BULLETIN OF THE

AMERICAN MATHEMATICAL SOCIETY.

CRITERIA FOR THE IRREDUCIBILITY OF FUNCTIONS IN A FINITE FIELD.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society, September 3, 1906.)

1. THEOREM. *A necessary condition that*

$$(1) \qquad f(x) \equiv x^m + c_1 x^{m-1} + \cdots + c_m$$

shall be irreducible in the $GF[p^n]$, $p > 2$, *is that its discriminant** *be a square or a not-square according as* m *is odd or even.*

If $f(x) = 0$ is irreducible its roots are $\lambda^{p^{ni}} (i = 0, 1, \cdots, m-1)$. Its discriminant is therefore the square of P, where

$$P = \prod_{i<j}^{i,j=0,1,\ldots,m-1} (\lambda^{p^{ni}} - \lambda^{p^{nj}}) \equiv \Pi f_{i,j}.$$

For $j < m - 1$, we have $f^{p^n}_{i,j} = f_{i+1,j+1}$. But $f^{p^n}_{i,m-1} = -f_{0,i+1}$. Hence

$$P^{p^n} = (-1)^{m-1} P,$$

so that P equals a mark of the $GF[p^n]$, $p > 2$, if and only if m is odd.

Remark. The condition is also sufficient if $m = 2$.

2. LEMMA. *The necessary and sufficient condition that a cubic shall have one and but one root in the* $GF[p^n]$, $p > 2$, *is that its discriminant be a not-square.*

* As in the theory of algebraic equations, it is here convenient to designate as the discriminant the product of the squares of the differences of the roots. Most writers on cognate subjects insert the factor $(-1)^{\frac{1}{2}m(m-1)}$, and some insert also the factor $1/m^m$.