AN EXTENSION OF THE THEORY OF NUMBERS BY MEANS OF CORRESPONDENCES BETWEEN FIELDS.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society, September 4, 1916.)

1. To each number a of a field or domain of rationality R let correspond a unique number $F(a)$ of R. Define two operations $\oplus$ and $\odot$ on the numbers $F(a)$ by the equations

$$F(a) \oplus F(b) = F(a+b), \quad F(a) \odot F(b) = F(ab),$$

holding for any two equal or distinct numbers a, b of R. These operations obey the commutative, associative, and distributive laws of ordinary addition and multiplication. For example,

$$\{F(a) \oplus F(b)\} \odot F(c) = F\{(a+b)c\}$$
$$= \{F(a) \odot F(c)\} \oplus \{F(b) \odot F(c)\}.$$

The set of numbers $F(a)$ combined by these two operations therefore form a field $F(R)$, whose zero of addition is $F(0)$ and unity of multiplication is $F(1)$.

2. In particular, let R be the domain of all rational numbers and let the coefficients of $F(a)$ be rational. If a, b and $a/b = q$ are all integers, then $F(a) = F(b) \odot F(q)$ and $F(a)$ will be said to be divisible by $F(b)$. Since $a = bq + r$ implies

$$F(a) = \{F(b) \odot F(q)\} \oplus F(r),$$

Euclid's process for finding the G.C.D. of two integers a, b leads to the G.C.D. of $F(a)$, $F(b)$. We call $F(a)$ a prime if its only divisors are $F(\pm a)$ and $F(\pm 1)$. When the preceding equation holds, we say that $F(a)$ and $F(r)$ are congruent modulo $F(b)$. It is now a simple matter to enunciate the analogues, for the numbers $F(a)$ and the operations $\oplus$ and $\odot$, of the theorems in the theory of numbers. If p is a prime not dividing a, then $F(a) \odot F(a) \cdots \odot F(a)$, to $p - 1$ factors, is congruent to $F(1)$ modulo $F(p)$. Again, $F(1) \odot F(2) \cdots \odot F(p-1)$ is congruent to $F(-1)$. These analogues to Fermat's and Wilson's theorems follow at once