A DOUBLY-INFINITE SYSTEM OF SIMPLE GROUPS.

(Abstract of a Paper presented to the Congress of Mathematics at Chicago, August 25, 1893.)*

BY PROF. E. HASTINGS MOORE.

1. *List of orders of systems of simple groups.*

The following is, so far as I know, a complete list of the orders of systems of simple groups which have as yet been determined (q = prime, n = positive integer).

(1) q.

(2) $\frac{1}{2}\,n!$, $\quad (n > 4)$.

(3) $\frac{1}{2}\,q(q^2-1)$, $\quad (q > 3)$;

the group of the modular equation for the transformation of elliptic functions of order q.

(3′) $\frac{1}{2}\,q^n(q^{2n}-1)$, $\quad (q > 2,\ (q, n) \neq (3, 1))$.

$q^n(q^{2n}-1)$, $\quad (q = 2,\ n > 1)$.

This system of simple groups is a generalization of the system (3) to be explained in this paper.

(4) $$\frac{(q^n-1)q^{n-1}(q^{n-1}-1)q^{n-2}\ldots(q^2-1)q}{\delta},$$

$((q, n) \neq (2, 2), (3, 2))$,

in which $\delta = [n, q-1]$, the greatest common divisor of n and $q-1$.

(5) $\frac{1}{2}\,(q^{2n}-1)q^{2n-1}(q^{2n-2}-1)q^{2n-3}\ldots(q^2-1)q$, $\quad (q > 2)$.

$(q^{2n}-1)q^{2n-1}(q^{2n-2}-1)q^{2n-3}\ldots(q^2-1)q$, $\quad (q = 2, n > 2)$.

(6) $(P_n-1)2^{2n-2}(P_{n-1}-1)2^{2n-4}\ldots(P_2-1)2^2$. $\quad (n > 2)$,

in which $P_n = 2^{2n-1} + 2^{n-1}$

* This paper will be published in full in the Proceedings of the Congress. It will also appear as the first part of a paper, "The sub-groups of the simple group whose order is $\frac{1}{2}q^n(q^{2n}-1)$ if $q > 2$, or $q^n(q^{2n}-1)$ if $q = 2$," to be published in the *Mathematische Annalen*.

The systems* (4), (5), (6) are either given by Jordan or are derived from Jordan's decompositions of certain linear groups by the principle that the quotient-group† of any two consecutive groups in the series of composition of any group is a simple group.‡

The systems (1), (2), (3), (6) are simply infinite; the systems (3′), (4), (5) are doubly infinite. It is clear that of the three doubly-infinite systems the new system (3′) is the densest, that is, its orders increase least rapidly as q and n increase.

Professor Cole discovered last spring a new simple group of order 504 not contained in the six systems (1), (2), (3), (4), (5), (6). The facts (a) that in the system (3′) the group having $(q, n) = (3, 2)$, order 360, had previously been identified as holoedrically isomorphic with the alternating group in six letters (a simple group), and (b) that the group having $(q, n) = (2, 3)$ had the order 504 of Cole's new simple group, led to the present investigation.

The simple groups of composite order < 660 have been completely enumerated by Hölder (*Math. Annalen*, vol. 40) and Cole (*Amer. Journal of Math.*, vol. 14; BULLETIN OF NEW YORK MATH. SOCIETY, vol. 2, p. 254, foot-note). They are one group each for the orders 60, 168, 360 and 504. These are all included in the new system (3′), being the groups having, respectively, $(q, n) = (5, 1)$ or $(2, 2)$, $(7, 1)$, $(3, 2)$, and $(2, 3)$.

2. *The simply-infinite system* (3) *of simple groups of order* $\frac{1}{2}q(q^2-1)$, $(q > 3)$.

The formula

$$\omega' \equiv \frac{\alpha\omega + \beta}{\gamma\omega + \delta} \pmod{q},$$

where

$$\alpha\delta - \beta\gamma \equiv 1 \pmod{q}$$

and where $\alpha, \beta, \gamma, \delta$ are integers taken modulo q, and ω, ω' run through the series of $q+1$ values $0, 1, 2, \ldots q-1, \infty$, may be considered an analytic expression of a certain substitution on the $q+1$ symbols or marks $0, 1, 2, \ldots q-1, \infty$. The totality of all such distinct substitutions constitutes a

* See Jordan, "Traité des Substitutions," (4) p. 106, (5) pp. 176, 178, (6) pp. 205, 213. These references were given by Professor Cole in the paper, "On simple groups," presented by him to the Congress.

† See Hölder, *Math. Annalen*, vol. 34.

‡ Two systems of order (6) are given.

group of order $\frac{1}{2}q(q^2-1)$, a particular form of the (abstract) group in question. The group is for every $q > 3$ simple. For an admirable exposition of the properties of this group, together with further references, see Klein-Fricke, "Modulfunctionen," vol. I, pp. 419–491.

The existence and properties of the abstract group as studied under this form depend above all things upon

(a) The existence of the system of q marks, 0, 1, 2, . . . $q-1$, which may be combined by the four fundamental operations of algebra, and in which the $q-1$ marks (0 excluded) are given as the successive powers of one of them (a primitive congruence-root, modulo q);

(b) The introduction of the mark ∞ (due to Galois).

3. *The Galois-field of order $s = q^n$.*

Suppose we have a system of symbols or *marks*, μ_1, μ_2 . . . μ_s, in number s, and suppose that these s marks may be combined by the four fundamental operations of algebra—addition, subtraction, multiplication, and division—the operations being subject to the ordinary abstract operational laws of algebra ($\mu_f + \mu_g = \mu_g + \mu_f$, $\mu_f\mu_g = \mu_g\mu_f$, etc.), and that when the marks are so combined the results of these operations are in every case uniquely determined and belong to the system of marks. Such a system of s marks we call *a field of order s*.

The most familiar instance of such a field, of order $s = q =$ a prime, is the system of q incongruous classes (modulo q) of rational integral numbers a.

Galois discovered an important generalization of the preceding field. Let $F_n(\xi) = \sum_0^n c_i\xi_i$, where the c_i are integers and $c_n = 1$, be irreducible, modulo q. Then the Galois-field of order $s = q^n$, $GF[q^n]$, consists of the system of q^n incongruous classses (modulis q, $F_n(\xi)$) of rational integral functions of ξ with integral coefficients. In this $GF[q^n]$ there exist *primitive roots;* the $q^n - 1$ successive powers of a primitive root are the $q^n - 1$ marks of the field (0 excluded). The $GF[q^n]$ is *uniquely defined* for every $q =$ prime, $n =$ positive integer; that is,

(1) $F_n(\xi)$ which are irreducible (modulo q) do exist;

(2) The $GF[q^n]$ is independent of the particular $F_n(\xi)$ used in its construction.

For the details of this Galois theory, see Serret, "Algèbre supérieure," 5th edition, vol. II pp. 122–189, and Jordan, "Substitutions," pp. 14–18.

It should be remarked further that every field of order s is in fact abstractly considered a Galois-field of order $s = q^n$.

4. *The doubly-infinite system* (3′) *of simple* groups of order* $\frac{1}{2}q^n(q^{2n}-1)$ *if* $q>2$, *or* $q^n(q^{2n}-1)$ *if* $q=2$.

Let α, β, γ, δ be marks of the $GF[q^n]$ satisfying the equation $\alpha\delta-\beta\gamma=1$. Let ω, ω' be variable marks, each assuming, besides the q^n values of the $GF[q^n]$, the value ∞. The formula

$$\omega'=\frac{\alpha\omega+\beta}{\gamma\omega+\delta} \qquad (\alpha\delta-\beta\gamma=1)$$

expresses a certain substitution on the q^n+1 marks ω. The totality of all such distinct substitutions constitutes a group of order $\frac{1}{2}q^n(q^{2n}-1)$ if $q>2$ or $q^n(q^{2n}-1)$ if $q=2$, a particular form of the (abstract) group in question.

For brevity we write hereafter s for q^n and $M(s)=M(q^n)$ for the order. I prove in this paper that this group $G_{M(s)}$ is a simple group in all except the two particular cases

$$\begin{cases} n=1,\ q=2,\ s=2,\ M(s)=\ 6 \\ n=1,\ q=3,\ s=3,\ M(s)=12 \end{cases}$$

when the $G_{M(s)}$ are in fact known to be

$$\begin{cases} \text{the } G_{6=3!} \text{ symmetric substitution-group on } s+1=3 \text{ letters,} \\ \text{the } G_{12} \text{ tetraedron group or alternating substitution-group on } s+1=4 \text{ letters,} \end{cases}$$

and to have as self-conjugate sub-groups

$$\begin{cases} \text{a } G_3 \text{ cyclic-group.} \\ \text{a } G_4 \text{ four-group.} \end{cases}$$

To this end it is necessary *first* to discuss the individual operators and the cyclic and commutative† sub-groups of the $G_{M(s)}$, and *secondly* to establish a diophantine equation for the order of a self-conjugate sub-group, which shall lead to the conclusion that the only self-conjugate sub-groups of the $G_{M(s)}$ are the identity and the $G_{M(s)}$ itself.

5. *The individual operators and the cyclic and commutative sub-groups of the* $G_{M(s)}$.

By an investigation differing somewhat in details from that of Serret‡ and Gierster§ for the case $n=1$, as given

* $(q, n)=(2, 1), (3, 1)$ excepted.

† A group is called *commutative* if its operators are commutative.

‡ Serret: *Comptes Rendus*, 1859, 1860; "Algèbre supérieure," vol. II, p. 368 ff.

§ Gierster: *Math. Annalen*, vol. 18, pp. 319-365; "Die Untergruppen der Galois'schen Gruppe der Modulargleichungen für den Fall eines primzahligen Transformationsgrades."

in Klein-Fricke, "Modulfunctionen," vol. I, pp. 419–450, it is found that *every substitution* (the identity excepted) *determines and lies in one and only one largest commutative sub-group.* These sub-groups may be arranged in three different sets, the groups of each set being conjugate with one another under the $G_{M(s)}$.

I. $s+1$ conjugate commutative G_{s-q^n}. These s^2-1 substitutions are all of period q, and for $q=2$ they are all conjugate, while for $q>2$ they separate into two sets of $\frac{1}{2}(s^2-1)$ conjugate substitutions. The $q-1$ substitutions of a cyclic group G_q belong

for $q>2$ $\begin{cases} n \text{ odd, half to one and half to the other} \\ n \text{ even, all to the same} \end{cases}$ $\Big\}$ set of conjugate substitutions.

II. $\frac{1}{2}s(s+1)$ conjugate cyclic groups $G_{s-\frac{1}{2}}$ if $q>2$, or G_{s-1} if $q=2$.

III. $\frac{1}{2}s(s-1)$ conjugate cyclic groups $G_{s+\frac{1}{2}}$ if $q>2$, or G_{s+1} if $q=2$.

6. *The diophantine equation for the order of a self-conjugate sub-group of the* $G_{M(s)}$.

Let G_d be a self-conjugate sub-group of the $G_{M(s)}$. If it contains one of a set of conjugate substitutions or sub-groups of the $G_{M(s)}$, it will contain all of that set. Whence the G_d contains $\frac{1}{2}s(s+1)$ conjugate G_{d_-} from the conjugate groups (II), and $\frac{1}{2}s(s-1)$ conjugate G_{d_+} from the conjugate groups (III).

Further, the G_d contains either no substitution of period q, or

$\left.\begin{cases} q>2, \ n \text{ odd, all of both sets} \\ q>2, \ n \text{ even, all of one set or of both sets} \\ q=2, \text{ all of the one set} \end{cases}\right\}$ of conjugate substitutions of period q.

The enumeration of the substitutions of the self-conjugate G_d leads to the diophantine equation

$$-\tfrac{1}{2}(s^2-1)h+\tfrac{1}{2}s(s+1)d_-+\tfrac{1}{2}s(s-1)d_+=d,$$

to be satisfied for positive integral values of d, d_-, d_+, h, where d, d_-, d_+ are divisors of $\frac{1}{2}s(s^2-1)$, $\frac{1}{2}(s-1)$, $\frac{1}{2}(s+1)$, respectively, if $q>2$, or of $s(s^2-1)$, $s-1$, $s+1$, respectively, if $q=2$, and where h has the value

$\begin{cases} h=2 \text{ or } 0, \text{ for } q>2, \ n \text{ odd, and for } q=2, \\ h=2, \ 1 \text{ or } 0, \text{ for } q>2, \ n \text{ even.} \end{cases}$

From this equation follows the simplicity of the $G_{M(s)}$ in all except the two particular cases $(q, n) = (2, 1)$ and $(3, 1)$.

THE UNIVERSITY OF CHICAGO, *October* 13, 1893.

NOTE ON MONOGENIC FUNCTIONS OF A SINGLE VARIABLE.

BY PROF. T. CRAIG.

THE following remark is so obvious that it seems impossible that it has not been made before; still neither the writer nor those to whom he has spoken have seen it.

Suppose $P(x, y)$, $Q(x, y)$ to be real functions of the real variables x, y. Form $P + iQ$: in order that this shall be a monogenic function of $x + iy = z$ it is necessary first that P and Q be functions satisfying Laplace's equation

$$\nabla P = \frac{\partial^2 P}{\partial x^2} + \frac{\partial^2 P}{\partial y^2} = 0,$$

$$\nabla Q = \frac{\partial^2 Q}{\partial x^2} + \frac{\partial^2 Q}{\partial y^2} = 0.$$

But it is not sufficient that P and Q satisfy this equation. If P be a solution of the equation, Q must be determined by aid of Cauchy's equations

$$\text{(1)} \qquad \begin{aligned} \frac{\partial P}{\partial x} - \frac{\partial Q}{\partial y} &= 0, \\ \frac{\partial P}{\partial y} + \frac{\partial Q}{\partial x} &= 0: \end{aligned}$$

that is, Q will be given by the integral

$$Q = \int_{(x_0, y_0)}^{(x, y)} -\frac{\partial P}{\partial y} dx + \frac{\partial P}{\partial x} dy,$$

in which the condition of integrability is satisfied, since $\nabla P = 0$.