Primitive roots of ideals in algebraic number-fields.

By

JACOB WESTLUND of La Fayette (U. S. A.).

Introduction.

If A is an ideal in an arbitrary algebraic number-field, every algebraic integer α, which is prime to A, is said to belong to a certain exponent e, if e is the least exponent for which $\alpha^e \equiv 1$, mod. A. This exponent is always a divisor of $\varphi(A)$, the number of incongruent (mod. A) algebraic integers, which are prime to A. An algebraic integer which belongs to the exponent $\varphi(A)$ is called a *primitive root* of A. In the number-field consisting of the rational numbers the only numbers which have primitive roots are the numbers of the form p^m, $2p^m$, and 2^n, where p is any odd prime and $n < 3$. The object of the present paper is to solve the more general problem of determining all the ideals in an arbitrary algebraic number-field which admit of primitive roots.*)

Let $A = P_1^{a_1} P_2^{a_2} \cdots P_n^{a_n}$, where $P_1, P_2, \cdots, P_n$ are distinct prime ideals and $a_1, a_2, \cdots, a_n$ positive integers, and let m be the least common multiple of $\varphi(P_1^{a_1})$, $\varphi(P_2^{a_2})$, $\cdots$, $\varphi(P_n^{a_n})$. Then for any algebraic integer α prime to A we have

$$\alpha^m \equiv 1, \text{ mod. } P_i^{a_i} \qquad (i = 1, 2, \cdots, n). \tag{1}$$

But

$$\varphi(A) = \varphi(P_1^{a_1})\, \varphi(P_2^{a_2}) \cdots \varphi(P_n^{a_n})$$

and

$$\varphi(P_i^{a_i}) = p_i^{f_i(a_i-1)}(p_i^{f_i} - 1)^{**})$$

where p_i is the rational prime divisible by P_i and f_i the degree of P_i. Hence if two or more of the numbers $p_i^{f_i} - 1$ have a common factor no

*) Since the above paper was printed the author's attention has been called to an article by A. Wiman in Översigt af Svenska Vetenskapsakademiens Förhandlingar 56, in which most of the results obtained in this paper are derived by a somewhat different method.

**) Hilbert, „Die Theorie der algebraischen Zahlkörper". Jahresbericht der deutschen Mathematiker-Vereinigung 4, p. 192.

primitive roots of A exist. The only ideals, which may have primitive roots are therefore ideals of the following two types: 1° $A = P^n$ and 2° $A = Q_1 Q_2 \cdots Q_m P^n$, where $Q_1, Q_2, \cdots, Q_m$ are prime ideal factors of 2 and P any prime ideal, P being different from $Q_1, Q_2, \cdots, Q_m$ in case P is an ideal factor of 2.

I. $A = P^n$.

It is easily seen that every primitive root of P^n is also a primitive root of P^{n-1} and hence a primitive root of P. For suppose ω to be a primitive root of P^n, and let e be the exponent to which ω belongs mod. P^{n-1}. Also let p be the rational prime divisible by P and f the degree of P. Then

$$\omega^e = 1 + \alpha\beta, \tag{2}$$

where β is an algebraic integer divisible by P^{n-1}. Hence

$$\omega^{pe} \equiv 1, \text{ mod. } P^n \tag{3}$$

and hence

$$e = p^a(p^f - 1). \tag{4}$$

But since e is a factor of $p^{(n-2)f}(p^f - 1)$, it follows that $a = (n-2)f$, and hence ω is a primitive root of P^{n-1}.

We will now determine when a primitive root of P is also a primitive root of P^2. Let ω be a primitive root of P and let e be its exponent mod. P^2. Then $e = p^a(p^f - 1)$, where $a \leqq f$. But ω being a primitive root of P, we have

$$\omega^{p(p^f-1)} \equiv 1, \text{ mod. } P^2.$$

Now in order that ω shall be a primitive root of P^2 we must have $a = f$, and hence $f = 1$. Hence the following theorem:

If P be a prime ideal of a degree higher than the first, there exist no primitive roots of P^n, $n > 1$, p being either odd or even.

In the following we will then consider only ideals of the first degree.

Now let ω be a primitive root of P and $e = p^i(p-1)$, where $0 \leqq i \leqq n-1$, its exponent mod. P^n. In order that ω shall be a primitive root of P^n and hence of P^2 it is evident that $\omega^{p-1} - 1$ should be divisible by P but not by P^2. We will then consider only those primitive roots ω of P which satisfy this condition*). It is evident that these ω are primitive roots of P^2.

*) That such primitive roots exist can easily be shown. Cf. Weber, Lehrbuch der Algebra, 2nd ed., vol. I, p. 686.

Now let P^d be the highest power of P contained in p. Then two cases present themselves according as $1+d \leqq p$ or $1+d > p$.

Case I. $1+d \leqq p$.

Since $\omega^{p-1}-1$ is divisible by P but not by P^2, it follows that

$$\omega^{p^i(p-1)} \equiv 1, \text{ mod. } P^{1+id}. \tag{5}$$

Hence in order that ω shall be a primitive root of P^n we must have

$$1+(n-2)d < n \leqq 1+(n-1)d. \tag{6}$$

1. $d=1$, $p>2$. In this case $1+d<p$, and P^{1+id} is the highest power of P contained in $\omega^{p^i(p-1)}$. Hence $P^{1+(n-1)d}$ and $P^{1+(n-2)d}$ are the highest powers of P contained in $\omega^{p^{n-1}(p-1)}-1$ and $\omega^{p^{n-2}(p-1)}-1$ respectively, and hence ω is a primitive root of P^n $(n \geqq 2)$.

2. $d=1$, $p=2$. In this case ω^2-1 is divisible by P^3. For let $\omega-1=\alpha\pi$, where α is prime to P and π divisible by P but not by P^2. Then taking norms we have

$$N(\omega+1) = N[2+(\omega-1)]$$

or

$$N(\omega+1) \equiv N(\omega-1)+2a, \text{ mod. } 4$$

where a is the sum of the products obtained by taking all the conjugate values of $\omega-1$ except one at a time. All these products except one being divisible by $\omega-1$ and hence by P, it follows that a is not divisible by 2, since $N(\omega-1)$ is not divisible by 4. Hence

$$N(\omega+1) \equiv 0, \text{ mod. } 4$$

and hence $\omega+1$ divisible by P^2 and ω^2-1 divisible by P^3. Hence there are no primitive roots of P^n $(n>2)$, if $p=2$ and $d=1$.

3. $d>1$. From (6) we obtain as a necessary condition that ω shall be a primitive root of P^n

$$d < \frac{n-1}{n-2}. \tag{7}$$

But the maximum value of $\frac{n-1}{n-2}$ for $n>2$ is 2. Hence in this case there exist no primitive roots of P^n, if $n>2$.

Case II. $1+d>p$.

In this case p is a factor of the fundamental number, since $d>1$. Now let k satisfy the conditions

$$\begin{cases} p^k < p^{k-1}+d, \\ p^{k+1} \geqq p^k+d. \end{cases} \tag{8}$$

Then the highest power of P contained in $\omega^{p^i(p-1)}-1$ is P^{p^i}, if $i \leqq k$, and $\omega^{p^{k+1}(p-1)}-1$ is divisible by P^{p^k+d}.

If $k \geqq n-2$, the highest power of P contained in $\omega^{p^{n-2}(p-1)}-1$ is $P^{p^{n-2}}$. But if $p>2$, $p^{n-2} \geqq n$ except for $n=2$, and hence it follows that ω cannot be a primitive root of P^n $(n>2)$.

If $k<n-2$, $\omega^{p^{n-2}(p-1)}-1$ is divisible by $P^{p^k+(n-2-k)d}$. But if $p>2$, $p^k+(n-2-k)d>n$ for $n>3$, and hence ω is not a primitive root of P^n.

Let us now consider the case when $p=2$. The highest power of P contained in ω^2-1 is P^2, and ω^4-1 is divisible by P^4. Hence there exist no primitive roots for $n>3$.

Summarizing these results we have the following theorem:

The primitive roots of P^n, when such roots exist, are those primitive roots ω of P for which $\omega^{p-1}-1$ is divisible by P but not by P^2.

If p is an odd prime which is not a factor of the fundamental number, there exist primitive roots of P^n, $n \geqq 2$.

If $p=2$ and the fundamental number is odd, there exist no primitive roots of P^n except for $n=2$.

If p is an odd factor of the fundamental number, there exist no primitive roots of P^n except for $n=2$.

If $p=2$ and the fundamental number is even there exist primitive roots of P^n for $n=2$ and 3 but not for higher powers of P.

II. $A = Q_1 Q_2 \cdots Q_m P^n$.

If ω is a primitive root of A, it must also be a primitive root of Q_i $(i=1,2,\cdots,m)$ and of P^n. Hence the only cases when there exist primitive roots of A are when there exist primitive roots of P^n and in addition no two of the numbers $2^{f_i}-1$, where f_i is the degree of Q_i, have a common factor. We will now show how to find the primitive roots of A, when such roots exist.

Determine the algebraic integers $\alpha_1, \alpha_2, \cdots, \alpha_m, \beta$ such that

$$(9) \qquad \begin{cases} \alpha_i \equiv 1, \text{ mod. } Q_i, \\ \alpha_i \equiv 0, \text{ mod. } Q_k, \quad \text{when } i \neq k, \\ \alpha_i \equiv 0, \text{ mod. } P^n \end{cases}$$

and

$$(10) \qquad \begin{cases} \beta \equiv 0, \text{ mod. } Q_i, \\ \beta \equiv 1, \text{ mod. } P^n. \end{cases}$$

Now let $\omega_1, \omega_2, \cdots, \omega_m, \omega$ be primitive roots of $Q_1, Q_2, \cdots, Q_m, P^n$ respectively. Then setting

$$\gamma = \alpha_1\omega_1 + \cdots + \alpha_m\omega_m + \beta\omega$$

we have

$$\gamma \equiv \omega, \text{ mod. } P^n \tag{11}$$

and hence γ is a primitive root of P^n. Similarily we prove that γ is a primitive root of Q_i $(i = 1, 2, \cdots, m)$. Hence, if no two of the numbers $2^{f_i} - 1$ have a common factor, γ is a primitive root of A.

Since the above paper was written, my attention has been called to an article by Dr. A. Ranum in Vol. 11, No. 2 of the *Transactions of the American Mathematical Society*. In this article, entitled 'The group of classes of congruent quadratic integers with respect to a composite ideal modulus', Dr. Ranum derives by a different method and for the special case of a *quadratic* number-field the results obtained above.

Purdue University, La Fayette, Ind., U. S. A., May 1910.