ON POWER CHARACTERS OF SINGULAR INTEGERS IN A PROPERLY IRREGULAR CYCLOTOMIC FIELD*

BY

H. S. VANDIVER

Let

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

where l is an odd prime and let $\mathfrak{p}$ be a prime ideal in the field $k(\zeta)$ and ω an integer in the field with $\mathfrak{p}$ and ω prime to l. Then there exists an integer a such that, if $N(\mathfrak{p})$ is the norm of $\mathfrak{p}$,

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

and we write

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

The symbol on the left is termed a power character. The integer ω is congruent to the lth power of an integer in the field $k(\zeta)$ modulo $\mathfrak{p}$ if, and only if,

$$\left\{\frac{\omega}{\mathfrak{p}}\right\} = 1.$$

If

$$\mathfrak{P} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_s$$

then

$$\left\{\frac{\omega}{\mathfrak{P}}\right\} = \left\{\frac{\omega}{\mathfrak{p}_1}\right\}\left\{\frac{\omega}{\mathfrak{p}_2}\right\} \cdots \left\{\frac{\omega}{\mathfrak{p}_s}\right\}.$$

For the case where ω is a unit in $k(\zeta)$ these power characters were considered by Kummer† who gave among other results the relation (1) below. Kummer also‡ gave the following theorem:

If $\mathfrak{p}$ and $\mathfrak{q}$ are different from each other and from $\lambda = (1-\zeta)$ and are both prime ideals in the regular cyclotomic field $k(\zeta)$, then

$$\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}.$$

The symbol $\{\mathfrak{p}/\mathfrak{q}\}$ is defined as follows:

$$\mathfrak{p}^{h h_1} = (\pi),$$

* Presented to the Society, August 29, 1929; received by the editors in January, 1930.

† Journal für Mathematik, vol. 44 (1852), pp. 121–130; Vandiver, Annals of Mathematics, vol. 30 (1929), pp. 487–491.

‡ Berichte der Akademie der Wissenschaften zu Berlin, 1858, 1859, 1861; Hilbert, *Bericht über die Theorie der Algebraischen Zahlkörper*, p. 471.

where $h\ h_1 \equiv 1 \pmod{l}$ and π is an integer in $k(\zeta)$, h being the class number of $k(\zeta)$; then

$$\{\mathfrak{p}/\mathfrak{q}\} = \left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = \left\{\frac{\pi}{\mathfrak{q}}\right\}.$$

Further π is selected to be primary. A regular cyclotomic field is one in which h is prime to l.

In 1909 Furtwängler proved that

$$\left\{\frac{\alpha}{\beta}\right\} = \left\{\frac{\beta}{\alpha}\right\}$$

where α and β are integers in a field K prime to each other and to l, at least one being primary, the said field K including the field $k(\zeta)$.

Takagi* proved that the value of the symbol $\{\mu/\mathfrak{r}\}$ depends only upon the ideal class modulo $\mathfrak{f}$ to which the ideal $\mathfrak{r}$ belongs, where $\mathfrak{f}^{l-1}$ is the relative discriminant of the field K, with respect to k. In the above theorem μ is an integer in a field which contains $k(\zeta)$ and $\mathfrak{r}$ is an arbitrary ideal prime to l in this field. Two ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are said to belong to the same class modulo $\mathfrak{f}$ if, and only if, two integers γ_1 and γ_2 exist such that $\gamma_1\mathfrak{a}_1 = \gamma_2\mathfrak{a}_2$ with $\gamma_1 \equiv \gamma_2 \pmod{\mathfrak{f}}$. Other theorems concerning power characters have been given, but reference to the above will be sufficient to indicate the character of the results given in the present paper.

In the first place we may note that Furtwängler's result is not a direct generalization of Kummer's law of reciprocity, as the symbol $\{\mathfrak{p}/\mathfrak{q}\}$ is not employed in the general field; in fact it is not defined when $\mathfrak{p}$ belongs to an exponent which is a multiple of l. Furtwängler's result may be deduced from Takagi's, quoted above, the latter result obviously giving us information concerning the power character of $\{\mu/\mathfrak{r}\}$ when $\mathfrak{r}$ belongs to an exponent which is a multiple of l, as well as all other types of ideals.

The proofs of the results of Furtwängler and Takagi are extremely long and complicated. It seems to me possible that simpler proofs might be obtained for the cyclotomic field at least by introducing new points of view into the theory of the power characters in the cyclotomic field itself. Having this in view, in the present paper I shall show how the value of the symbol $\{\mu/\mathfrak{r}\}$ may be completely determined where μ is an integer and $\mathfrak{r}$ any ideal in the field $k(\zeta)$, the integer μ being singular and $k(\zeta)$ being properly irregular. A cyclotomic field $k(\zeta)$ is said to be properly irregular if it is irregular and none of the units E_i, $i=1, 2, \cdots, (l-3)/2$, is the lth power of a unit in $k(\zeta)$, where $E_n = \epsilon^R$;

* Journal of the College of Science of Tokio University, 1922, §5, p. 39.

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

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

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

Also the integer ω in $k(\zeta)$ is said to be singular, if and only if (ω) is the lth power of an ideal $\mathfrak{j}$ in $k(\zeta)$ but $\mathfrak{j}$ is not a principal ideal.

In this type of field it will first be necessary to determine the value of the symbol $\{\omega/\mathfrak{p}\}$ where ω is a unit in $k(\zeta)$ and $\mathfrak{p}$ is an arbitrary ideal in $k(\zeta)$ prime to l. The germ of the method I shall employ to accomplish this is due to Kummer who, in his 1857 Memoir on Fermat's last theorem,* found the value of

$$\left\{\frac{E_n}{\mathfrak{p}}\right\},$$

where the class number of $k(\zeta)$ was divisible by l and not by l^2 and B_n was the single Bernoulli number in the set $B_1, B_2, \cdots, B_{(l-3)/2}$ which was divisible by l; $B_1=1/6$, $B_2=1/30$, etc.; $\mathfrak{p}$ was an arbitrary ideal in the field. However, during the course of this proof Kummer employed without proof or reference the relation

$$\frac{d_0^{ml^i}\log\phi(e^v)}{dv^{ml^i}}\equiv\frac{d_0^{ml^i}\log\phi_1(e^v)}{dv^{ml^i}}\pmod{l^{i+1}},$$

where m is not a multiple of $l-1$ and the subscript zero of d indicates that $v=0$ is substituted in the result after the operations are performed. Also ϕ and ϕ_1 are polynomials in e^v with rational integral coefficients and $\phi(\zeta)=\phi_1(\zeta)$.†

I encountered the principal difficulty in carrying through this investigation in connection with this unproved statement of Kummer; in fact, I have been able to establish it only under restrictions (cf. Lemma 2).

Concerning properly irregular cyclotomic fields, it should be noted that through some computations carried out recently by Miss E. T. Stafford and the writer it was found that the fields defined by $l=37$, 59, 67, 101, 103,

* Berlin Abhandlungen, Mathematisch-Physikalische Klasse, 1857, pp. 41–74.

† Several of the devices employed in my method for deriving this result, under restrictions, are not used by Kummer in any of his papers and I have no idea of the method he used if he really possessed a proof. It is possible that he employed the erroneous formula obtained by him and quoted on page 45, (7a), of the report on *Algebraic Numbers*, II, Bulletin, National Research Council, February, 1928, as differential coefficients, of the type used in the theorem under discussion, appear therein.

131, 149 and 157 are properly irregular. The work was carried through for all primes l less than 200. No irregular fields other than properly irregular fields were discovered.

The theorem of Kummer's, given in the first article of his quoted in the present paper, is as follows:

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

where

$$\left\{\frac{E_n}{\mathfrak{q}}\right\} = \zeta^{\text{ind}E_n};$$

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

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

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

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

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. It is known that

$$\text{(2)} \qquad \psi_a(\zeta) = \prod \mathfrak{q}_c,$$

where c ranges over the integers

$$cc_1 \equiv 1 \pmod{l},$$

and

$$|ac_1| + |c_1| > l,$$

$|x|$ is the least positive residue of x modulo l, and c_1 is in the set $1, 2, \cdots, l-1$. Also, the $\mathfrak{q}_c$ represents the ideal obtained from $\mathfrak{q}$ by the substitution (ζ/ζ^c). Assume that $\mathfrak{q}$ belongs to the exponent jl^{i-1}, where j is prime to l and $i>1$, so that $\mathfrak{g}^{jl^{i-1}(l-1)} = (\omega)$, where ω is an integer in $k(\zeta)$ such that

$\omega \equiv 1 \pmod{(1-\zeta)}$. Raising both sides of (2) to the power $jl^{i-1}(l-1)$ we obtain

$$(\psi_a(\zeta))^{jl^{i-1}(l-1)} = \eta \prod_c \omega_c,$$

where n is a unit in $k(\zeta)$. Let t be a positive integer such that $x^t\psi_a(x) = \psi_a'(x)$ is a polynomial in x. Then

$$\sum_h \zeta^{-(a+1)h+\operatorname{ind}(g^h+1)+t}$$

is a polynomial in ζ, and if ω_c is obtained from ω by the substitution (ζ/ζ^c) then

$$(\psi_a'(\zeta))^{jl^{i-1}(l-1)} = \eta \prod_c \omega_c. \tag{2a}$$

Now $\omega_c \equiv 1 \pmod{(1-\zeta)}$ and if

$$\omega_c = d_0 + d_1\zeta + \cdots + d_{l-2}\zeta^{l-2}$$

with the d's rational integers, we write

$$\omega_c(x) = d_0 + d_1x + \cdots + d_{l-2}x^{l-2} + \frac{1 - (d_0 + d_1 + \cdots + d_{l-2})}{l} \cdot \frac{x^l - 1}{x - 1}. \tag{2b}$$

Raise both sides of (2a) to the power l. We may then apply Lemma 2 (which is proved later) to the resulting relation, noting that $(\psi_a'(1))^{jl^i(l-1)} \equiv 1 \pmod{l^{i+1}}$; $\omega_c(\zeta) = \omega_c$; $\omega_c(1) = 1$ and if $m \not\equiv 0 \pmod{(l-1)}$ we obtain, after dividing through by l,

$$\begin{aligned}(l-1)jl^{i-1}\frac{d_0^{ml^i}\log\psi_a'(e^v)}{dv^{ml^i}} &\equiv (l-1)jl^{i-1}\frac{d_0^{ml^i}\log\psi(e^v)}{dv^{ml^i}} \\ &\equiv \sum_c \frac{d_0^{ml^i}\log\omega_c(e^v)}{dv^{ml^i}} \pmod{l^i},\end{aligned} \tag{3}$$

and using a relation which I have proved in another paper* we obtain

$$\sum_c \frac{d_0^{ml^i}\log\omega_c(e^v)}{dv^{ml^i}} \equiv \sum_c c^{ml^i}\frac{d_0^{ml^i}\log\omega(e^v)}{dv^{ml^i}} \pmod{l^i}. \tag{3a}$$

The expression $\sum_c c^{ml^i}$ may be reduced as follows. Consider

$$\sum_{h=1}^{l-1} \frac{|ah| + |h| - |(a+1)h|}{l} h^{ml^i} = L,$$

* These Transactions, vol. 31 (1929), p. 619, relation (3e).

which is readily seen to equal $\sum c_1 m l^i$ where c_1 ranges over those integers satisfying $|ac_1|+|c_1|>l$ in the set $1, 2, \cdots, l-1$. Now

$$|ah| = ah + lw,$$

where w is a rational integer and

$$(ah)^{l^i m} \equiv |ah|^{l^i m} \pmod{l^{i+1}},$$

whence

$$h^{l^i m} \equiv (a)^{-l^i m + l^i(l-1)} |ah|^{l^i m} \pmod{l^{i+1}}.$$

Similarly we have

$$(h)^{l^i m} = |h|^{l^i m} \pmod{l^{i+1}}.$$

Hence

$$h^{l^i m} \equiv (a+1)^{l^i(l-1)-l^i m} |(a+1)h|^{l^i m} \pmod{l^{i+1}}.$$

Writing $b = l^i(l-1) - l^i m$, we obtain from the last two relations after dividing through by l and noting that

$$\sum_h |ah| = 1 + 2 + \cdots + (l-1)$$

and similarly for $|h|$ and $|(a+1)h|$,

$$L \equiv \frac{a^b + 1 - (a+1)^b}{l} \sum_{n=1}^{l-1} n^{l^i m + 1} \pmod{l^i}.$$

Set

$$d = ml^i + 1.$$

We shall now prove the relation

(3b) $$S_d(l) \equiv (-1)^{d/2-1} l B_{d/2} \pmod{l^{i+2}},\ l > 3,$$

where

$$S_d(l) = 1^d + 2^d + \cdots + (l-1)^d.$$

We have

$$S_d(l) = lb_d^* + l\binom{d}{2}(lb_{d-1}^*) + l^2 \frac{d(d-1)}{2 \cdot 3}(lb_{d-2}^*) + \cdots + l\frac{l^{r-1}}{r+1}\binom{d}{r}(lb_{d-r}^*) + \cdots,$$

where

$$b_{2a} = (-1)^{a-1} B_a,\ b_{2a+1}^* = 0,\ a > 0.$$

Consider the general term in this expansion. The numerator in the binomial coefficient is divisible by l^i. We shall now show that

$$\frac{l^{r-1}}{(r+1)!}$$

is a fraction whose numerator is divisible by l, for, by a known result, if l^μ is the highest power of the prime l which divides factorial $r+1$ then

$$\mu = \frac{r+1-s}{l-1},$$

where $s=a_0+\cdots+a_n$ is the sum of the digits of $r+1$ to the base l,

$$r+1 = a_0 l^n + a_1 l^{n-1} + \cdots + a_n \qquad (0 \leqq a_1 < l).$$

Hence we have to show that

$$r-1 > \frac{r+1-s}{l-1}.$$

We have $(l-2)r>l-s$. Transposing $-r$ to the right hand member and also adding $1-l$ to each member, we obtain our results after dividing through by $l-1$. Hence (3b) follows if we note that the second term in the expansion is zero and $l>3$, and also by the von-Staudt-Clausen theorem lb^*_{-r} is a fraction whose denominator is prime to l; and applying (3b) to the congruence involving L we obtain

$$L \equiv ((a+1)^b - a^b - 1)(-1)^{d/2-1} B_{d/2} \pmod{p^i}.$$

We have

$$cc_1 \equiv 1 \pmod{l}.$$

Write

$$cc_1 = 1 + wl,$$

hence

$$\frac{1}{c^{ml^i}} \equiv (c_1)^{ml^i} \pmod{l^{i+1}},$$

and

$$c^{ml^i} \equiv (c_1)^b \pmod{l^{i+1}},$$

hence

$$\sum_m c^{ml^i} \equiv ((a+1)^{ml^i} - a^{ml^i} - 1)(-1)^{(b+1)/2} B_{(b+1)/2} \pmod{l^i}.$$

Consider (3a) and substitute the value which is obtained for $\sum_c c^{ml^i}$. We have

$$\sum_c \frac{d_0^{ml^i} \log \omega_c(e^v)}{dv^{ml^i}} \equiv ((a+1)^{l^i m} - a^{l^i m} - 1) \cdot (-1)^{(b+1)/2} B_{(b+1)/2} \frac{d_0^{ml^i} \log \omega(e^v)}{dv^{ml^i}} \pmod{l^i}. \tag{4}$$

The writer has proved† that

$$\frac{(n^i - 1)\sum_{a=1}^{p-1} a^i}{p} = \sum_{a=1}^{p-1} \sum_{s=1}^{i} \binom{i}{s} \left(\frac{y_a}{a}\right)^s p^{s-1} a^i,$$

where i is an arbitrary integer, n is an integer prime to the prime p and not unity, and

$$y_a \equiv -\frac{a}{p} \pmod{n} \quad (0 \leqq y_a < n).$$

Put $i=(b+1)$ in this relation; we obtain, as in the proof of (3b), if $p=l$

$$\frac{(n^{b+1} - 1)\sum_{a=1}^{l-1} a^{b+1}}{l(b+1)} \equiv \sum_{a=1}^{l-1} y_a a^b \pmod{l^{i+1}}.$$

Using (3b) in this relation, we obtain

$$(n^{b+1} - 1)(-1)^{(b-1)/2} B_{(b+1)/2} \equiv \sum_{a=1}^{l-1} y_a a^b \pmod{l^i}. \tag{5}$$

In a similar way we have, using (3b) and setting

$$s = l^{i-1}(l-1) - l^{i-1}m,$$

$$(n^{s+1} - 1)(-1)^{(s-1)/2} B_{(s+1)/2} \equiv (s+1)\sum_{a=1}^{l-1} y_a a^s \pmod{l^i}.$$

Subtracting this relation from (5) we obtain

$$(-1)^{(b-1)/2} B_{(b+1)/2} \equiv \frac{(-1)^{(s-1)/2} B_{(s+1)/2}(n^{s+1} - 1)}{(s+1)(n^{b+1} - 1)} \pmod{l^i}.$$

Using (4) in connection with the above relation and noting that $n^{s+1}-1 \equiv n^{b+1}-1 \pmod{l^i}$ we obtain

$$\frac{d_0^{ml^i} \log \psi_a(e^v)}{dv^{ml^i}} \equiv \frac{a^{l^i m} + 1 - (a+1)^{l^i m}}{j} \cdot (-1)^{(s-1)/2} \frac{B_{(s+1)/2} d_0^{ml^i} \log \omega(e^v)}{l^{i-1} dv^{ml^i}} \pmod{l}. \tag{5a}$$

† Annals of Mathematics, vol. 18 (1917), p. 112, relation (7a).

In this relation set $i+1$ in place of i. Now if we put

$$D(\omega) = \frac{d\omega(e^v)}{dv}$$

then

$$\frac{d^{ml^{i+1}} \log \omega(e^v)}{dv^{ml^{i+1}}} \equiv \frac{d^{ml^{i+1}-1}}{dv^{ml^{i+1}-1}} \left(\frac{D(\omega)}{\omega(e^v)}\right).$$

We shall consider

$$\frac{d^{ml^{i+1}-1}}{dv} \left(\omega(e^v)^{l^{i+1}} \cdot \frac{D(\omega)}{\omega(e^v)}\right).$$

Carrying out the differentiation of this fraction considered as a product, by Leibnitz's theorem, we have

$$\left[\frac{d^k(\omega(e^v)^{l^{i+1}})}{dv^k}\right]_{v=0} \equiv 0 \pmod{l^{i+1}},$$

and therefore, since $[\omega(e^v)]_{v=0} \equiv 1 \pmod{l}$,

$$\frac{d^{ml^{i+1}-1}}{dv^{ml^{i+1}-1}} \left[\frac{D(\omega)}{\omega(e^v)}\right]_{v=0} \equiv \left[\frac{d^{ml^{i+1}-1}}{dv} ((\omega(e^v))^{l^{i+1}-1} D(\omega))\right]_{v=0} \pmod{l^{i+1}}.$$

The expression in the large parenthesis on the right is a polynomial in e^v with rational integral coefficients, say

$$f_0 + f_1 e^v + f_2 e^{2v} + \cdots + f_k e^{kv},$$

hence the right hand member may be written

$$f_1 + 2^{ml^{i+1}-1} f_2 + \cdots + k^{ml^{i+1}-1} f_k.$$

Hence

$$\left[\frac{d^{ml^i} \log \omega(e^v)}{dv^{ml^i}}\right]_{v=0}$$

is congruent (mod l^{i+1}) to

$$f_1 + 2^{ml^i-1} f_2 + \cdots + k^{ml^i-1} f_k,$$

and since if s is a rational integer

$$s^{ml^i-1} \equiv s^{ml^{i+1}-1} \pmod{l^{i+1}},$$

we have

$$\frac{d_0^{ml^i} \log \omega(e^v)}{dv^{ml^i}} \equiv \frac{d_0^{ml^{i+1}} \log \omega(e^v)}{dv^{ml^{i+1}}} \pmod{l^{i+1}}.$$

In a similar way we find

$$\frac{d_0^{ml^i}\log\psi_a(e^v)}{dv^{ml^i}} \equiv \frac{d_0^m\log\psi_a(e^v)}{dv^m} \pmod{l}.$$

Using these relations together with (1) and (5a) we have the

THEOREM. *We have the relation*

$$\text{ind } E_n \equiv \frac{r^{2n}-1}{2j}(-1)^{(s-1)/2}\frac{B_{(s+1)/2}d_0^{(l-2n)l^i}\log\omega(e^v)}{l^i dv^{(l-2n)l^i}} \pmod{l} \tag{6}$$

where

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

r is a primitive root of l, $\mathfrak{q}$ is a prime ideal in the field $k(\zeta)$ belonging to the exponent jl^i; $s=(2n-1)l^i$; j prime to l;

$$\mathfrak{q}^{jl^i(l-1)} = (\omega);$$

$$\omega \equiv 1 \pmod{\lambda};\ \lambda = (1-\zeta);\ i > 0;$$

the B's are the Bernoulli numbers, $B_1=1/6$, $B_2=1/30$ etc. The symbol

$$\frac{d_0^a f(e^v)}{dv^a}$$

indicates that $v=0$ is substituted in the ath derivative of $f(e^v)$ with respect to v, and $\omega(e^v)$ is defined as in (2b).

The case where $i=0$ is disposed of in the first paper of Kummer's referred to in the present article. By means of these several results we may determine the value of the symbol $\{\eta/\mathfrak{q}\}$ where η is any unit in $k(\zeta)$ and $\mathfrak{q}$ is any ideal prime to l in $k(\zeta)$, since the units e_i, $i=1, 2, \cdots, (l-3)/2$, constitute an independent system of units, that is, there exists an integer t such that η can be expressed as the products of integral powers of the E's. Since the field $k(\zeta)$ is properly irregular we may select t to be prime to l. Hence (6) enables us to determine the value of the symbol.

Suppose now that θ is a singular integer in $k(\zeta)$ which is not necessarily a unit. Since the field is properly irregular, the second factor of the class number is prime to l so that if $\mathfrak{q}$ is a prime ideal in $k(\zeta)$ prime to θ and l, then

$$(\mathfrak{q}\mathfrak{q}_{-1})^g = (\xi),$$

where ξ is an integer in $k(\zeta)$ and g is a rational integer prime to l. Hence by Furtwängler's law of reciprocity we have, if $\mathfrak{l}=(1-\zeta)$,

$$\left\{\frac{\theta}{qq_{-1}}\right\}^{\sigma} = \left\{\frac{\xi, \theta}{1}\right\}\left\{\frac{\xi}{\theta}\right\} = \left\{\frac{\xi, \theta}{\ }\right\}. \tag{7}$$

To reduce the symbol

$$\left\{\frac{\theta}{qq_{-1}}\right\}$$

we note that this may be written as

$$\left\{\frac{\theta}{q}\right\}\left\{\frac{\theta_{-1}}{q}\right\}^{-1}.$$

But since

$$\theta\theta_{-1} = \eta\lambda^{l}$$

where η is a unit in $k(\xi)$ and λ an integer in that field, we have

$$\theta_{-1} = \eta\lambda_1^{l}\theta^{l-1},$$

so that (7) gives

$$\left\{\frac{\theta}{q}\right\}^{2\sigma} = \left\{\frac{\xi, \theta}{1}\right\}\left\{\frac{\eta}{q}\right\}$$

and the last symbol on the right hand side is determined by means of (6); hence $\{\theta/q\}$ is completely determined.

We now consider

LEMMA I. *If A_r represents the sum of terms of the type*

$$cu^{ap^r}v^{bp^r},$$

where a, b and c are rational integers, p is a prime integer, then

$$(u + v)^{p^i s} = A_i + pA_{i-1} + p^2A_{i-2} + \cdots + p^iA_0,$$

where i and s are rational integers.

We may prove this result by means of the following theorem given by Kummer*:

The highest power p^N of p dividing the binomial coefficient

$$\frac{(A + B)!}{A!B!}$$

is given by

$$N = \epsilon_0 + \epsilon_1 + \cdots + \epsilon_l,$$

* Journal für Mathematik, vol. 9 (1832), p. 73; cf. also Stern, vol. 12 (1834), p. 288; Dickson, *History of the Theory of Numbers*, vol. I, p. 270–71; proof of Kummer corrected by Mitchell, these Transactions, vol. 17 (1916), pp. 170–72.

where the ϵ's are determined as follows. Set

$$A = a_0 + a_1 p + \cdots + a_l p^l,$$
$$B = b_0 + b_1 p + \cdots + b_l p^l,$$

where the A's and B's belong to the set $0, 1, \cdots, p-1$. We may find c_1 in this set and $\epsilon_i = 0$ or 1 such that

$$a_0 + b_0 = \epsilon_0 p + c_0,$$
$$\epsilon_0 + a_1 + b_1 = \epsilon_1 p + c_1,$$
$$\epsilon_1 + a_2 + b_2 = \epsilon_2 p + c_2.$$

Whence

$$A + B = c_0 + c_1 p + \cdots + c_l p^l + \epsilon_l p^{l+1}.$$

Applying Kummer's theorem to Lemma I, let $d_0 \not\equiv 0$, and

$$p^i s = d_0 p^i + d_1 p^{i+1} + \cdots + d_j p^{i+j},$$

the d's in the set $0, 1, \cdots, p-1$. Consider $p^r t$, with

$$t = e_0 + e_1 p + \cdots + e_k p^k, \quad e_0 \not\equiv 0,$$

the e's in the set $0, 1, \cdots, p-1$. Then in

$$\frac{(A+B)!}{A!B!}$$

we have

$$A = p^r t,$$

and we also have

$$B = p^i s - p^r t$$

or

$$B = p^r(p - e_0) + p^{r+1}(p - (e_1 + 1)) + \cdots + p^{i-1}(p - (e_{i-r-1} + 1)) + Ep^i$$

where E is a rational integer > 0. Hence by Kummer's result

$$\frac{A+B}{A!B!}$$

is divisible by

$$p^{\epsilon_r + \cdots + \epsilon_i \cdots} = p^{i-r+h},$$

where h is a rational integer $\geqq 0$, since

$$\epsilon_r = \epsilon_{r+1} = \cdots = \epsilon_i = 1.$$

Kummer's argument for the proof of the theorem on which the above proof depends is very complicated, however, so I shall give another proof of Lemma I.

We have

$$(u+v)^p = A_1 + pA_0,$$
$$(u+v)^{p^2} = (A_1 + pA_0)^p = A_2' + pA_1' + p^2A_0',$$

where the (A')'s, (A'')'s have similar properties to the A's. Now assume the theorem is true for the exponent p^i. We shall then prove it true for the exponent p^{i+1}. Raising both sides of the equation mentioned in the lemma for $s=1$, to the power p, obviously the result may be written

$$(A_i + pA_{i-1} + \cdots + p^{i-1}A_1)^p + p^{i+1}A_0'' .$$

Also, the term involving the parenthesis may be written

$$(A_i + pA_{i-1} + \cdots + p^{i-2}A_2)^p + p^iA_1'' .$$

Proceeding in this manner the lemma is proved for the exponent p^{i+1}, hence is true for any exponent which is a power of p. Using this expression for $(u+v)^{p^i}$ and raising to the power s the result may be written

$$(A_i + pA_{i-1} + \cdots + p^{i-1}A_1)^s + p^iA_0.$$

Proceeding in this manner the lemma is established.

We now prove

LEMMA II. *Suppose*

$$\alpha = e^{2i\pi/p};$$

p an odd prime;

$$\phi = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_d\alpha^d$$

where the a's are rational integers, and

$$\phi_1 = a_0' + a_1'\alpha + a_2'\alpha^2 + \cdots + a_d'\alpha^d,$$

d an arbitrary positive rational integer, the a''s rational integers;

$$\phi = \phi_1,$$
$$\phi(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d,$$

and similarly for $\phi_1(x)$; i is a rational integer $\geqq 0$;

$$\phi(1) \equiv \phi_1(1) \pmod{p^{i+1}};$$
$$\phi_1(1) \not\equiv 0 \pmod{p};$$

m a positive integer such that $m \not\equiv 0 \pmod{p-1}$. Then

$$\frac{d_0{}^{mp^i} \log \phi(e^v)}{dv^{mp^i}} \equiv \frac{d_0{}^{mp^i} \log \phi_1(e^v)}{dv^{mp^i}} \pmod{p^{i+1}}.$$

As shown in a previous article (these Transactions, 1929, pp. 617–8) we obtain from $\phi = \phi_1$ the following identity in e^v:

$$\phi(e^v) = \phi_1(e^v) + (e^{vp} - 1)V + \frac{e^{vp} - 1}{e^v - 1} c_1,$$

where c_1 is a rational integer. Setting $v = 0$ in this relation we obtain, since

$$\phi(1) \equiv \phi_1(1) \pmod{p^{i+1}},$$

the relation

$$pc_1 \equiv 0 \pmod{p^{i+1}},$$

whence

$$c_1 = cp^i,$$

where c is a rational integer. The resulting relation may be written in the form

$$\frac{\phi(e^v)}{\phi_1(e^v)} = 1 + (e^{vp} - 1)\frac{V}{\phi_1(e^v)} + cp^i \frac{e^{vp} - 1}{\phi_1(e^v)(e^v - 1)}. \tag{8}$$

Set

$$y = (e^{vp} - 1)W + \frac{e^{vp} - 1}{e^v - 1} Z,$$

where

$$W = \frac{V}{\phi_1(e^v)}$$

and

$$Z = \frac{cp^i}{\phi_1(e^v)}.$$

We have

$$\frac{d \log (1 + y)}{dv} = \frac{dy/dv}{1 + y}$$

and

$$\begin{aligned} \frac{d^{mp^i} \log (1 + y)}{dv^{mp^i}} &= \frac{d^{mp^i - 1}}{dv^{mp^i - 1}} \left(\frac{1}{1 + y} \cdot \frac{dy}{dv} \right) \\ &= \frac{1}{1 + y} \frac{d^{mp^i} y}{dv^{mp^i}} + (mp^i - 1) \frac{d}{dv} \left(\frac{1}{1 + y} \right) \cdot \frac{d^{mp^i - 1} y}{dv^{mp^i - 1}} \\ &\quad + \cdots + \frac{d^{mp^i - 1}}{dv^{mp^i - 1}} \left(\frac{1}{1 + y} \right) \cdot \frac{dy}{dv}. \end{aligned}$$

Now

$$\frac{d_0 y}{dv} \equiv 0 \pmod{p},$$

and if $k \not\equiv 0$,

$$\left[\frac{d^k}{dv^k}\left(\frac{1}{1+y}\right)\frac{d^{mp^i-k}y}{dv^{mp^i-k}}\right]_{v=0} \equiv \left[\frac{d^k}{dv^k}\left(\frac{1}{1+y}\right)\frac{d^{mp^i-k}x}{dv^{mp^i-k}}\right]_{v=0} \pmod{p^{i+1}},$$

if

$$x = (e^{vp} - 1)W.$$

Also

$$\left[\frac{d^k}{dv^k}\left(\frac{1}{1+y}\right)\right]_{v=0} \equiv \left[\frac{d^k}{dv^k}\left(\frac{1}{1+x}\right)\right]_{v=0} \pmod{p^i}.$$

Now if $k=0$, we note that

$$\frac{d_0^{mp^i} y}{dv^{mp^i}} \equiv \frac{d_0^{mp^i} x}{dv^{mp^i}} \pmod{p^{i+1}}$$

since $m \not\equiv 0 \pmod{(p-1)}$. Hence

$$\frac{d_0^{mp^i}\log(1+y)}{dv^{mp^i}} \equiv \frac{d_0^{mp^i}\log(1+x)}{dv^{mp^i}} \pmod{p^{i+1}}.$$

We have

$$\frac{d\log(1+x)}{dv} = \frac{dx/dv}{1+x},$$

$$\frac{d^{mp^i}\log(1+x)}{dv^{mp^i}} = \frac{d^{mp^i-1}}{dv}\left(\frac{dx/dv}{1+x}\right),$$

whence

$$\frac{dx/dv}{1+x}(1+x)^{p^i} = \frac{dx}{dv}(1+x)^{p^i-1}.$$

Differentiating the left hand member as a product we obtain

$$\frac{d^{mp^i}\log(1+x)}{dv^{mp^i}} \equiv \frac{d^{mp^i-1}}{dv}\left(\frac{dx/dv}{1+x}\right) \equiv \frac{d^{mp^i-1}}{dv}\left[\frac{dx}{dv}(1+x)^{p^i-1}\right]$$

(mod p^{i+1}) if $v=0$, since

$$\left[\frac{dx}{dv}\right]_{v=0} \equiv 0 \pmod{p}$$

and

$$[(1+x)^{p^i}]_{v=0} \equiv 1 \pmod{p^{i+1}}.$$

We also have

$$(1+x)^{p^{i-1}} = 1 + (p^i - 1)x + \binom{p^i - 1}{2} x^2 + \cdots + x^{p^{i-1}},$$

$$(p^i - 1)(p^i - 2)\cdots(p^i - r) \equiv (-1)^r r! \pmod{p^i}.$$

Hence

$$(1+x)^{p^{i-1}} \equiv 1 - x + x^2 - \cdots + x^{p^{i-1}} \pmod{p^i}$$

and since dx/dv for $v=0$ is divisible by p we have

$$\frac{d^{mp^{i-1}}}{dv}\left[\frac{dx}{dv}(1+x)^{p^{i-1}}\right]_{v=0} \equiv \frac{d^{mp^{i-1}}}{dv}\left[\frac{dx}{dv} - x\frac{dx}{dv} + x^2\frac{dx}{dv} - \cdots + \frac{dx}{dv}x^{p^i-1}\right]_{v=0} \pmod{p^{i+1}}.$$

Since

$$\frac{1}{n}\frac{dx^n}{dv} = x^{n-1}\frac{dx}{dv}$$

it follows that the right hand member of the above reduces to

$$\left[(-1)^{n-1}\sum_{n=1}^{p^i}\frac{1}{n}\frac{d^{mp^i}x^n}{dv}\right]_{v=0}.$$

Now take logarithms of (8) and differentiate mp^i times. We then obtain, from what precedes,

$$\left[(-1)^{n-1}\sum_{n=1}^{p^i}\frac{1}{n}\frac{d^{mp^i}x^n}{dv}\right]_{v=0} \equiv \frac{d_0^{mp^i}\log\phi(e^v)}{dv^{mp^i}} - \frac{d_0^{mp}\log\phi_1(e^v)}{dv^{mp^i}} \pmod{p^{i+1}}.$$

It will now be shown that the left hand member of the above is congruent to zero (mod p^{i+1}). We have

$$x^n = ((e^{vp}-1)W)^n.$$

Assume that n is prime to p.

Then

$$\frac{d^{p^i m}(W_1(e^{vp}-1))}{dv^{p^i m}} = (e^{vp}-1)\frac{d^{p^i m}W_1}{dv^{mp^i}} + p^i m\frac{d(e^{vp}-1)}{dv}\frac{d^{p^i m-1}W_1}{dv^{p^i m-1}} + \cdots + \frac{W_1 d^{p^i m}(e^{vp}-1)}{dv^{p^i m}}, \tag{9}$$

where

$$W_1(e^{vp}-1) = W^n(e^{vp}-1)^n.$$

We have obviously

$$\frac{d^k(e^{vp}-1)}{dv^k} = p^k e^{vp}. \tag{10}$$

Consider the general term in the above expression, namely

$$\binom{p^i m}{j} \frac{d^j(e^{vp}-1)}{dv^j} \frac{d^{p^i m-j} W_1}{dv^{p^i m-j}}.$$

According to Lemma I,

$$\binom{p^i m}{j}$$

is divisible by p^{i-s}, if $j=qp^s$; $s \geqq 0$. Using (10) for $v=0$ the general term becomes a fraction whose denominator is prime to p and whose numerator is divisible by p^{i-s+qp^s}. Hence it is divisible by p^{i+1} since $i-s+qp^s \geqq i+1$. Consequently our term x^n/n in the original expansion becomes after the differentiation and substitution of $v=0$ a fraction whose denominator is prime to p and whose numerator is divisible by p^{i+1}. Now consider the term in the original expansion $x^{p^a h}/p^a h$ where $p^a h \leqq p^i m$ and h is prime to p. Put the expression $(W(e^{vp}-1))^{p^a h}$ in the form $W_2(e^{vp}-1)^{p^a}$. We have

$$(e^{vp}-1)^{p^a} = e^{vp^{a+1}} - p^a e^{vp(p^a-1)} + \binom{p^a}{2} e^{vp(p^a-2)} - \cdots - 1.$$

Consider the general term of this expansion, namely

$$\pm \binom{p^a}{j} e^{vp(p^a-j)},$$

where $j=qp^r$, q being prime to p. Also consider from this the general term obtained in

$$\frac{d^s(e^{vp}-1)^{p^a}}{dv^s},$$

that is,

$$\pm p^s \binom{p^a}{j} (p^a-j)^s e^{vp(p^a-j)}.$$

As before the expression

$$\binom{p^a}{j}$$

is divisible by p^{a-r}. Hence this general term becomes after substituting $v=0$ an integer divisible by

$$p^{a-r} \cdot p^s \cdot (p^a - qp^r)^s,$$

or is divisible by

$$p^{a-r+rs+s}.$$

This exponent is obviously greater than or equal to $a+s$ for $s>0$ so that we have, for $s \geqq 0$,

$$\frac{d_0^s(e^{vp}-1)^{p^a}}{dv^s} \equiv 0 \pmod{p^{a+s}}. \tag{11}$$

Now consider

$$\frac{d^{p^i m}(W_2(e^{vp}-1)^{p^a})}{dv^{p^i m}}.$$

Expand by Leibnitz's theorem and consider the general term:

$$\binom{p^i m}{p^k n} \frac{d^{p^k n}(e^{vp}-1)^{p^a}}{dv^{p^k n}} \cdot \frac{d^{p^i m - p^k n} W_2}{dv^{p^i m - p^k n}}$$

when $k \geqq 0$. For $v=0$ it is divisible by

$$p^{i-k+a+p^k n}$$

which is divisible by p^{i+1+a} since h is prime to p and $p^k n - k \geqq 1$. Hence all terms in the original expansion of the right hand member of (8), after differentiation $p^i m$ times and substituting $v=0$, become fractions whose denominators are prime to p and whose numerators are all divisible by p^{i+1}. Hence the lemma is established.

We shall close this article by extending to higher powers of l the criterion of Kummer and Takagi* that a principal ideal be the lth power of an ideal in $k(\zeta)$. Assume that

$$(\omega) = \mathfrak{a}^{l^i},$$

where $\mathfrak{a}$ is an ideal in $k(\zeta)$ and ω is an integer in that field. Hence from (2) and the formulas following it,

$$\prod_c \omega_c^{l-1} = \zeta^{k\theta l^i},$$

where $\theta \equiv 1 \pmod{\lambda}$; $\lambda = (1-\zeta)$; also $cc_1 \equiv 1 \pmod{l}$ and c_1 ranges over the integers which satisfy $|ac_1| + |c_1| > 1$. Replace this relation by means of an identity in e^v as usual and differentiate ml^i times; apply Lemma II and substitute $v=0$. We obtain, as in the proof of our main theorem,

$$B_{(s+1)/2} \frac{d_0^{(l-2n)l^i} \log \omega(e^v)}{dv^{(l-2n)l^i}} \equiv 0 \pmod{l^{i+1}},$$

where $s=(2n-1)l^i$.

* Kummer, Berlin Abhandlungen, Mathematisch-Physikalische Klasse, 1857, p. 65; Takagi, Proceedings of the Physico-Mathematical Society of Japan, (3), vol. 4 (1922), pp. 170–182; Journal für die reine und angewandte Mathematik, vol. 157 (1927), pp. 230–8.

UNIVERSITY OF TEXAS,
AUSTIN, TEXAS