On eliminating first y_1^3 and then c^2 between (16) and (11), and in the latter case removing the factor $y_1 - b \neq 0$, we get

$$(17) \quad by_1^2 - b^2y_1 - 4dy_1 + 4bd - \tfrac{3}{2}c^2 = 0, \quad 3y_1^2 - 2by_1 - 4d = 0.$$

But the Sylvester eliminant of these is found to equal $-\frac{3}{4}\Delta$, where Δ is the discriminant of (11) for $a = 0$. Hence the case $p \neq 3$ is excluded. For $p = 3$, $by_1 = d \neq 0$; but for this value of y_1 (11) becomes $\Delta = 0$. Hence in every case the conditions are sufficient to make the quartic irreducible.

UNIVERSITY OF CHICAGO,
June, 1906.

ON THE THEORY OF EQUATIONS IN A MODULAR FIELD.

BY PROFESSOR L. E. DICKSON.

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

1. The object of this note is to point out that the Galois theory of algebraic equations may be extended to equations in a field F having a modulus p. For a finite field the theory is so obvious that this case furnishes a simple, but characteristic, example of the Galois theory.

2. Let the domain of rationality be the $GF[p^n]$. Consider an equation $f(x) = 0$ with coefficients in this field and having distinct roots $x_1, \cdots, x_m$. By a Galois resolvent of $f(x) = 0$ will be meant an equation $\phi(V) = 0$, irreducible in the $GF[p^n]$, with a root V which is a rational function of $x_1, \cdots, x_m$, and such that each x_i is a rational function of V with coefficients in the field. Let $m_1, m_2, \cdots$ be the distinct degrees of the irreducible factors of $f(x)$ in the $GF[p^n]$, and let l be the least common multiple of $m_1, m_2, \cdots$. Then the smallest field which contains all the roots x_i of $f(x) = 0$ is the $GF[p^{nl}]$. Any primitive root of the latter may be taken as the desired function V. In fact the power $(p^{nl} - 1)/(p^{nm_i} - 1)$ of V is a primitive root ρ_i of the $GF[p^{nm_i}]$, so that the x's are powers of $\rho_1, \rho_2, \cdots$ and hence of V. Further, V is a rational function of the ρ's and hence of the x's. Indeed, if m_1 and m_2 have the greatest common divisor g and the least common multiple λ, an

irreducible equation of degree m_1 decomposes in the $GF[p^{nm_2}]$ into g irreducible equations, any one of which defines the $GF[p^{n\lambda}]$, so that the marks of the latter are rational functions of ρ_1 and ρ_2.

The Galois resolvent $\phi(V) = 0$ has the m roots

$$V^{p^{ni}} \qquad (i = 0, 1, \cdots, m-1).$$

Hence the Galois group of $f(x) = 0$ in the $GF[p^n]$ is simply isomorphic with the cyclic group of order m generated by the substitution

$$V' = V^{p^n}.$$

3. One standard method (following Galois) of obtaining the Galois resolvent of an algebraic equation of degree m in a domain of rationality R depends upon the existence of an $m!$ valued rational function V of the roots x_i. When R is the $GF[p^n]$, this method cannot be applied unless p^n exceeds a certain limit. For example, if all the x's belong to the $GF[p^n]$, V evidently does not exist when $m! > p^n$. Again, if the irreducible factors of $f(x)$ are all of degree $\leqq 2$, V does not exist when $m! > p^{2n}$. Except for certain values of p^n, small in relation to m, there exists an $m!$ valued function V and the theory presents no difficulty.*

4. There is an interesting point in the determination of an $m!$ valued linear function of the distinct roots $x_1, \cdots, x_m$. It is illustrated in the case $m = 3$. If $t = \alpha x_1 + \beta x_2 + \gamma x_3$ is six valued, so is $t - \gamma(x_1 + x_2 + x_3)$ six valued. Hence we may restrict our attention to $V = qx_1 + x_2$. The necessary and sufficient condition that V be six valued is that q be distinct from

$$0,\ 1,\ (x_2 - x_3)/(x_1 - x_3),\ (x_1 - x_2)/(x_1 - x_3),\ (x_3 - x_2)/(x_1 - x_2),$$

and the reciprocals of the last three. Denoting the first of these fractions by λ, we find that the other two are $1 - \lambda$ and

* In a discussion of the Galois group of order N (*cf.* Dickson's Algebraic Equations, p. 53), there is a proof that if $\phi_1 = \phi_2 = \cdots = \phi_N$, then $\phi_1 = N^{-1}(\phi_1 + \cdots + \phi_N) = N^{-1}$ (a number of R). This step would now be invalid if N is a multiple of the modulus p. But we may proceed as follows: Let $N = p^s k$, k prime to p. Take the ${}_N C_p = p^{s-1}k_1$ products π_i of the ϕ's p at a time; take the $p^{s-2}k_2$ products π'_i of the π_i p at a time; etc. Finally, we reach $k_s \phi^{p^s}$ as a symmetric function of the ϕ_i. But k_s is prime to p, and the extraction of (p^s)th roots is possible in the field.

$\lambda/(\lambda-1)$. Hence

$$(1)\quad q \neq 0,\ 1,\ \lambda,\ 1-\lambda,\ \frac{\lambda}{\lambda-1},\ \frac{1}{\lambda},\ \frac{1}{1-\lambda},\ \frac{\lambda-1}{\lambda}\quad (\lambda \neq 0,\ 1).$$

Here the six functions of λ are the six elements of the cross-ratio group, and each differs from 0 and 1. Hence equalities arise only when $\lambda = -1,\ 2$, or $\frac{1}{2}$, or when $\lambda^2 - \lambda + 1 = 0$.

When x_1, x_2, x_3 are distinct, $qx_1 + x_2$ is six valued only in the following cases: (i) one of the x's is an arithmetical mean between the other two, with $q \neq 0,\ 1,\ -1,\ 2,\ \frac{1}{2}$; (ii) $\Sigma x_j^2 = \Sigma x_j x_k$, with $q \neq 0,\ 1,\ \lambda,\ 1/\lambda$ (where $\lambda^2 - \lambda + 1 = 0$); (iii) neither of the relations on the x's holding, with q not equal to one of the eight distinct values (1).

It may now be readily shown that there exist six valued linear functions of the roots x_i of a cubic in the $GF[p^n]$ when $p^n > 8$; when $p^n = 7$; and when $p^n = 5$ or 8, with the x_i not all in the $GF[p^n]$.

5. In conclusion it may be remarked that the Galois theory as presented in Weber's Algebra may readily be extended to apply to modular fields, provided his argument on page 500 (of volume 1 of the second edition) be replaced by that in § 2 above.

THE UNIVERSITY OF CHICAGO,
July, 1906.

NOTE ON THE VARIATION OF THE DEFINITE INTEGRAL.

BY MR. N. J. LENNES.

(Read before the Chicago Section of the American Mathematical Society. April 14, 1906.)

A function is said to be of limited variation on an interval ab if the set of sums

$$\left[\sum_{i=0}^{n-1} |f(x_i) - f(x_{i+1})|\right]$$

is bounded for the set of all partitions of ab. The points $a = x_0, x_1, x_2 \cdots, x_{n-1}, x_n = b$ of each partition are ordered on the interval according to the subscripts. The least upper