathfrak{q}$, where $\mathfrak{q}$ is a prime ideal factor of q which is selected so that

$$g^{(q^t-1)/\lambda} \equiv \zeta_n \pmod{\mathfrak{q}}.$$

The symbol ind (g^h+1) stands for an integer k in the relation

$$(g^h+1) \equiv g^k \pmod{\mathfrak{q}}.$$

This function has the property proved by Mitchell:†

$$\psi_r(\zeta)\psi_r(\zeta^{-1}) = q^t.$$

The method of proof employed there shows that in lieu of the above relation we may write an identity in the form

$$\psi_r(x)\psi_r(x^{l-1}) = q^t + V(x)W(x), \tag{6}$$

where $V(x) = 1+x+x^2+\cdots+x^{\lambda-1}$. Consider

* Loc. cit., p. 103.

† Transactions of this Society, vol. 17 (1916), pp. 165–177.

$$\frac{d^{m+1}\log\psi_r(e^v)}{dv^{m+1}} = \frac{d^m\left(\frac{d\psi_r(e^v)}{dv}\cdot\frac{1}{\psi_r(e^v)}\right)}{dv^m}.$$

If we set

$$\frac{1}{\psi_r(e^v)} = u,$$

then we have by Leibnitz's theorem

$$\frac{d^{m+1}\log\psi_r(e^v)}{dv^{m+1}} = \frac{d^{m+1}\psi_r(e^v)}{dv^{m+1}}u + \frac{m}{1}\,\frac{d^m\psi_r(e^v)}{dv^m}\,\frac{du}{dv} + \cdots . \tag{7}$$

Now set $x=e^v$ in (6). We have

$$\frac{d^i\psi_r(e^{-v})}{dv^i} = \frac{d^iu}{dv^i}(q^t + VW) + \frac{i}{1}\,\frac{d^{i-1}u}{dv^{i-1}}\,\frac{d(VW)}{dv} + \cdots .$$

Set $v=0$ in this relation. Then V and all its derivatives except those of orders which are multiples of $l-1$ are divisible by λ.

By a special treatment of the derivatives of orders which are multiples of $(l-1)$ of (VW) we obtain from the last relation

$$\frac{d_0{}^i u}{dv^i} \equiv (-1)^i\frac{d_0{}^i\psi_r(e^v)}{dv^i} \equiv (-1)^iD_i \pmod{\lambda},$$

from which

$$\frac{d_0{}^{m+1}\log\psi_r(e^v)}{dv^{m+1}} \equiv D_{m+1}D_0 - \frac{m}{1}D_mD_1 + \frac{m(m-1)}{1\cdot 2}D_{m-1}D_2 - \cdots , \pmod{\lambda}.$$

Proceeding as Kummer* did in the special case, we obtain

$$\frac{d_0{}^{m+1}\log\psi_r(e^v)}{dv^{m+1}} \equiv (1 + r^{m+1} - (r+1)^{m+1}) \cdot\sum_h h^m \operatorname{ind}(g^h - 1) \pmod{\lambda} \tag{8}$$

* Loc. cit., pp. 125–130.

for $h=1, 2, 3, \cdots, q^t-2$. The right-hand member of this may be transformed into an expression involving units in the field $k(\zeta_n)$ if we note that

$$\sum_h h^m \operatorname{ind}(g^h - 1) \equiv \sum_i \sum_k i^m \operatorname{ind}(g^{i+k\lambda} - 1)$$

for $i=1, 2, 3, \cdots, \lambda-1$; $k=0, 1, 2, \cdots, \nu-1$, where

$$\nu = \frac{q^t - 1}{\lambda}.$$

We also have

$$(q^i - 1)(g^{i+\lambda} - 1)(g^{i+2\lambda} - 1) \cdots (g^{i+(\nu-1)\lambda} - 1) \equiv 1 - g^{\nu i} \pmod{\mathfrak{q}}$$

and

$$\sum \operatorname{ind}(g^{i+k\lambda} - 1) \equiv \operatorname{ind}(1 - g^{\nu i}) \equiv \operatorname{ind}(1 - \zeta_n^i) \pmod{l},$$

since $g^\nu \equiv \zeta_n \pmod{\mathfrak{q}}$. Carrying out the summation with respect to k, we have

$$\sum h^m \operatorname{ind}(g^h - 1) \equiv \sum_i i^m \operatorname{ind}(1 - \zeta_n^i)$$

for $i=1, 2, 3, \cdots, \lambda-1$. Setting $i\gamma$ in place of i, multiplying by γ^{-m} and subtracting the original from the second congruence, we have

$$(\gamma^{-m} - 1) \sum h^m \operatorname{ind}(g^h - 1) \equiv \sum i^m \operatorname{ind}\left(\frac{1 - \zeta_n^{\gamma i}}{1 - \zeta_n^i}\right).$$

Applying this to (8) we have an extension of (1).

THE UNIVERSITY OF TEXAS