p^2 in K. As the product of such operators of order p and p^2 respectively would be of order p^2 but would not be in K, this is impossible. That is, *G cannot involve any operators of order p^2 when the subgroups $H_1, H_2, \cdots, H_\lambda$ have the same order.* In fact, the preceding proof holds when the order of the largest of these subgroups does not exceed p times the order of some other one of them.

The preceding proof can be directly extended so as to apply to any group of any order whatsoever in which all the operators are found in a series of subgroups of the same order such that any two of them have only identity in common. That is, such a group G cannot involve any operator whose order is the square of some number.* Suppose that G involved an operator of order p^2, where p is a prime, and let P represent one of its Sylow subgroups of order p^m. If $P_1, P_2, \cdots, P_\lambda$ represent the subgroups of P which are found in the different subgroups of G which have only identity in common, it follows from what was proved above that not more than one of these subgroups can involve operators of order p^2. The operators whose orders exceed p in P would therefore generate a subgroup of order p^α where α does not exceed $\frac{1}{2}m$. As this is impossible, we have proved that G cannot contain an operator whose order is a square greater than unity.

NOTE ON THE FACTORS OF FERMAT'S NUMBERS.

BY DR. J. C. MOREHEAD.

(Read before the Chicago Section of the American Mathematical Society, April 14, 1906.)

FERMAT'S numbers $F_n = 2^{2^n} + 1$ are known to be prime for $n = 0, 1, 2, 3, 4$, and composite for $n = 5, 6, 7, 9, 11, 12, 18, 23, 36, 38$. By calculating the residues (mod $2^{75}\cdot 5 + 1$) of the reciprocals †

* The minimum order of G is evidently the square of the order of one of these subgroups. Dr. Manning proved that G is abelian whenever it has this minimum order.

† In many cases the residue of $1/2^{2^n}$ (mod N) is more readily calculated than the residue of 2^{2^n}. In the present case $-2^{75}\cdot 5 \equiv 1$ mod $(2^{75}\cdot 5 + 1)$. Therefore $1/2^{2^6} \equiv -2^{11}\cdot 5$, $1/2^{2^7} \equiv 2^{22}\cdot 5^2, \cdots, 1/2^{2^9} \equiv 2^{88}\, 5^8 \equiv -2^{13}\cdot 5^7, \cdots$, $1/2^{2^{12}} \equiv -5^{26}\, 10^{29}$, at which stage division by $2^{75}\cdot 5 + 1$ may be begun.