and by copious references : in the latter point it is entirely deficient. The freedom from mistakes is worthy of note in a first edition, if we neglect the inaccuracies in the reference to articles. In the last line of p. 144 the last term should be $\frac{a}{f^2-a^2}$ not $\frac{ea}{f^2-a^2}$. In line 8 of p. 157 the last term should be $\frac{1}{2}\frac{b^2}{a^2}$ not $\frac{1}{2}\frac{b^2}{a^3}$.

A. STANLEY MACKENZIE.

BRYN MAWR COLLEGE,
BRYN MAWR, PA.

---

# THE SUBSTITUTION GROUPS WHOSE ORDER IS THE PRODUCT OF TWO UNEQUAL PRIME NUMBERS.

BY DR. G. A. MILLER.

The regular groups of order $pq$ ($p$ and $q$ represent prime numbers, $p > q$) were determined by Netto.* It is the object of this paper to determine *all* the substitution groups of this order and to find formulas by means of which their number may be readily found for any given values of $p$, $q$ and $n$ † even if the groups themselves are unknown.

We shall determine the cyclical and the noncyclical groups separately. It will be found that the number of the noncyclical groups, when the values of $p$ and $q$ are such that groups of this type occur, is always equal to or one larger than the number of the cyclical groups for any given values of $p$, $q$ and $n$.

We shall employ the symbol $R\,G_{pq}^{mpq}$ to represent the intransitive group which is obtained by establishing a simple isomorphism between $m$ regular groups of order $pq$. The symbol $G_y^x$ will be used to represent, as usual, any group whose degree is $x$ and whose order is $y$.

## § 1

### *The Cyclical Groups.*

Each one of these groups belongs to one and only one of the following three classes :

* Theory of Substitutions (Cole's edition) § 130.

† $n$ represents the degree of the groups.

(1) Those which may be formed by establishing a $p$, 1 isomorphism between $R\,G_{pq}^{mpq}$* and $G_q^{n-mpq}$, $(m \geqq 1)$. Groups of this class can occur only when $w=a\,q$.† Their number is the largest integer which does not exceed $\frac{a}{p}$.

(2) Those which may be formed by establishing a $q$, 1 isomorphism between $R\,G_{pq}^{mpq}$, and $G_p^{n-mpq}$, $\left(m, \frac{n-m\,p\,q}{p} \geqq 1\right)$. Groups of this class can occur only when $n=b\,p$. Their number is the largest integer which is less than $\frac{b}{q}$.

(3) Those which may be formed by establishing a simple isomorphism between $R\,G_{pq}^{mpq}$ and $G_p^{cp} \times G_q^{n-cp-mpq}$, $\left(c, \frac{n-cp-mpq}{q} \geqq 1\right)$. Their number is equal to the number of solutions of the following Diophantine equation

$$\text{(A}'\text{)} \qquad px+qy=a'+k'pq \ (k'=0, 1, 2, \cdots, k'_1)$$

$(x, y \geqq 1$ ; $a'$=smallest number‡ for which $px+qy=a'$ can be solved and which also satisfies the equation $a+k_1'pq=n$. The last equation determines also $k_1'$.) Since $(A')$ has one solution for $k'=0$, two for $k'=1$, three for $k'=2$, etc., the number $(N')$ of the groups of this class can be readily found by means of the following formula:

$$N'=\frac{1}{2}(k_1'+1)(k_1'+2)$$

The groups are found by making $m=k'$, $c=x$ and $\frac{n-cp+mpq}{q}=y$ in the given simple isomorphism; $k'$, $x$ and $y$ being any set of values that satisfies $(A')$. All the possible cyclical groups are hereby determined. Their total number $(N_1)$ is therefore equal to the number of solutions of

$$\text{(A)} \qquad px+qy= a+kpq \ (k=0, 1, 2, \cdots, k_1)$$

---

* Only the cyclical groups represented by this symbol occur in this §.

† The number symbols throughout the article represent only positive integers.

‡ $a' \leqq 2pq$, cf. Jordan's Traité des substitutions, p. 4. Hence $a'$ can always be found by at most two simple trials.

($x, y \overline{>} 1$ when $k=k_1$; $a=$the smallest number* for which $px+qy=a$ can be solved and which also satisfies the equation $a+k_1pq=n$. The last equation determines also $k_1$.) Hence $N_1$ may be found directly by means of the following formula

$$N_1=\frac{1}{2}(k_1+1)(k_1+2)-m_1$$

$m_1=2$ when $n$ is an exact multiple of $pq$, $m_1=1$ when $n$ is an exact multiple of either $p$ or $q$ but not of both, $m_1=0$ when $n$ is an exact multiple neither of $p$ nor of $q$.

As $k_1$ and $m_1$ can easily be determined for any given values of $p$, $q$ and $n$ the given formula is convenient. When $n=pq$ the corresponding group† will be transitive. All the other groups are intransitive.

## § 2

### *The Noncyclical Groups.*

Each one of these groups contains one and only one self-conjugate sub-group. Its order is $p$. If non-regular transitive groups exist they must be of degree $p$‡ and sub-groups of the metacyclic group $G^p_{p(p-1)}$. This group has one and only one sub-group for each one of the different divisors of $p-1$ §. Hence there is one non-regular transitive group, as well as one regular noncyclical group of order $pq$ whenever $q$ is a divisor of $p-1$.

In the following we shall assume that this condition is fulfilled. We shall denote the group obtained by establishing a simple isomorphism between $l$ of these non-regular transitive groups by the symbol $H^{lp}_{pq}$.

We may construct all the possible non-cyclical groups by first establishing a $p$, 1 isomorphism between $H^{lp}_{pq}$ and $G^{n-mpq-lp}_q$, and then a simple isomorphism between this group and $G^{mpq}_{pq}$ ||. It is clear that $m$ and $l$ cannot both be zero at the same time. The number ($N_2$) of these groups is, therefore, equal to the number of the solutions of the following equation

$$(B) \qquad px+qy=a+kpq \quad (k=0, 1, 2, \cdots k_1)$$

* $a<2pq$ cf. foot-note on $a'$.

† In this case $a=0$, $k_1=1$ and $m_1=2$. Hence $n_1=\frac{2.3}{2}-2=1$.

‡ Since their order must be a multiple of their degree and they must contain the given self-conjugate sub-group.

§ Cf. Netto, l. c. § 132.

|| Only the non cyclical groups represented by this symbol occur in this §.

[$x \overline{\gtrless} 1$ when $k=k_1$; $a$ and $k$ satisfy the same conditions as in $(A)$]. Hence the formula

$$N_2=\tfrac{1}{2}(k_1+1)(k_1+2)-m_2$$

$m_2=1$ when $n$ is an exact multiple of $q$, $m_2=0$ when this is not the case.

The groups may be constructed by making $m=k$, $l=x$ and $\dfrac{n-mpq-lp}{q}=y$ in the given isomorphism, where $k$, $x$ and $y$ are any set of values that satisfy $(B)$.

The total number of groups of order $pq$ is, therefore, equal to $N_1$ when $q$ is not a divisor of $p-1$. In the other case it is equal to $N_1+N_2=N_3$, where

$$N_3=(k_1+1)(k_1+2)-m_3.$$

$m_3=3$ when $n$ is an exact multiple of $pq$; $m_3=2$ when $n$ is an exact multiple of $q$ but not of $p$; $m_3=1$ when $n$ is an exact multiple of $p$ but not of $q$; $m_3=0$ when $n$ is an exact multiple of neither $p$ nor $q$.

## § 3

### *Examples.*

We shall employ the last formula to determine the numbers of the groups of orders 6 and 10 when $n \overline{\lessgtr} 10$* and when $n=50$. It is not difficult to construct the groups according to the given methods.

| *Order* | *Degree* | $a$ | $N_3$ |
|---|---|---|---|
| 6 | 3 | 3 | $(0+1)(0+2)-1=1$ |
| | 4 | 4 | $(0+1)(0+2)-2=0$ |
| | 5 | 5 | $(0+1)(0+2)-0=2$ |
| | 6 | 0 | $(1+1)(1+2)-3=3$ |
| | 7 | 7 | $(0+1)(0+2)-0=2$ |
| | 8 | 2 | $(1+1)(1+2)-2=4$ |
| | 9 | 3 | $(1+1)(1+2)-1=5$ |
| | 10 | 4 | $(1+1)(1+2)-2=4$ |
| | 50 | 2 | $(8+1)(8+2)-2=88$ |
| 10 | 5 | 5 | $(0+1)(0+2)-1=1$ |
| | 6 | 6 | $(0+1)(0+2)-2=0$ |
| | 7 | 7 | $(0+1)(0+2)-0=2$ |
| | 8 | 8 | $(0+1)(0+2)-2=0$ |
| | 9 | 9 | $(0+1)(0+2)-0=2$ |
| | 10 | 0 | $(1+1)(1+2)-3=3$ |
| | 50 | 0 | $(5+1)(5+2)-3=39$ |

* These results may be compared with the lists of these groups in the *Quarterly Journal of Mathematics*, vols. 25, 26 and 27. For the groups of order 6 and degree 9 cf. footnote, ibid. vol. 27, p. 102.

It is clear that the number of these groups increases very rapidly with the increase of $n$. *E. g.*, when $n=1000$, there are $(166+1)(166+2)-2=28{,}054$ of order 6.

This article may be regarded as a continuation of "*The substitution groups whose order is four*," *Philosophical Magazine*, vol. 41 (1896), pp. 431–437.

PARIS, *May*, 1896.

---

# NOTE ON THE SPECIAL LINEAR HOMOGENEOUS GROUP.

BY PROFESSOR HENRY TABER.

On page 232 of the BULLETIN are given the conditions necessary and sufficient in order that a transformation of the special linear homogeneous group in $n$ variables may be generated by the repetition of an infinitesimal transformation of this group. As a corollary of these conditions it ollows that a transformation of this group can be generated fthus if the multiplicities of the several roots of its characteristic equation have no common factor, or if the roots of its characteristic equation are all equal to $+1$. But one or other of these conditions is satisfied if $n$ is an odd prime. Therefore, if $n$ is an odd prime, every transformation of the special linear homogeneous group in $n$ variables can be generated by the repetition of an infinitesimal transformation of this group, that is, belongs to a continuous one-term sub-group containing the identical transformation.

On the other hand, if $n = 2$ or is composite, it follows from the conditions given on page 232 that the special linear homogeneous group in $n$ variables contains an assemblage of transformations no one of which can be generated by the repetition of an infinitesimal transformation of this group. Nevertheless, by the repetition of an infinitesimal transformation of this group we may approximate as nearly as we please to any transformation of this assemblage. Thus corresponding to any transformation $A$ of the special linear homogeneous group that cannot be generated by the repetition of an infinitesimal transformation of this group can always be found a transformation $A_\rho$ of this group, whose coefficients are rational functions of a parameter $\rho$, such that for all but a finite number of the values of $\rho$, $A_\rho$ can be generated by the repetition of an infinitesimal transformation of this group, and by taking $\rho$ sufficiently