that followed by Jordan in his Traité des Substitutions, pages 13–14.

A Galois field may be considered as made up of roots of unity 1, ϵ, ϵ^2, $\cdots$ or what comes to the same thing, of a primitive root of unity and its various powers. A Guldberg field can be thought of as made up of e^{ϵ}, $e^{\epsilon x}$, $e^{\epsilon 2x}$, $\cdots$ (ϵ = root of unity) and the various derivatives of these quantities. From a certain point of view this field will be infinite since x is an independent variable.

THE UNIVERSITY OF CHICAGO,
April, 1903.

FIELDS WHOSE ELEMENTS ARE LINEAR DIFFERENTIAL EXPRESSIONS.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society, April 25, 1903.)

A. GULDBERG * has considered expressions of the form

$$Ay = a_\alpha \frac{d^\alpha y}{dx^\alpha} + a_{\alpha-1} \frac{d^{\alpha-1} y}{dx^{\alpha-1}} + \cdots + a_1 \frac{dy}{dx} + a_0 y,$$

in which $a_\alpha, \cdots, a_0$ are integers taken modulo p, p being a prime number. The *product* $Ay \cdot By$ of two such expressions in defined by Boole's symbolic method † to be

$$\left(a_\alpha \frac{d^\alpha}{dx^\alpha} + \cdots + a_1 \frac{d}{dx} + a_0\right)\left(b_\beta \frac{d^\beta}{dx^\beta} + \cdots + b_1 \frac{d}{dx} + b_0\right) y,$$

so that the expansion may be effected as if d/dx were a constant. If, in this manner, $Ay \cdot By \equiv Cy \pmod p$, we say that Ay and By are *divisors* modulo p of Cy. Euclid's algorithm for the greatest common divisor is seen to hold. We may therefore define reducible and irreducible differential expressions modulo p. Let

$$\Delta y = \delta_n \frac{d^n y}{dx^n} + \cdots + \delta_1 \frac{dy}{dx} + \delta_0 y$$

---

* "Sur des congruences différentielles linéaires," *Comptes rendus*, vol. 125, p. 489 (1897).

† Boole, Differential Equations, p. 381, seq.

be irreducible modulo p. Then any expression Ay is congruent modulis p, Δy with one and but one of the p^n expressions

$$c_{n-1}\frac{d^{n-1}y}{dx^{n-1}} + \cdots + c_1\frac{dy}{dx} + c_0 y, \tag{1}$$

where $c_{n-1}, \cdots, c_0$ take independently the values $0, 1, \cdots, p-1$. Guldberg then states without proof certain theorems on congruences (modd p, Δy) with coefficients of type (1). The proofs of these and related theorems have recently been made by Dr. S. Epsteen, using the methods in the author's Linear Groups.

These results, however, follow at once from the Galois field theory if we show that the p^n differential expressions (1) define a field identical, aside from notation, with the $GF[p^n]$. To the expression (1) we make correspond the mark

$$c_{n-1}z^{n-1} + \cdots + c_1 z + c_0 \tag{2}$$

of the $GF[p^n]$, where z is a root of the congruence

$$\Delta' z = \delta_n z^n + \cdots \delta_1 z + \delta_0 \equiv 0 \pmod{p},$$

irreducible in view of the above assumption as to Δy. Since product relations are preserved by this correspondence (in view of the symbolic method for products), evidently any rational function of the differentials (1) corresponds to the same rational function of the corresponding marks (2).

An interesting feature of the field of the elements (1) is that the derivative of any element is again an element of the set.

An evident generalization consists in taking as the coefficients of the differential expressions elements of an arbitrary field instead of the special field of the integers modulo p.

THE UNIVERSITY OF CHICAGO,
April 20, 1903.