ON THE CONGRUENCE $x^{\phi(P)} \equiv 1$, MOD. P^n.

BY PROFESSOR JACOB WESTLUND.

(Read before the American Mathematical Society, August 31, 1903.)

1. LET $k(\theta)$ be any algebraic number field and P a prime ideal in $k(\theta)$. Then we know that every algebraic integer, which is prime to P, satisfies the congruence

$$x^{\phi(P)} \equiv 1, \text{ mod. } P, \tag{1}$$

where $\phi(P) = n(P) - 1$, $n(P)$ denoting the norm of P. The object of the present note is to determine the roots of the congruence

$$x^{\phi(P)} \equiv 1, \text{ mod. } P^n, \tag{2}$$

for $n > 1$.*

2. To determine the roots of (2) we introduce the function $q_n(\alpha)$, defined in the following way. Suppose that α be a root of

$$x^{\phi(P)} \equiv 1, \text{ mod. } P^n,$$

and let μ_n be an algebraic integer, divisible by P^n and by no higher power of P. Then we can find an algebraic integer, which we denote by $q_n(\alpha)$, such that

$$\alpha^{\phi(P)} \equiv 1 + \mu_n q_n(\alpha), \text{ mod. } P^{n+1}. \tag{3}$$

For if

$$\alpha^{\phi(P)} = 1 + \pi,$$

where π is divisible by P^n, we should have

$$\pi \equiv \mu_n q_n(\alpha), \text{ mod. } P^{n+1},$$

and

$$\frac{\gamma\pi}{\mu_n} \equiv \gamma q_n(\alpha), \text{ mod. } P, \tag{4}$$

if γ is an algebraic integer, prime to P, such that $\gamma\pi/\mu_n$ is an

* For $k(1)$ or the number field consisting of the rational numbers, see Bachmann : Niedere Zahlentheorie, p. 159.