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 $-2^{75}\cdot 5 \equiv 1 \bmod (2^{75}\cdot 5 + 1)$. Therefore $1/2^{26} \equiv -2^{11}\cdot 5$, $1/2^{27} \equiv 2^{22}\cdot 5^2, \cdots, 1/2^{29} \equiv 2^{88}\, 5^8 \equiv -2^{13}\cdot 5^7, \cdots$, $1/2^{212} \equiv -5^{26}\, 10^{29}$, at which stage division by $2^{75}\cdot 5 + 1$ may be begun.

$$1/2^{26}, \quad 1/2^{27}, \quad 1/2^{28}, \cdots$$

I have found that

$$-1 \equiv 1/2^{273} \pmod{2^{75}\cdot 5 + 1},$$

which establishes the composition of F_{73}.

This leads to an interesting secondary result,—the identification of the *twenty-four place* prime*

$$P = 2^{75}\cdot 5 + 1 = 188\ 894\ 659\ 314\ 785\ 808\ 547\ 841.$$

The prime character of P is a consequence of the fact that all factors of F_{73} must have the form

$$Q = 2^{75}q + 1.$$

For, if P were not prime then a factor of P, $< \sqrt{P}$, and hence not of the form Q, would be a factor of F_{73}.

Further computation recently carried out shows that under $2^{79}\cdot 5 + 1$, the only factors of F_n of the form $2^{\kappa}\cdot 5 + 1$ are

$$2^{7}\cdot 5 + 1, \quad 2^{25}\cdot 5 + 1, \quad 2^{39}\cdot 5 + 1, \quad 2^{75}\cdot 5 + 1;$$

and in fact, for $\kappa < 79$, $2^{\kappa}\cdot 5 + 1$ is prime only for $\kappa = 1, 3, 7, 13, 15, 25, 39, 55, 75$.

An investigation of the numbers $2^{\kappa}\cdot 3 + 1$ shows that $2^{41}\cdot 3 + 1$ is the only number of this form under $2^{105}\cdot 3 + 1$ that is a factor of a Fermat number, the only *odd* values of κ for which $2^{\kappa}\cdot 3 + 1$ is prime being $\kappa = 1, 5, 41$. A prime of the form

$$\Pi = 2^{2\kappa}\cdot 3 + 1$$

cannot be a factor of a Fermat number. For if Π is a factor of F_n, $n \leqq 2\kappa - 2$, the congruence

$$2^{(\Pi-1)/3} \equiv 1 \pmod{\Pi} \tag{1}$$

must be satisfied; and this requires that Π be expressible in the form †

$$\Pi = a^2 + 3b^2 \tag{2}$$

* $2^{61} - 1$ is the highest number hitherto definitely known to be prime. See Seelhoff, *Zeitschrift für Math. u. Phys.*, vol. 31 (1886), p. 178; and Ball, *Messenger*, vol. 21, pp. 34-40.

† For general conditions that $2^{(p-1)/n} \equiv 0 \pmod{p}$, see Cunningham, *Quar. Jour. of Math.*, vol. 37 (1905), pp. 124-135.

where

$$b \equiv 0 \pmod 3. \tag{3}$$

Since a given prime is expressible in not more than one way in the form $a^2 + 3b^2$, and since

$$\Pi = (1)^2 + 3(2^\kappa)^2$$

it follows that condition (3), and therefore (1), is not satisfied.

It is easy to show that *composite* numbers of the forms $2^\kappa \cdot 3 + 1$, $2^\kappa \cdot 5 + 1$ can not be factors of Fermat's numbers.

NORTHWESTERN UNIVERSITY,
April, 1906.

THEORETICAL MECHANICS.

A Treatise on the Analytical Dynamics of Particles and Rigid Bodies; with an Introduction to the Problem of Three Bodies. By E. T. WHITTAKER. Cambridge, The University Press; New York, The Macmillan Company, 1904. xiii+414 pp.

AT Cambridge, England, mathematics means for the most part mechanics, mathematical physics, or even physics sometimes not so very mathematical. The famous tripos — the mathematical tripos, of course, which goes back at any rate to 1747—seems, at least to an outsider, to lay its main stress on the theoretical application of mathematics rather than on pure mathematics. Very likely this is a tradition that has come down from the time of Newton, and it is certainly maintained by the eminent physicists such as Stokes, Kelvin, Maxwell, Rayleigh, J. J. Thomson, who have been high wranglers. This tripos with its great prestige gives an attractive and distinctive touch to the university and although the ever-increasing pressure of pure mathematics, with its possibilities for various kinds of unessential and mediocre work infinitely wider than those to be found in theoretical applied mathematics, will probably tell on the training at Cambridge sooner or later, may we not look forward to that date with some regrets on the general uniformizing that is taking place and lament the fact that other realms than physics are possessed of an entropy? At present, how-