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

from the latter by the principle of correspondence and need not be proved independently of them. A like remark is true of the reciprocity law and other theorems of the theory of numbers.

3. The advantage of choosing a linear fractional function

$$F(a) = \frac{la + m}{na + t} \quad (lt - mn \neq 0) \tag{1}$$

as our $F(a)$ lies in the fact that the correspondence between the fields R and $F(R)$ is now (1, 1), so that the numbers of R form a field also when combined by the new operations $\oplus$ and $\odot$. We have

$$\alpha \oplus \beta = \frac{(mn^2 - 2ntl)\alpha\beta + l^2t(\alpha + \beta) - ml^2}{-n^2t\alpha\beta + mn^2(\alpha + \beta) + l^2t - 2mnl}, \tag{2}$$

$$\alpha \odot \beta = \frac{(mn^2 + lt^2)\alpha\beta - ml(n + t)(\alpha + \beta) + ml(m + l)}{nt(n + t)\alpha\beta - nt(m + l)(\alpha + \beta) + m^2n + l^2t}. \tag{3}$$

In particular, if $n = 0$, $t = 1$, then $F(a) = la + m$, and

$$\begin{aligned} \alpha \oplus \beta &= \alpha + \beta - m, \\ \alpha \odot \beta &= \frac{1}{l}(\alpha - m)(\beta - m) + m. \end{aligned} \tag{4}$$

The special case of the latter in which l and m are certain expressions in a single parameter was treated by L. Schrutka,* who resorted to computations to prove the associative and distributive laws in this special case and devoted many pages to the proofs of the analogues of theorems in the theory of numbers, without making clear that the results follow at once by correspondence.

4. The operation defined by

$$\alpha \odot \beta = \frac{a\alpha\beta + b(\alpha + \beta) + c}{d\alpha\beta + e(\alpha + \beta) + f} \tag{5}$$

obeys the associative law if and only if

$$be = cd, \quad b^2 + ce = ac + bf, \quad e^2 + bd = ae + df. \tag{6}$$

First, let $a, \cdots, f$ be integers and let $b = b_1d_1$, $c = b_1c_1$, where d_1 and c_1 are relatively prime integers. Then $e = e_1c_1$,

* "Theorie der Polygonalreste," *Monatshefte für Mathematik und Physik*, vol. 16 (1905), pp. 167–192.

$d = e_1 d_1$, where e_1 is an integer. The remaining conditions (6) now hold if and only if $a - e_1 c_1 = q d_1$, $f - b_1 d_1 = -q c_1$, where q is an integer. Next, when $a, \cdots, f$ are any numbers (not necessarily integers) of the field R, the conditions (6) are equivalent to

$$b = b_1 d_1, \quad c = b_1 c_1, \quad e = e_1 c_1, \quad d = e_1 d_1,$$
$$a = e_1 c_1 + q d_1, \quad f = b_1 d_1 - q c_1,$$

where b_1, c_1, d_1, e_1, q are numbers of R. We now have the most general operation (5) under which the numbers of R form a group.

5. We are led to a fraction of the form (5) in which α and β enter linearly if we demand that the inverse operation shall be applicable to every pair of numbers of the field. Suppose that also $\alpha \oplus \beta$ is a similar symmetric function of α and β. If these two operations obey the associative and distributive laws, it seems probable that they must be of type (2) and (3), defined by the linear fractional correspondence (1). This is easily proved for integral functions:

$$\alpha \oplus \beta = A\alpha\beta + B(\alpha + \beta) + C,$$
$$\alpha \odot \beta = a\alpha\beta + b(\alpha + \beta) + c.$$

Of the conditions for $(\alpha \oplus \beta) \odot \gamma = (\alpha \odot \gamma) \oplus (\beta \odot \gamma)$, those which involve γ^2 show that $Aa = Ab = 0$, whence $A = 0$, and the remaining conditions are

$$aC + b = 2Bb, \qquad bC + c = 2Bc + C.$$

By the associative law for $\oplus$, $B^2 = B$, whence $B = 1$. Thus $b = aC$, $c = aC^2 - C$, and we get (4) with $m = -C$, $l = 1/a$.

NOTE ON THE DISTRIBUTION OF QUADRATIC RESIDUES.

BY MR. H. S. VANDIVER.

(Read before the American Mathematical Society, October 30, 1915.)

THE present note relates mainly to the distribution of quadratic residues for a rational prime modulus. A special quadratic form is also considered.