ON THE FUNDAMENTAL NUMBER OF THE ALGEBRAIC
NUMBER-FIELD \( k(\sqrt[p]{m}) \)

BY

JACOB WESTLUND

Introduction.

The object of the present paper is the determination of an integral basis and the fundamental number of the algebraic number-field \( k(\sqrt[p]{m}) \) generated by the real \( p \)th root of \( m \), where \( m \) is a positive integer greater than unity which is not divisible by the \( p \)th power of an integer, and where \( p \) is any odd prime. The case \( p = 3 \) has already been discussed by Dedekind.* The conjugate values of \( \sqrt[p]{m} \) being \( \sqrt[p]{m}, \sqrt[p]{m}^p, \ldots, \sqrt[p]{m}^{p-1} \), where \( \rho = e^{2\pi i/p} \), the number-fields \( k(\rho \sqrt[p]{m}), \ldots, k(\rho^{p-1} \sqrt[p]{m}) \) are all different from \( k(\sqrt[p]{m}) \).

In order to obtain all possible number-fields of this type we let \( m \) run through all positive integers which are not divisible by the \( p \)th power of a prime. But the fields generated in this way are not all distinct. For any positive integer \( m \) which is not divisible by the \( p \)th power of a prime may be expressed in one way only in the form

\[
m = a_1 a_2^2 \cdots a_{p-1}^2 \]

where \( a_1 a_2 \cdots a_{p-1} \) is not divisible by the square of a prime. If we then set

\[
\alpha_s = \sqrt[p]{a_1^i a_2^i \cdots a_{p-1}^i},
\]

where \( i_s \equiv si \pmod{p} \) and \( 0 < i_s < p \) for \( s = 1, 2, 3, \ldots, p - 1 \), it is evident that \( \alpha_1, \alpha_2, \ldots, \alpha_{p-1} \) are algebraic integers in \( k(\alpha_1) \), and hence \( k(\alpha_1), k(\alpha_2), \ldots, k(\alpha_{p-1}) \) are identical, while \( k(\alpha_1) \) is a primitive field.

1. Rational basis.

As a rational basis of \( k(\alpha_1) \) we may take either

\[
1, \alpha_1, \alpha_1^2, \ldots, \alpha_1^{p-1}
\]

or

\[
1, \alpha_1, \alpha_2, \ldots, \alpha_{p-1}.
\]


License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Denote the discriminants of these bases by $D_1$ and $D_2$, respectively. We have

$$D_1 = \begin{vmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{p-1} \\ 1 & \rho \alpha_1 & \ldots & \rho^{p-1} \alpha_1^{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \rho^{p-1} \alpha_1 & \ldots & \rho^{(p-1)p-1} \alpha_1^{p-1} \end{vmatrix} = m^{p-1} \begin{vmatrix} 1 & 1 & \ldots & 1 \\ 1 & \rho & \ldots & \rho^{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \rho^{p-1} & \ldots & \rho^{(p-1)^2} \end{vmatrix}$$

Hence*

$$D_1 = (-1)^{k(p-1)} p^m m^{p-1}.$$

In a similar way we obtain

$$D_2 = (-1)^{k(p-1)} p^p (a_1 a_2 \cdots a_{p-1})^{p-1}.$$

If $\Delta$ be the fundamental number of $k(\alpha_1)$, we must have $D_2 = n^2 \Delta$ where $n$ is a rational integer. Hence

$$\Delta = (-1)^{k(p-1)} p \left[ \frac{(pa_1 a_2 \cdots a_{p-1})^{(p-1)} \gamma}{n} \right]^2 = (-1)^{k(p-1)} p d^2$$

where $d$ is a rational integer, and this shows that $\Delta$ contains the factor $p$.

2. Ideal Prime Factors of $p$ and $m$.

Let $q$ be a prime factor of $m$ and $Q$ an ideal prime factor of $q$. Then since $\alpha_i = q^i r$, where $r$ is prime to $q$ and $0 < i < p$, it follows that $\alpha_i$ is divisible by $Q$. Suppose that $Q^r$ is the highest power of $Q$ contained in $q$. Then $\alpha_i$ must be divisible by $Q^r$ and $si \equiv 0 \pmod{p}$. Hence $s = p$ and $(q) = Q^p$, i.e., every prime factor of $m$ is equal to the $p$th power of a prime ideal of the first degree.

Let us next consider the prime $p$. If $p$ is a factor of $m$ it comes under the case already considered. Suppose then that $p$ is not contained in $m$. Since $p$ is a factor of the fundamental number, it is divisible by the square of a prime ideal $P$. Now consider the integer $p = a_1 - b$, where $b = a_1 a_2^p \cdots a_{p-2}^p$. We have

$$(\mu + b)^p - b a_{p-1}^{p-1} = 0$$

or, if we set $d = b^{p-1} - a_{p-1}^{p-1}$,

$$\mu^p + p b \mu^{p-1} + \cdots + p b^{p-1} \mu + bd = 0.$$

Since $d \equiv 0 \pmod{p}$ it follows that $\mu^p$ is divisible by $p$ and $\mu$ by $P$ and hence $d$ is divisible by $P^3$. Two cases arise according as $d$ is divisible by $p^2$ or not.

I. $d$ not divisible by $p^2$. In this case $p$ must be divisible by $P^3$. Hence, if $p > 3$, $d$ must be divisible by $P^4$ and therefore $p$ divisible by $P^4$. Reasoning

*PASCAL, Determinanten, p. 139.
in this way we find that \( p \) must be divisible by \( P^p \). Hence \( \mu = P^p \), i.e., if \( p \) is prime to \( m \) and \( d = b^{p-1} - a_{p-1}^{p-1} \) not divisible by \( p^2 \), then \( p \) is equal to the \( p \)-th power of a prime ideal of the first degree.

II. \( d \) divisible by \( p^2 \). Let \( p^s (s \geq 2) \) be the highest power of \( p \) contained in \( d \) and \( P^r \) the highest power of \( P \) contained in \( \mu \). The equation satisfied by \( \mu \) may be written

\[
\mu (\mu^{p-1} + p\beta) + bd = 0,
\]

where \( \beta \) is prime to \( P \). If \( r \) were greater than unity, \( \mu^{p-1} \) would be divisible by a higher power of \( P \) than \( P^p \), and since \( p \) cannot contain a higher power of \( P \) than \( P^p \), it follows from the equation above that \( \mu \) would be divisible by \( p \). But if \( \mu \) were divisible by \( p \), its conjugates would be divisible by \( p \), but this is impossible, since the coefficient of \( \mu \) in the equation above contains only the first power of \( p \). Hence \( r = 1 \). It is then easily seen that \( p \) must be divisible by \( P^{p-1} \) and by no higher power of \( p \). Hence if \( p \) is prime to \( m \), and \( b^{p-1} - a_{p-1}^{p-1} \) is divisible by \( p^2 \), we have \( \mu = P^{p-1}Q \), where \( P \) and \( Q \) are different prime ideals of the first degree.

3. Integral basis.

Any integer \( \omega \) in \( k(\alpha_i) \) may be expressed in the form

\[
\omega = \frac{x_0 + x_1 \alpha_1 + \cdots + x_{p-1} \alpha_{p-1}}{D^p},
\]

where \( x_0, x_1, \ldots, x_{p-1} \) are rational integers. Let \( q \) be a prime factor of \( \alpha_i \) and let \( (q) = Q^r \). Then the highest power of \( Q \) contained in \( \alpha_i \) is \( Q^{i^*} \), where \( i^* \equiv i (\mod p) \) and \( 0 < i^* < r \). Hence \( x_0 \) must be divisible by \( Q \) and hence by \( q \). Denote by \( \alpha_{r_1}, \alpha_{r_2}, \ldots, \alpha_{r_{p-1}} \) the numbers \( \alpha_1, \alpha_2, \ldots, \alpha_{p-1} \) arranged according to increasing powers of \( Q \). It then follows that \( x_{r_1} \) must be divisible by \( Q \) and hence by \( q \). In the same way we find that \( x_{r_2}, \ldots, x_{r_{p-1}} \) are divisible by \( q \). It is then easily seen that \( \omega \) may finally be written in the form

\[
\omega = \frac{x_0 + x_1 \alpha_1 + \cdots + x_{p-1} \alpha_{p-1}}{p^p},
\]

where \( x_0, x_1, \ldots, x_{p-1} \) are rational integers.

If \( p \) is a factor of \( m \) we proceed as above and find that

\[
\omega = y_0 + y_1 \alpha_1 + \cdots + y_{p-1} \alpha_{p-1},
\]

where \( y_0, y_1, \ldots, y_{p-1} \) are rational integers.

If \( p \) is prime to \( m \), two cases arise, according as \( d = b^{p-1} - a_{p-1}^{p-1} \) is divisible by \( p^2 \) or not.

I. \( d \) not divisible by \( p^2 \). Introducing the algebraic integer \( \mu = \alpha_i - b \) mentioned above and making use of the fact that \( \alpha_i = \alpha_i^*/c_i \), where \( c_i \) is a rational
integer prime to \( p \), we obtain

\[
\omega = y_0 + y_1\mu + \cdots + y_{p-1}\mu^{p-1}.
\]

In this case we have \( (p) = P^p \) and, as is easily seen, \( \mu \) is divisible by \( P \) but not by \( P^2 \). Reasoning in exactly the same way as above we find that \( y_0, y_1, \ldots, y_{p-1} \) are all divisible by \( p \). Hence we finally get

\[
\omega = z_0 + z_1\mu + \cdots + z_{p-1}\mu^{p-1},
\]

where \( z_0, z_1, \ldots, z_{p-1} \) are rational integers. But since all the prime factors of \( c \) are contained in \( m \), it follows that \( \omega \) may be written in the form

\[
\omega = x_0 + x_1\alpha_1 + \cdots + x_{p-1}\alpha_{p-1},
\]

where \( x_0, x_1, \ldots, x_{p-1} \) are rational integers. We then have the following result:

If \( b^{p-1} - \alpha_{p-1}^{p-1} \) is not divisible by \( p^2 \), the \( p \) numbers \( 1, \alpha_1, \alpha_2, \ldots, \alpha_{p-1} \) form an integral basis of \( k(\alpha_1) \) and \( \Delta = D_2 = (-1)^{p-1/2}p^{p}(\alpha_1\alpha_2\cdots\alpha_{p-1})^{p-1} \).

II. \( d \) divisible by \( p^2 \). In this case we know that \( (p) = P^{p-1}Q \). We also know that \( \mu^p \) is divisible by \( p \), and hence \( \mu \) is divisible by \( PQ \) and \( \mu^{p-1} \) divisible by \( pQ^{p-2} \). But

\[
\mu^{p-1} = (\alpha_1 - b)^{p-1} = \alpha_1^{p-1} - (p - 1)\alpha_1^{p-2}b \cdots + b^{p-1}
\]

\[
= \left[ \alpha_1^{p-1} + \alpha_1^{p-2}b + \cdots \alpha_1 b^{p-2} + 1 \right] - \left[ p\alpha_1^{p-2}b - \left\{ \frac{(p - 1)(p - 2)}{2} - 1 \right\} \alpha_1^{p-3}b^2 + \cdots - b^{p-1} + 1 \right]
\]

and since \( b^{p-1} \equiv 1 \pmod{p} \), it follows that

\[
\gamma = \frac{\alpha_1^{p-1} + \alpha_1^{p-2}b + \cdots + \alpha_1 b^{p-2} + 1}{p}
\]

is an algebraic integer. We shall now prove that the \( p \) numbers

\[
\gamma, \alpha_1, \alpha_2, \ldots, \alpha_{p-1}
\]

form an integral basis of \( k(\alpha_1) \). It is evident that these numbers form a rational basis. Denoting the discriminant of this basis by \( D_3 \) we get the following value

\[
D_3 = (-1)^{p-1/2}p^{p-2}(\alpha_1\alpha_2\cdots\alpha_{p-1})^{p-1}.
\]

Now any algebraic integer \( \omega \) may be written in the form

\[
\omega = \frac{x_0\gamma + x_1\alpha_1 + \cdots + x_{p-1}\alpha_{p-1}}{D_3}
\]

where \( x_0, x_1, \ldots, x_{p-1} \) are rational integers. It is easily seen that \( x_0 \) must be
divisible by $D_3$. For, denoting by $\omega, \omega', \ldots, \omega^{(p-1)}$ the conjugate values of $\omega$, we have

$$\omega + \omega' + \cdots + \omega^{(p-1)} = \frac{x_0}{D_3}.$$ 

Hence $x_0$ is divisible by $D_3$. Let us then consider the algebraic integer

$$\omega_1 = \frac{x_1 \alpha_1 + \cdots + x_{p-1} \alpha_{p-1}}{D_3}.$$ 

If $q$ be a prime factor of $m$ we infer in the same way as above that $x_1, \ldots, x_{p-1}$ are divisible by $q$, and hence that $\omega_1$ may be written in the form

$$\omega_1 = \frac{y_1 \alpha_1 + \cdots + y_{p-1} \alpha_{p-1}}{p^{p-3}}.$$ 

Replacing $\alpha_1$ by $\mu + b$ we get

$$p^{p-2}c\omega_1 = z_0 + z_1 \mu + \cdots + z_{p-1} \mu^{p-1}$$

where $z_0, z_1, \ldots, z_{p-1}$ are rational integers and $c$ is prime to $p$. By a simple argument it can then be shown that $z_0, z_1, \ldots, z_{p-1}$ and hence also $y_1, y_2, \ldots, y_{p-1}$ must be divisible by $p$ and that $\omega$ may finally be written in the form

$$\omega = x_0 \gamma + x_1 \alpha_1 + \cdots + x_{p-1} \alpha_{p-1}.$$ 

Hence we have the following result: If $b^{p-1} - \alpha_{p-1}$ is divisible by $p^2$, the $p$ numbers $\gamma, \alpha_1, \alpha_2, \ldots, \alpha_{p-1}$ form an integral basis of $k(\alpha_1)$ and

$$\Delta = D_3 = (-1)^{p-1}p^{p-2}(a_1, a_2, \ldots, a_{p-1})^{p-1}.$$ 

Purdue University.