His work is then incomplete; but this is not a criticism which I make against him. Incomplete one must indeed resign one's self to be. It is enough that he has made the philosophy of mathematics take a long step in advance, comparable to those which were due to Lobachevsky, to Riemann, to Helmholtz, and to Lie.

Since* the printing of the preceding lines, Professor Hilbert has published a new note on the same subject ("Ueber die Grundlagen der Geometrie," *Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen*, 1902, Heft 3). He seems to have made here an attempt to fill in the gaps which I have noticed above. Although this note is very concise, one sees clearly two thoughts running through it. In the first place he seeks to present the axioms of order emancipated from all dependence on projective geometry; he uses for this a theorem of Professor Jordan. Next, he reconnects the fundamental principles of geometry with the notion of a group. He comes nearer then to the point of view of Lie, but he makes an advance on the work of his predecessor, since he frees the theory of groups from all appeal to the principles of the differential calculus.

H. POINCARÉ.

ON LINEAR DIFFERENTIAL CONGRUENCES.

BY DR. SAUL EPSTEEN.

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

IN his note entitled "Sur des congruences différentielles linéaires," Guldberg† concludes that there exists for linear differential forms a theory which is analogous to the Galois field theory. Being unable to find anything on this subject beyond that written by Guldberg, it may be permitted me to correct him in some points and to give a brief résumé of some additional results.

---

*[See footnote at the beginning of this translation. Since this postscript was written, still another article by Hilbert has appeared: "Ueber die Grundlagen der Geometrie," *Math. Annalen*, vol. 56 (1902), pp. 381–422. *Tr.*]

†Guldberg, *Comptes rendus*, vol. 125 (1897), p. 489.

I define a differential Guldberg field ($DGuF$) analogous to the Galois field (GF) and show, 1° that every finite differential field is a $DGuF$, and 2° that there exists one and only one $DGuF$ of order p^n, p being a prime and n any integer.

§ 1.

This section is mainly a summary of Guldberg's results. We consider linear differential forms with integral coefficients

$$D(y) = Dy = \sum_{i=0}^{n} a_i \frac{d^i y}{dx^i}$$

and agree to understand the word "product" in the well known symbolic sense of Boole.*

If $D_1 y = D_2 y + p \cdot D_3 y$, then we may write the congruence $D_1 y \equiv D_2 y \pmod{p}$. When a differential expression Dy is given, we first reject the terms whose coefficients are multiples of p, then if $Dy = D_1 y \cdot D_2 y \pmod{p}$, we say that $D_1 y$ and $D_2 y$ are divisors of Dy modulo p.

In one and only in one of the *associated* forms $1\,D$, $2\,D$, $3\,D$, $\cdots$, $(p-1)D$ is the coefficient of the term of highest order congruent to 1 modulo p. This one is called the *principal* form.

A form D which is not divisible by other differential forms (except by its associated forms) is said to be *irreducible* or *prime* modulo p.

An algorithm analogous to Euclid's for finding the greatest common divisor holds† and from this it can be shown that: Any Dy (or simply D) can be decomposed in one and only one way into the product of an integer and irreducible principal forms.

The fact that D is divisible by Δ, modulo p can be expressed thus: $D \equiv 0 \pmod{p, \Delta}$, which means that $D = \phi \cdot \Delta + p \cdot D_1$. Likewise $D_1 \equiv D_2 \pmod{p, \Delta}$ means that $D_1 = \phi \cdot \Delta + pD_3 + D_2$. If Δ is of order n, any form D is congruent to one and only one of the p^n forms

$$\sum_{0}^{n-1} a_i \frac{d^i y}{dx^i}$$

* Boole's Differential Equations, p. 381.

† Although Guldberg's conclusions are correct in a general sort of way his notation is not always so, he does not seem to notice that in this theory integers cannot appear by themselves, but are always accompanied by y or a derivative of y (zero excepted). See also the correction at the end of this section.

modulis (p, Δ), where the coefficients a_i take all the values $0, 1, 2, \cdots, (p-1)$. These p^n expressions constitute a complete system of residues moduli (p, Δ).

The chief result attained by Guldberg is a generalization of Fermat's theorem: Let Δy be an irreducible form of order n and Dy a residue prime to Δ, then $Dy^{p^n-1} \equiv 1 \pmod{p, \Delta}$.*

§ 2. *The Differential Guldberg Field.*†

Let Δ [*i. e.*, $\Delta(y)$] be a linear homogeneous differential form of order n having integral coefficients not all divisible by a given integer p. If an arbitrary form D, likewise with integral coefficients, is divided by Δ there results a quotient Q and a remainder which can be written $\phi(y) + p \cdot \psi(y)$, where ϕ is of the form

$$\phi = \sum_{i=0}^{n-1} a_i \frac{d^i y}{dx^i},$$

each a_i belonging to the series $0, 1, 2, \cdots, (p-1)$. Then $D = \phi + p \cdot \psi + \Delta \cdot Q$. The totality of functions obtained by giving to Q and ψ all possible forms will be said to constitute a class of residues; two functions are congruent if, and only if, they belong to the same class of residues. Evidently there are p^n residues. From

$$D_i = \phi_i + p \cdot \psi_i + \Delta \cdot Q_i \qquad (i = 1, 2)$$

we see that the classes to which $D_1 \pm D_2$ or $D_1 \cdot D_2$ depends merely upon $\phi_1 \pm \phi_2$ and $\phi_1 \cdot \phi_2$. Suppose we differentiate D_1 twice and D_2 once and add

---

* We shall see in § 2, No. 6, that this should read $Dy^{p^n-1} \equiv y \pmod{p, \Delta}$.

† In § 2, Dickson's Linear Groups, Chapters I and II, are closely followed. The analogy with the Galois field theory is necessarily very close, indeed at most times it is scarcely more than a difference in notation, differential forms taking the place of algebraic forms; for example:

In Galois field theory

$$(a_\alpha Z^\alpha + \cdots + a_0)(b_\beta Z^\beta + \cdots + b_0) = a_\alpha b_\beta Z^{\alpha+\beta} + \cdots + a_0 b_0.$$

In Guldberg field theory

$$\left(a_\alpha \frac{d^\alpha}{dx^\alpha} + \cdots + a_0\right)\left(b_\beta \frac{d^\beta}{dx^\beta} + \cdots + b_0\right) y = a_\alpha b_\beta \frac{d^{\alpha+\beta} y}{dx^{\alpha+\beta}} + \quad + a_\alpha b_\beta y.$$

$$D_1'' + D_2' = \phi_1'' + \phi_2' + p(\psi_1'' + \psi_2') + \Delta'' Q_1 + \Delta'(2Q_1' + Q_2) + \Delta(Q_1'' + Q_2').$$

Since multiplication is symbolic we have $\Delta' = \Delta \cdot y', \Delta'' = \Delta \cdot y''$, whence

$$D_1'' + D_1' = \phi_1'' + \phi_2' + p(\psi_1'' + \psi_2') + \Delta(y'' Q_1 + 2y' Q_1' + y_1' Q_2 + Q_1'' + Q_2').$$

Similarly, upon multiplying, there results an expression of the form $D_1'' \cdot D_2' = \phi_1'' \phi_2' + p \cdot \Phi + \Delta \cdot \Psi$; and in general, when we differentiate D_1 r times and D_2 s times, the results of addition and multiplication are of the form

$$D_1^{(r)} \pm D_2^{(s)} = \Phi_1 + p\Psi_1 + \Delta\theta_1$$
$$D_1^{(r)} \cdot D_2^{(s)} = \Phi_2 + p\Psi_2 + \Delta\theta_2.$$

Hence, after any number of differentiations, classes of residues combine without ambiguity, under addition, subtraction and multiplication. In order that division of any arbitrary class by any class $C(\neq 0)$ shall lead uniquely to a third class, it is necessary and sufficient that p shall be prime and Δ irreducible modulo p.

The p^n classes of residues above defined form what we shall call a Guldberg field $GuF(p^n)$ of order p^n (it being understood that p is a prime and Δ is irreducible modulo p). Sometimes for clearness we shall speak of it as a *differential* field $DGuF(p^n)$.

Example:

$$\text{Let } p = 3, \text{ and } \Delta = \frac{d^2y}{dx^2} - \frac{dy}{dx} - y.$$

The 3^2 residues are

$$0, y\left(=\frac{d^0y}{dx^0}\right), \quad -y, \quad \frac{dy}{dx}, \quad \frac{dy}{dx}+y, \quad \frac{dy}{dx}-y, \quad -\frac{dy}{dx},$$
$$-\frac{dy}{dx}+y, \quad -\frac{dy}{dx}-y.$$

We should notice at this point that there does not arise a numerical residue (excepting 0).

The sum, difference, product or derivative of any two of these may be reduced moduli 3 and $y'' - y' - y$ to one of the nine residues. Moreover the quotient of any one by any residue except 0 may be reduced to one of the set. It will be necessary, however, to bear in mind that multiplication and division are symbolic, for this reason it is best to write

$$y = \frac{d^0 y}{dx^0} = y^{(0)},$$

thus making it clear that

$$\frac{d^i y / dx^i}{y} = \frac{d^i y}{dx^i}.$$

$$\frac{y}{dy/dx} = \frac{y^{(0)}}{y'} = \frac{y^{(0)}(y' - y^{(0)})}{y'(y' - y^{(0)})} = \frac{y' - y^{(0)}}{y'' - y'} = \frac{y' - y^{(0)}}{y^{(0)}}$$

$$= y' - y^{(0)} = y' - y.$$

The nine residues thus form a $DGuF(3^2)$. It should be noticed that for purposes of multiplication $y = y^{(0)} = \frac{d^0 y}{dx^0}$ acts like an ordinary unit.

1° Theorem: If two differential forms D and Δ having integral coefficients admit of no common divisor containing y or its derivatives modulo p, p being a prime, we can determine two functions D_1 and Δ_1 having integral coefficients such that

$$D_1 \cdot D - \Delta_1 \cdot \Delta \equiv y \pmod{p}.$$

The proof is analogous to that in Linear Groups, page 8.

Consider a general field $F(s)$ composed of a finite number of elements $v_0, v_1, \cdots, v_{s-1}$ which have the property of *not vanishing when differentiated any number of times with respect to* x. As there exists every difference, the zero element must be a mark of the field. However, this zero element is in a sense extraneous, no other number can occur in the field unless multiplied by a v. This assumption is made in order to have all the differential forms which will arise homogeneous. Any number of differentiations of a mark of the field is still a mark of the field. We will therefore change the notation somewhat and write for the marks

$$o,\ u_0,\ u_1,\ \cdots,\ u_{s-2}.$$

Denoting by p the least integer such that $v_p = 0$, the p marks

$$o,\ u_0,\ u_1,\ \cdots,\ u_{p-2}$$

are all distinct.

2° Theorem: This integer p is a prime. (For the proof *cf.* Linear Groups, page 9.)

3° Theorem: The order of $F(s)$ is a power of p (*cf.* Linear Groups, page 10).

4° Theorem. Any mark u of $F(s=p^n)$ satisfies a differential equation of order $k \leqq n$, viz.,

$$\sum_{i=0}^{k} c_i \frac{d^i U}{dx^i} = 0 \qquad (c_k \neq 0,\ k \leqq n)$$

(*cf.* Linear Groups, page 10).

The least positive integer e for which

$$\frac{d^e u}{dx^e} = u = \frac{d^0 u}{dx^0}$$

we will call the *period* of the mark u and u will be said to belong to the exponent e. The marks $u^{(0)}, u', u'', \cdots, u^{(e-1)}$ are all distinct.

5° Theorem: The period of any mark ($\neq 0$) of the differential field $DF(p^n)$ is a divisor of $p^n - 1$ (*cf.* Linear Groups page 11).

6° Theorem: Every mark of the $DF(p^n)$ satisfies the equation

$$\frac{d^{p^n-1}u}{dx^{p^n-1}} = u.*$$

Since $d^e u/dx^e = u^{(0)}$ and $u^{(0)}, u', u'', \cdots, u^{(e-1)}$ are all distinct, it follows that all these e marks can be obtained from any one of them by differentiation; and it is clear then that when a certain number of marks $u_1, u_2, \cdots$ are given all the other marks of the field can be obtained from these by differentiation.

---

* Guldberg (*loc. cit.*) incorrectly gives this as $\frac{d^{p^n-1}u}{dx^{p^n-1}} = 1$.

7° Theorem : If two marks u_1, u_2 belong respectively to the exponents e_1, e_2 which are relatively prime, their product $u_1 \cdot u_2$ belongs to the exponent $e_1 \cdot e_2$ and

$$\frac{d^{f_1}u_1}{dx^{f_1}} \; \frac{d^{f_2}u_2}{dx^{f_2}} \quad \begin{pmatrix} f_1 = 0, 1, \cdots, e_1 - 1 \\ f_2 = 0, 1, \cdots, e_2 - 1 \end{pmatrix}$$

are all distinct (*cf.* Linear Groups, pages 11–12).

8° Theorem : Any equation of the kth order cannot have more than k linearly independent integrals (solutions) which belong to the field unless it is an identity, when every mark of the field is an integral.

9° Theorem : For every divisor f of $s - 1$ the equation $d^f U/dx^f = U$ has in the DF $(s = p^n)$ exactly f solutions (*cf.* Linear Groups, page 12).

A mark belonging to the exponent $s - 1$ is called a *primitive integral* of the equation $d^{s-1}U/dx^{s-1} = U$ and also a primitive integral of the DF (s). Since $\frac{du}{dx}, \frac{d^2u}{dx^2}, \cdots, \frac{d^{s-1}u}{dx^{s-1}}$ are all distinct we have

10° Theorem : The $p^n - 1$ marks $(\neq 0)$ of the DF $(s = p^n)$ are the $p^n - 1$ successive derivatives of a primitive integral of that field (*cf.* Linear Groups, page 13).

Corollary : If d is a divisor of $p^n - 1$, the mark $d^{\frac{p^n-1}{d}} u/dx^{\frac{p^n-1}{d}}$ belongs to the exponent d.

We may now identify the field $F(s)$ with the Guldberg field of order $s = p^n$ and show that not more than one such field can exist, in a manner quite analogous to the corresponding investigation for the Galois field theory (*cf.* Linear Groups, pages 13–14) and thus arrive at the theorem which corresponds to the theorem of Moore.*

Fundamental Theorem : *Every existent differential field of order s may be represented as a Guldberg field of order* $s = p^n$. *The* $DGuF$ (p^n) *is defined uniquely by its order ; in particular, it is independent of the special irreducible differential congruence used in its construction.*

There remains now to be shown that *for any integer n there exists at least one irreducible differential congruence of order n.* This is easily accomplished in a manner which is analogous to

* E. H. Moore, Chicago Congress Mathematical Papers ; BULLETIN, December, 1893.

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.