$d = e_1 d_1$, 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.