I hope, however, to have shown in this sketch the origin and reason of the close bonds which unite analysis with geometry and with physics, more generally with every science bearing on quantities which can be measured numerically. The mutual influence of analysis and the physical theories has been in this respect particularly instructive. What has the future in reserve? More difficult problems, corresponding to a higher order of approximation, will introduce complications that we can only vaguely foresee, speaking, as I did just now, of functional equations replacing systematically the differential equations of our present time, or again of integration of equations infinite in number, and involving an infinity of unknown functions. But whatever happens, mathematical analysis will always remain that language which, in Fourier's words, "has no symbols to express confused thoughts," a language endowed with a wonderful power of transformation and able to condense within its formulas an immense number of results.

ON THE CLASS OF THE SUBSTITUTIONS OF VARIOUS LINEAR GROUPS.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society, April 29, 1905.)

1. In a recent memoir * by M. Edmond Maillet the question of the possible number of real elements of a geometric configuration (such as the 27 straight lines on a cubic surface) is made to depend upon the class of the substitutions of the Galois group G of the equation determining the elements or of any known group containing G. In view of such an application in various geometric and function-theoretic problems, Maillet emphasizes the importance of a knowledge of the class of the substitutions of various linear modular groups. For the general linear group on m variables with coefficients modulo n, Maillet determines completely the class of its substitutions when n is a prime, while for n a power of a prime he determines a set of

* *Annales de l'Université de Toulouse* (2), vol. 6 (1904), pp. 277–349. In a paper to appear in the July number of the *Annals of Mathematics*, I obtain wide generalizations of Màillet's geometric results, the methods employed being much simpler than his.

numbers among which the classes must occur. The analysis employed to obtain these incomplete results is very elaborate.

Some years ago I effected an immediate determination of the class of the substitutions S of the m-ary linear homogeneous group in the Galois field of order p^n, when represented [*] as a substitution group on the $p^{nm} - 1$ symbols $\lambda_1\xi_1 + \cdots + \lambda_m\xi_m$, the λ's being arbitrary marks not all zero of the $GF[p^n]$ and the ξ's being arbitrary variables. If S leaves fixed the linear functions $f_1, \cdots, f_k$ of the ξ's, it leaves fixed $\mu_1 f_1 + \cdots + \mu_k f_k$, for arbitrary marks μ_i. Any linear homogeneous function with coefficients in the $GF[p^n]$ is either linearly independent of $f_1, \cdots, f_k$ or else is expressible in the form $\sum \mu_i f_i$. Hence the number of distinct linear functions whose coefficients are marks not all zero and which are invariant under S is of the form $p^{nt} - 1$. Hence the class (the number of letters displaced) is $p^{nm} - p^{nt}$ ($t = 0, 1, \cdots,$ or $m - 1$), the identity substitution not being considered. That there exist substitutions of each of these classes follows [†] as in § 2.

Although the preceding representation of the linear group is the more advantageous in the theory of linear groups and renders the preceding theorem quite obvious, I shall employ in the remainder of the paper the representation [‡] on the letters $l_{\xi_1, \ldots, \xi_m}$, written also $(\xi_1, \cdots, \xi_m)$, the ξ's being marks of a Galois field (or else integers modulo n), this method (used also by Maillet) being more suitable for the applications.

2. Theorem I. *The general m-ary linear homogeneous group in the $GF[p^n]$ contains substitutions of classes $p^{nm} - p^{nt}$ ($t = 0, 1, \cdots, m - 1$) exclusively, and is m-fold incompletely transitive. For the non-homogeneous group the only additional class is p^{nm}; it is $(m + 1)$-fold incompletely transitive. The class of the two groups is $p^{nm} - p^{n(m-1)}$.*

As the substitution $\xi_i' = \xi_i + 1 (i = 1, \cdots, m)$ displaces all p^{nm} letters, and as the non-homogeneous group is transitive, it

[*] Linear Groups, § 98; *American Journal*, vol. 23 (1901), pp. 337–377.

[†] By taking the transposed of the matrices of the substitutions there given.

[‡] To connect the two methods, we note that S replaces $l_{\xi_1, \ldots, \xi_m}$ by $l_{\xi_1', \ldots, \xi_m'}$, where $\xi_i' = \sum_{j=1}^{m} a_{ij}\xi_j$, and replaces $\sum \lambda_i \xi_i$ by $\sum \lambda_i' \xi_i$, where $\lambda_i' = \sum_{j=1}^{m} a_{ji}\lambda_j$. It follows readily that S leaves fixed the same number of symbols in each case and that the corresponding permutations are *similar*. Further, for the general linear group, the hyperorthogonal, the abelian, the two hypoabelian, and the first orthogonal groups, the transposed matrix belongs to the group, so that the two representations are identical.

suffices to determine the class of the substitutions leaving fixed $l_{0,\ldots,0}$, viz., of the homogeneous substitutions

$$(1) \qquad \xi_i' = \sum_{j=1}^{m} \alpha_{ij}\xi_j \qquad (i=1,\cdots,m).$$

But if (1) leaves fixed the letters $(\xi_i) \equiv (\xi_1,\ldots,\xi_m)$ and (ξ_i^*), so that

$$\xi_i = \Sigma\alpha_{ij}\xi_j, \qquad \xi_i^* = \Sigma\alpha_{ij}\xi_j^* \qquad (i=1,\cdots,m),$$

it leaves fixed $(\alpha\xi_1 + \beta\xi_1^*, \cdots, \alpha\xi_m + \beta\xi_m^*)$, for arbitrary marks α, β. Hence all the letters left fixed by (1) may be expressed in the form

$$(2) \qquad \left(\sum_{j=1}^{t}\mu_j\xi_1^{(j)}, \cdots, \sum_{j=1}^{t}\mu_j\xi_m^{(j)}\right), \ (\mu_1, \cdots, \mu_t \text{ arbitrary marks}),$$

in which the letters $(\xi_i^{(1)}), \cdots, (\xi_i^{(t)})$ are independent in the sense that (2) is $(0, \cdots, 0)$ if and only if $\mu_1 = \cdots = \mu_t = 0$. Hence the number of fixed letters is p^{nt} and the classes $p^{nm} - p^{nt}$.

It remains to exhibit a substitution which leaves fixed only the p^{nt} letters (ξ_i) with $\xi_1, \cdots, \xi_t$ arbitrary, $\xi_{t+1} = \cdots = \xi_m = 0$. If $p^n > 2$, we take

$$\xi_i' = \xi_i \ (i=1,\cdots,t), \xi_j' = \alpha\xi_j \ (j = t+1, \cdots, m), \ \alpha \neq 0,\ 1.$$

If $p^n = 2$, $m = 1$, S is the identity. If $p^n = 2$, $m > 1$, we take

$$\xi_i' = \xi_i (i=1,\cdots,t-1), \xi_m' = \xi_m, \xi_j' = \xi_j + \xi_{j+1} (j=t,\cdots,m-1);$$

$$\xi_i' = \xi_{i+1}(i = 1, \cdots, m-1), \qquad \xi_m' = \xi_m' + \xi_1;$$

according as $t > 0$ or $t = 0$.

Confining our attention to substitutions of determinant 1, we derive the

COROLLARY. *The special m-ary linear homogeneous group in the* $GF[p^n]$ *contains substitutions of classes* $p^{nm} - p^{nt}$ $(t = 0, 1, \cdots, m-1)$ *exclusively and is* $(m-1)$*-fold incompletely transitive. The special non-homogeneous group contains in addition only substitutions of class* p^{nm} *and is m-fold incompletely transitive.*

3. THEOREM II. *For any integers m and n, the general m-ary linear homogeneous group modulo n contains substitutions of classes*

$n^m - d_i$ *exclusively, where* d_i *ranges over the divisors*[*] *of* n^m. *For the non-homogeneous group the only additional class is* n^m.

The proof begins as in § 2. The letters invariant under (1) may be expressed in the form (2), which now, however, may reduce to $(0, \cdots, 0)$ without necessitating $\mu_1 \equiv \cdots \equiv \mu_t \equiv 0 \pmod{n}$. The number of distinct letters (2) is the number d of the distinct linear functions (compare § 1) $\sum_{j=1}^{t} \mu_j f_j$, when $\mu_1, \cdots, \mu_t$ range independently over all integers modulo n, where

$$f_j = \xi_1^{(j)} \xi_1 + \xi_2^{(j)} \xi_2 + \cdots + \xi_m^{(j)} \xi_m \quad (\xi_1, \cdots, \xi_m \text{ arbitrary variables}).$$

Hence d is the number of distinct elements of the *modul*[†] $[f_1, \cdots, f_t]$. It is thus readily proved that d is a divisor of n^m. This result may also be shown[‡] by a direct consideration of the number of incongruent sets of solutions of

$$(1') \quad a_{i1}\xi_1 + \cdots + a_{i\,i-1}\xi_{i-1} + (\alpha_{ii} - 1)\xi_i + \alpha_{i\,i+1}\xi_{i+1} + \cdots + \alpha_{im}\xi_m \equiv 0 \pmod{n}.$$

It remains to exhibit a substitution which leaves fixed exactly d_i letters. In view of § 2 we may assume here that n is not prime. For $n > 2$, it suffices to employ a combination of the following types of substitutions:

$$\xi_1' = (1 + \delta)\xi_1, \quad \xi_i' = \xi_i \, (i > 1), \quad \delta \text{ a divisor} < n \text{ of } n;$$

$$\xi_1' = \xi_1 + \delta_2 \xi_2, \quad \xi_2' = \xi_2 + \delta_1 \xi_1, \quad \xi_i' = \xi_i \, (i > 2),$$
$$\delta_1, \delta_2 \text{ divisors of } n, \ \delta_1\delta_2 \neq 1;$$

$$\xi_1' = 2\xi_1 + \xi_2, \quad \xi_2' = \xi_1 + \xi_2, \quad \xi_i' = \xi_i \, (i > 2);$$

which leave fixed only the letters $(\xi_1, \cdots, \xi_m)$ for which, respectively,

$$\xi_1 \equiv 0 \pmod{n/\delta}; \quad \xi_1 \equiv 0 \pmod{n/\delta_1}, \ \xi_2 \equiv 0 \pmod{n/\delta_2};$$
$$\xi_1 \equiv \xi_2 \equiv 0 \pmod{n}.$$

[*] Positive integral divisors less than n^m.

[†] By an evident extension of Dedekind's definition, Zahlentheorie (4), p. 493, we may reduce the integral coefficients modulo n.

[‡] Bachmann, Arithmetik der quadratischen Formen (1), p. 353. The final step in the proof may also be derived from this reference.

4. Theorem III. *The general or special $2m$-ary linear abelian group in the $GF[p^n]$ contains substitutions of classes $p^{2nm} - p^{nt} (t = 0, 1, \cdots, 2m - 1)$ exclusively.*

In view of Theorem I, it remains only to show that these classes actually occur. Suppressing unaltered variables, we set

$$L_{i1}: \xi'_i = \xi_i + \eta_i; \quad U_i: \xi'_i = \xi_i + \eta_i, \eta'_i = -\xi_i.$$

Then $U_1 U_2 \cdots U_r \ (r \overline{\gtrless} m)$ leaves fixed only the letters with $\xi_i = \eta_i = 0 \ (i = 1, \cdots, r)$; while $U_1 U_2 \cdots U_r L_m (r < m)$ leaves fixed the letters with $\xi_i = \eta_i = 0 \ (i = 1, \cdots, r)$, $\eta_m = 0$.

5. Theorem IV. *The m-ary group H of all hyperorthogonal * substitutions in the $GF[p^{2s}]$ contains substitutions of classes $p^{2sm} - p^{2st} (t = 0, 1, \cdots, m - 1)$ exclusively. The same is true of the subgroup H_1 of determinant unity.*

We apply Theorem I. For H we use a product of the substitutions

$$(3) \qquad T_{i,\tau}: \xi'_i = \tau \xi_i, \ \xi'_j = \xi_j \ (j \neq i), \qquad (\tau^{p^s+1} = 1).$$

For H_1 with $p > 2$, the hyperorthogonal substitution on ξ_1, ξ_2,

$$(4) \qquad V_{12} \equiv \begin{pmatrix} 1 + \rho^{\frac{1}{2}(p^s+1)} & \rho \\ -\rho^{p^s} & 1 - \rho^{\frac{1}{2}(p^s+1)} \end{pmatrix},$$

$$\rho = \text{prim. root } GF[p^{2s}],$$

leaves fixed only the letters with $\xi_2 = -\rho^{\frac{1}{2}(p^s-1)} \xi_1$. Now $W \equiv T_{3,\tau} T_{4,\tau^{p^s}} \ldots T_{2t+1,\tau} T_{2t+2,\tau^{p^s}}$ for $\tau^{p^s+1} = 1, \tau \neq 1$, leaves fixed exactly $p^{2s(m-2t)}$ letters; $V_{12} W$ exactly $p^{2s(m-2t-1)}$ letters. If $m = 3$, a substitution displacing all the letters is $T_{1,\tau} \ T_{2,\tau} \ T_{3,\tau^{2p^s}}$, $\tau^{p^s+1} = 1$, $\tau^2 \neq 1$. If $p = 2$, we use $\binom{01}{10}$ instead of V_{12}.

Corollary. The theorem holds for the hyperabelian † group.

6. Theorem V. *The group O of all m-ary orthogonal substitutions in the $GF[p^n]$ contains substitutions of classes $p^{nm} - p^{nt}$ $(t = 0, 1, \cdots, m - 1)$ exclusively. The subgroup O_1 of orthogonal substitutions o*f *determinant $+1$ contains substitutions of classes $p^{nm} - p^{2kn} \ (k = 0, 1, \cdots, \frac{1}{2}m - 1)$ exclusively if m is even, but of classes $p^{nm} - p^{(2k-1)n} \ (k = 1, \cdots, \frac{1}{2}(m - 1))$ exclusively if m is odd.*

* Leaving invariant $\Sigma \xi_i^{p^s+1}$, Linear Groups, p. 131.

† Linear Groups, p. 115, p. 116 (§138).

For O the result follows from Theorem I and the existence of the orthogonal substitution $C_1C_2\cdots C_t$, where C_i changes the sign of ξ_i but leaves the remaining variables unaltered.

For O_1, we show that if (1) is orthogonal of determinant $+1$, the number of sets of solutions in the $GF[p^n]$ of (1′) is of the form p^{2kn} for m even, and $p^{(2k-1)n}$ for m odd. To this end we apply the theorem * that in the determinant

$$(5) \qquad \begin{vmatrix} a_{11}-1 & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22}-1 & \cdots & a_{2m} \\ \cdot & \cdot & \cdot & \cdot \end{vmatrix}$$

of equations (1′) if all the minors of order $2k$ vanish, then all the minors of order $2k-1$ vanish. Further, (5) vanishes if m is odd, as shown by the fact that the characteristic equation of a substitution of O_1 is a reciprocal equation $-\rho^n+\cdots+1=0$. Finally, $C_1C_2C_3\cdots C_{2t}$ occurs in O_1.

7. Theorem V holds true for the second orthogonal group O' defined by the invariant $\xi_1^2+\cdots+\xi_{m-1}^2+\nu\xi_m^2$, ν a particular not-square in the $GF[p^n]$. Indeed by the transformation $\xi_m^* = \nu^{1/2}\xi_m$, belonging to the $GF[p^{2n}]$, O' becomes O; while any minor in the matrix (5) obtained from a substitution of O' equals a constant times the corresponding minor for O. Hence, by Linear Groups, pages 156–158, *Theorem V holds true for the group of m-ary linear homogeneous substitutions which leave invariant a quadratic form* $\Sigma\gamma_{ij}\xi_i\xi_j$ *with coefficients in the* $GF[p^n]$, $p>2$, *and of discriminant* $\neq 0$.

The group defined by a quadratic form in the $GF[2^n]$ is either simply isomorphic with the abelian group or else is conjugate with one of the hypoabelian groups G_λ, $\lambda=0$ or λ' (Linear Groups, pages 197–201).

8. THEOREM VI. *The 2m-ary hypoabelian group* G_λ *in the* $GF[2^n]$ *contains substitutions of classes* $2^{2nm}-2^{nt}$ $(t=0, 1, \cdots, 2m-1)$ *exclusively.*†

We first apply Theorem I. Next, we note that for G_0 the letters left fixed by M_1, M_1M_2, M_1N_{121}, $M_1M_2N_{121}$, $M_1M_2N_{121}M_3$,

* I derived this theorem independently but later found it stated explicitly by Taber, *Proc. Lond. Math. Soc.*, vol. 27 (1896), p. 613, and inadequately by Voss, *Math. Ann.*, vol. 13, p. 330.

† The case $\lambda=0$, $m=1$, $n=1$ is to be excluded as G_λ is then the identity.

$M_1M_2N_{121}P_{13}$ are given by respectively 1, 2, 3, 4, 5, 6 independent linear relations between the variables, so that a suitable combination of these types leads to a substitution of class $2^{2nm} - 2^{nt}$. For $G_{\lambda'}$, we note that L and $M_1M_mN_{m11}$ (in the notations of Linear Groups, page 201) leave fixed the letters with $\xi_m = \eta_m = 0$, $\xi_m = \eta_m = \xi_1 = \eta_1 = 0$, respectively.

9. THEOREM VII. *The subgroup* J_λ of index two under G_λ contains substitutions of classes $2^{2nm} - 2^{2nj} (j = 0, 1, \cdots, m-1)$ exclusively.*

I have established this theorem for low values of m with n arbitrary; but as the method seems unwieldy for general m, I suppress the proof. This remarkable theorem in connection with Theorem VI furnishes an analogue to Theorem V.

THE UNIVERSITY OF CHICAGO,
February 10, 1905.

NOTE ON A PROBLEM IN MECHANICS.

BY MR. A. M. HILTEBEITEL.

(Read before the American Mathematical Society, February 25, 1905.)

IN an article† inserted in the twenty-eighth volume of the *Giornale di Matematiche*,‡ on the separation of the variables in the equations of the motion of a body acted upon by two fixed centers of force, the author, Dr. Carlo Bonacini, states with inadequate proof that the separation of the variables in the equations of motion is possible only when the two forces vary inversely as the squares of the respective distances of the body from the fixed centers.

That the variables can be separated when the forces vary inversely as the squares of the distances has been known since

* Linear Groups, p. 206, § 205.

† "Sulla separazione delle variabili nelle equazioni del moto di un punto soggetto all'azione di due centri fissi," *Giornale di Matematiche*, vol. 28 (1890), pp. 132–137. (Date of article, May, 1889.)

‡ The object of the paper is given by the author in the following words: "Noi dimostreremo a questo proposito che la separazione delle variabili nelle equazioni del moto è possibile solo quando le due forze sono Newtoniane."