THE GROUP OF A TACTICAL CONFIGURATION.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society, December 29, 1904.)

1. A tactical configuration, connected with the abelian group G_{p^m} of type $(1, 1, \cdots, 1)_m$ and serving to define the general linear homogeneous group H modulo p on m variables, has been given by Professor Moore.* As an obvious generalization, consider the configurations defining the various subgroups of H. The example that I give had its origin in the following problem:† Required the number N_n of all possible ways of separating the $2^{2n} - 1$ operators other than identity of $G_{2^{2n}}$ into $2^n + 1$ sets each of $2^n - 1$ operators, such that the operators of any set together with identity form a subgroup G_{2^n} and such that no two sets have a common operator. Here $G_{2^{2n}}$ is assumed to be an abelian group of type $(1, 1, \cdots, 1)_{2n}$; for example, the group of all linear transformations on $2n$ variables which multiply each variable by ± 1.

2. That such a separation is always possible is easily shown. The group of automorphisms of $G_{2^{2n}}$ may be taken concretely as the group of all linear homogeneous transformations modulo 2 on $2n$ variables. The latter contains ‡ a transformation S whose characteristic equation of degree $2n$ is irreducible modulo 2, so that S is of period $2^{2n} - 1$. In particular, an operator Σ of period $2^n - 1$ occurs. Let $I, a_1, b_1, a_1b_1, \cdots$ be the operators of a subgroup G_{2^n} of $G_{2^{2n}}$. A table of the operators of the latter may be formed with those of G_{2^n} in the first row and with the operators $I, a_2, b_2, \cdots$ of a second G'_{2^n} as multipliers. We may choose $\Sigma = \Sigma_1\Sigma_2$, where Σ_i permutes cyclically the $2^n - 1$ elements $a_i, b_i, a_ib_i, \cdots$, written in a suitable order. As the first set S_1 we take $a_1, b_1, a_1b_1, \cdots$; as the second set S_2 we take $a_2, b_2, \cdots$. To form the third set S_3, take any element, as a_1a_2, in neither S_1 nor S_2, and apply to it the powers of Σ; there result $a_1a_2, b_1b_2, \cdots$. To form the i^{th} set take any element not in $S_1, S_2, \cdots, S_{i-1}$ and apply to it the powers of Σ. In this way we obtain $2^n + 1$ sets with the desired properties.

---

* BULLETIN, vol. 2 (1895), pp. 33–43.
† For $n = 2$, see Burnside, Theory of Groups, p. 60, ex. 2; errata, p. xvi.
‡ Linear Groups, p. 236.

3. For $n = 2$, we take $\Sigma = (a, b, ab)(A, B, AB)$ and obtain

$$S_1 = \{a, b, ab\},\ S_2 = \{A, B, AB\},\ S_3 = \{aA, bB, abAB\},$$
$$S_4 = \{bA, abB, aAB\},\ S_5 = \{abA, aB, bAB\}.$$

A suitably chosen substitution of period 5 on the 15 letters (§2) will permute the S_i in a cycle. The following substitutions leaving a and b unaltered: $(A, aA)(B, bB)$,* (A, B, AB) induce on the S_i the substitutions $(S_2S_3)(S_4S_5)$ and $(S_3S_5S_4)$, respectively. Finally, $(a, b)(A, B)$ induces (S_4S_5). Hence the S_i may be permuted in all 120 ways. Next, in view of their origin, each set S_i is unaltered by Σ and its powers, but by no further substitution. Indeed, if each S_i is unaltered by T, we have $T = T_1T_2$, where T_1 affects the a, b, ab in the same way that T_2 affects A, B, AB. But if the T_i are transpositions, S_4 and S_5 are permuted.

The group of the configuration $S_1, \cdots, S_5$ is an imprimitive G_{360}^{15} which gives rise to all 120 permutations of the S_i.

4. For $n = 3$, we take as Σ

$$(a, abc, c, bc, ab, b, ac)(A, ABC, C, BC, AB, B, AC),$$

the first seven elements forming S_1, the second seven forming S_2. The remaining sets are formed as in §2:

$$S_3 = \{aA, bB, abAB, cC, acAC, bcBC, abcABC\},$$
$$S_4 = \{cA, aB, acAB, abC, abcAC, bBC, bcABC\},$$
$$S_5 = \{abA, cB, abcAB, acC, bcAC, aBC, bABC\},$$
$$S_6 = \{acA, abB, bcAB, abcC, bAC, cBC, aABC\},$$
$$S_7 = \{abcA, acB, bAB, bcC, aAC, abBC, cABC\},$$
$$S_8 = \{bA, bcB, cAB, aC, abAC, abcBC, acABC\},$$
$$S_9 = \{bcA, abcB, aAB, bC, cAC, acBC, abABC\}.$$

Thus Σ leaves each S_i unaltered. Any substitution T on the 63 letters which leaves unaltered each S_i is a power of Σ. In fact, T must affect the large letters in the same way that it does the small, in view of S_3. Now $T\Sigma^s$, where s is suitably chosen,

* The further cycles $(AB, abAB)(bA, abA)(aB, abB)(aAB, bAB)$ are suppressed. The shorter notation suffices as it gives the new generators. The same remark applies throughout.

will leave aB, and hence a, B, A, b, unaltered. But cA occurs in S_4, so that c, and hence C, are unaltered. Hence $T\Sigma^s$ is the identity.

Next S_1 may be thrown into any S_i. Further,

$$(A, aA)(B, bB)(c, cC), \qquad (A, ABC, C, BC, AB, B, AC),$$

each leaving a, b, c unaltered, induce on the S_i the substitutions

$$(S_2S_3)(S_4S_6)(S_7S_9)(S_5S_8), \qquad (S_3S_6S_8S_5S_9S_4S_7),$$

respectively. Hence the group induced on the S_i is triply transitive. The following substitution, leaving S_1, S_2, S_3, a, and A unaltered,

$$(b, bc, ac)(c, ab, abc)(B, BC, AC)(C, AB, ABC)$$

induces the substitution $(S_4S_5S_7)(S_6S_8S_9)$. But there is no substitution T corresponding to one leaving fixed S_1, S_2, S_3, and replacing S_4 by S_6, S_8, or S_9. Employing $T\Sigma^r$ instead of T, where r is suitably chosen, we may suppose that a and A are also fixed. Let then T replace S_4 by S_6. Hence T replaces c by ac, and B by ABC, in view of the coefficients of A and a in S_4 and S_6. But S must affect the large letters in the same way that it affects the small, in view of S_3. Hence T replaces C by AC, and b by abc. Hence T replaces abC of S_4 by $bcAC$, not in S_6. Similarly, T cannot replace S_4 by S_8 or S_9. Finally, an induced substitution which leaves S_1, S_2, S_3, S_4 each fixed, leaves every S_i fixed and is the identity.

The group of the configuration $S_1, \cdots, S_9$ is an imprimitive $G^{63}_{1512 \cdot 7}$ which gives rise to a triply transitive G^9_{1512} on the S_i.

5. Since the $2n$-ary linear homogeneous group H modulo 2 has the order

$$(2^{2n} - 1)(2^{2n} - 2)(2^{2n} - 2^2) \cdots (2^{2n} - 2^{2n-1}),$$

we conclude that $N_2 = 2^3.7$, $N_3 = 2^{12}.3.5.31$. In fact,* every separation of the required kind is conjugate within H with that obtained by Σ in §§3–4.

UNIVERSITY OF CHICAGO,
October, 1904.

* A direct proof is given in the *Amer. Math. Monthly*, Nov., 1904.