$$\psi \equiv S^2 + R^2 - PQ.$$

In terms of the initial variables $x$, $x_1$, $y$, $y_1$, we see that $\psi$ vanishes identically. Also

$$P \equiv |x + Ix_1| \equiv |X|, \quad Q \equiv |Y|,$$
$$\frac{Y}{X} \equiv \frac{R - IS}{P}, \quad \frac{X}{Y} \equiv \frac{R + IS}{Q}.$$

The group $G$ is hemiedrically isomorphic with the group of linear fractional substitutions

$$Z' = \frac{\alpha + \gamma Z}{\beta + \delta Z}, \quad Z \equiv \frac{Y}{X}. \tag{18}$$

The quaternary group on $P$, $Q$, $R$, $S$ is isomorphic with a ternary fractional group on $Q/P$, $R/P$, $S/P$. But

$$\frac{Q}{P} \equiv \left(\frac{R}{P}\right)^2 + \left(\frac{S}{P}\right)^2.$$

Eliminating $Q/P$, we obtain a group of birational quadratic transformations in the plane. It may evidently be obtained more directly from the transformations (18).

THE UNIVERSITY OF CHICAGO,
*January*, 1901.

---

## ON HOLOMORPHISMS AND PRIMITIVE ROOTS.

BY DR. G. A. MILLER.

(Read before the American Mathematical Society, February 23, 1901.)

IN an earlier note* it was observed that every holomorphism of an abelian group with itself can be obtained by establishing an isomorphism between the abelian group and one of its subgroups (which may sometimes be the entire group) and associating the product of corresponding operators with the original operator of the group. The present note is devoted to some additional developments along this line and especially to some elementary results in the theory of numbers which may be derived by this method.

Let $s_1$ represent an operator of order $p^m$ ($p$ being any prime number) and let $P$, the group generated by $s_1$, be

* BULLETIN, Vol. 6 (1900), p. 337.

made isomorphic with one of its subgroups of order $p^{m_1}$, $m_1 < m$. Each operator of $P$ is transformed, by some operator $t$ in the group of isomorphisms of $P$, into itself multiplied by the corresponding operator in this isomorphism. Assuming that $t^{-1} s_\alpha t = s_{\alpha+1} s_\alpha$, we have

$$t^{-n} s_\alpha t^n = s_{\alpha+n} s_{\alpha+n-1}^{n} \cdots s_{\alpha+n-r}^{\frac{n(n-1)\cdots(n-r+1)}{r!}} \cdots s_{\alpha+1}^{n} s_\alpha.$$

It is easy to prove that the order of the product of the operators which are multiplied into $s_\alpha$ is equal to the order of $s_{\alpha+1}^n$ whenever $p$ is odd. In case $n$ is prime to $p$ this follows directly from the fact that each of the factors which precede $s_{\alpha+1}$ is of a lower order than $s_{\alpha+1}$. In general, let $n = kp_\lambda$, $k$ being prime to $p$. The exponent of $s_{\alpha+\beta}$ is divisible by $p^{\lambda-m'}$, where $m'$ is the exponent of the highest power of $p$ that is contained in $\beta$, since the product of $n$ successive numbers is divisible by $n!$. As the order of $s_{\alpha+\beta}$ does not exceed the order of $(s_{\alpha+1})^{p^{\beta-1}}$, the order of the power of $s_{\alpha+\beta}$ which occurs in the above formula cannot exceed $(s_{\alpha+1})^{p^{\lambda+\beta-m'-1}}$. Hence it is less than the order of $s_{\alpha+1}^n$ whenever $\beta > 1$, and *the product of all the factors which are multiplied into $s_\alpha$ is of the same order as $s_{\alpha+1}^n$ when $p$ is odd.*

When $p$ is even we assume that $m_1 < m-1$. With the same notation as above it is clear that the order of $s_{\alpha+\beta}$ does not exceed the order of $(s_{\alpha+1})^{2^{2(\beta-1)}}$. Hence the order of the power of $s_{\alpha+\beta}$ in the formula cannot exceed

$$(s_{\alpha+1})^{2^{\lambda+2\beta-m'-2}}$$

As $m'+2$ is less than $2\beta$ whenever $\beta > 1$, it follows that in this case the order of the product of the factors which are multiplied into $s_\alpha$ is again equal to $s_{\alpha+1}^n$. Hence *$t$ is always of order $p^{m_1}$ and the group of isomorphisms of $P$ contains a cyclic subgroup of order $p^{m-1}$ when $p$ is odd and one of order $2^{m-2}$ when $p$ is even.*

The group of isomorphisms of a cyclic group is abelian,* and can be represented as a regular substitution group whose elements correspond to the operators of highest order in the cyclic group.† Hence the group of isomorphisms of the cyclic group of order $p^m$ is of order $p^{m-1}(p-1)$. In particular, the group of isomorphisms $I$ of the cyclic group of order $2^m$ is of order $2^{m-1}$. We have just found that $I$ contains a cyclic subgroup of order $2^{m-l}$, formed by all its operators which transform into itself an operator of order $2^l$ $(l > 1)$ in $P$.

* *Trans. Amer. Math. Soc.*, vol. 1 (1900), p. 397.

† The order of a cyclic group is said to have primitive roots whenever its group of isomorphisms is cyclic.

The group $I$ contains an operator $s'$ of order two which transforms each operator of $P$ into its inverse. As $s'$ is not contained in the above cyclic subgroup of order $2^{m-2}$, which is composed of all the operators of $I$ which transform an operator of order four in $P$ into itself, it and this subgroup must generate $I$.

It is now easy to determine the exponent to which a number belongs mod $2^m$, since this exponent is the order of the corresponding operator in $I$. In the above mentioned cyclic subgroup of order $2^{m-2}$, an operator of order $2^k$ is commutative with the operators of order $2^{m-k}$ in $P$, but not with those of order $2^{m-k+1}$. From this fact and the fact that $s'$ transforms each operator of $P$ into its inverse it follows that all the numbers which belong to exponent $2^k\,(k>1)$ mod $2^m$ are of the form $\pm\,(l\,2^{m-k}+1)$ where $l$ is any one of the $\varphi(2^k)$ numbers not greater than $2^k$ and prime to $2^k$; and *vice versa*. When $k=1$ we have to add $2^m-1$ to the numbers obtained in this way. Hence the numbers which belong to exponent $2^{m-2}$ are $\equiv 3$ or $5$ mod $8$.*

From what is proved above it follows that the group of isomorphisms $I_1$ of $P$ contains a cyclic subgroup of order $p^{m'-1}$, $p$ being any odd prime, which is composed of all the operators of $I_1$ commutative with each of the operators of order $p$ in $P$. By adding to this subgroup the operators which transform transitively these $p-1$ operators of order $p$, we obtain the $p^{m-1}(p-1)$ operators of $I$. The group of order $p-1$ according to which the operators of order $p$ are transformed contains no more than $d$ operators whose orders divide $d$, any factor of $p-1$, since $x^d\equiv 1$ mod $p$ can have no more than $d$ roots.† Hence it cannot have two subgroups of the same order and must therefore be cyclic. Since $I_1$ is abelian its operators of highest order are obtained by multiplying the operators of order $p-1$ in this cyclic subgroup by the operators of order $p^{m-1}$ in the above mentioned cyclic subgroup of order $p^{m-1}$. Hence $I_1$ is cyclic and the primitive roots of $p^m$ are also primitive roots of $p$.‡ It may be observed that *the above furnishes an independent proof of the existence of primitive roots of* $p^m$. That the cyclic group of order $2p^m$ has the same group of isomorphisms as the cyclic group of order $p^m$ follows directly from the fact that the operator of order two in the former must correspond to itself in every holomorphism of the group with itself. Hence $2p^m$ also has primitive roots.

* Cf. Mathews, Theory of numbers, 1892, p. 30.

† Gauss, Disquisitiones Arithmeticæ, 1801, Art. 54.

‡ Ibid., Art. 92.

The holomorphisms mentioned in the second and third paragraphs show that all numbers of the form $kp^{m-\alpha}+1$, where $k$ is any one of the $\varphi(p^\alpha)$ natural numbers which are not greater than $p^\alpha$ and prime to $p^\alpha$, belong to the exponent $p^\alpha$; $\alpha$ being any positive integer less than $m$ when $p$ is odd and less than $m-1$ when $p$ is even. In the preceding paragraph it is proved that these are the only numbers which belong to an exponent which is a power of an odd prime. The product of all the numbers which belong to exponent $p^{m-1}$, and the $\varphi(p-1)$ powers of a number which is not a primitive root of $p^m$, but belongs to exponent $p-1 \bmod p$, will clearly give all the primitive roots of $p^m$, since the corresponding operators in $I_1$ are all its operators of order $p^{m-1}(p-1)$. In particular the primitive roots of $3^m$ are the products of $3^m-1$ and the numbers of the form $3l+1$, $l$ being any one of the positive integers not greater than $3^{m-1}$ and prime to $3^{m-1}$.

The necessary and sufficient condition that an operator of $I_1$ corresponds to a primitive root of $p^\alpha$ is that its order is divisible by $p-1$ and that its $(p-1)$th power corresponds to a holomorphism of $P$ with itself which may be obtained by establishing a $p$, 1 isomorphism between $P$ and its subgroup of order $p^{m-1}$. Hence *the primitive roots of* $p^\alpha$ $(\alpha>1)$ *are also the primitive roots of every power of* $p$.* The $p$th power of a primitive root of $p$ is also a primitive root of $p$, but the $p$th power of a primitive root of $p^\alpha$ is not a primitive root of $p^\alpha$. The primitive roots of $p$ are therefore not always primitive roots of $p^\alpha$. In fact, we observe directly, from the orders of the operators of $I_1$, that just $\frac{p-1}{p}$ of the primitive roots of $p$ which are less than $p^m$ are also primitive roots of $p^m$.

The preceding considerations can readily be applied to the general cyclic group $C$ of order $2^{\alpha_0}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m}$ ($p_1, p_2, \cdots, p_m$ being odd prime numbers). By making $C$ isomorphic with its subgroup of order $2^{\alpha_0'}p_1^{\alpha_1'}p_2^{\alpha_2'}\cdots p_m^{\alpha_m'}$ (where $\alpha_0' < \alpha_0 - 1$; $\alpha_\gamma' < \alpha_\gamma$, $\gamma = 1, 2, \cdots, m$), and multiplying the corresponding operators, we obtain a holomorphism of $C$ with itself, which corresponds to an operator of order $2^{\alpha_0'}p_1^{\alpha_1'}p_2^{\alpha_2'}\cdots p^{\alpha_m'}$ in its group of isomorphisms. Since the latter group is the direct product† of the groups of isomorphisms of the cyclic groups of orders $2^{\alpha_1}, p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_m^{\alpha_m}$ and since the group of isomorphisms of each one of these groups involves operators of order two whenever the order of the group exceeds two, the

* Lebesgue, *Liouville's Journal*, vol. 19 (1854), p. 344.

† *Trans. Amer. Math. Soc.*, vol. 1 (1900), p. 396.

group of isomorphisms of $C$ is cyclic only when $\alpha_0 = 0$ or 1 and just one of the other exponents differs from 0, or when $\alpha_0 = 1$ or 2 and all the other exponents are 0.*

CORNELL UNIVERSITY,
*February*, 1901.

---

## BESSEL FUNCTIONS.

*Einleitung in die Theorie der Bessel'schen Funktionen.* By PROFESSOR J. H. GRAF und DR. E. GUBLER. Zweites Heft: *Funktionen zweiter Art.* Bern, Wyss and Co., 1900.

THE first part of this work appeared in 1898 and was reviewed in the BULLETIN, February, 1899, pp. 253–8. The general arrangement of the second part is similar to that of the first, the authors again emphasizing the fact that the work is done in the spirit of Schläfli's lectures, the manuscripts of which were in their hands, though many problems are extended and modernized. This fact explains the absence of many important phases of the theory of the Bessel functions which one might expect in a symmetric treatise. Moreover, the authors have been rather overgenerous in their references to papers originating at Bern, omitting others which contained proofs of fundamental theorems prior to their discovery by the Bern school, although probably no plagiarism could be charged. Several fundamental theorems by American authors have received no recognition in the book.

Here, as in Volume I, the loop integral is the principal factor in the investigation, and next in importance is the expansion in series. The differential equation is less frequently used. The procedure is rather original, and frequently markedly different proofs for well-known theorems are given, which in some instances have led to detection of error in papers already published.

The only attempt at a concrete illustration or application is the expansion of a few functions in terms of Bessel functions, though the relations which exist between these functions and others are quite fully brought out.

The second part begins with the expansion of $\frac{1}{x-y}$ in terms of Bessel functions, the result being

* Gauss, Disquisitiones Arithmeticæ, 1801, Art. 92.