RINGS OF ARITHMETIC FUNCTIONS

By Eckford Cohen

1. **Introduction.** In another paper [6; see also §4 of this paper], the author considers arithmetic functions defined over the ring of polynomials $\Omega = GF[p^n, x]$. It is the purpose of the present paper to show how the ideas developed in the polynomial case can be applied to the rational case and how the results in both cases can be interpreted algebraically.

Let r be a positive integer and F a field of characteristic 0 containing the r-th roots of unity. Then we say that a function $f(a)$ is (r, F) arithmetic or simply, arithmetic, if it defines a single-valued function in F for every rational integer a, with the requirement that $f(a) = f(a')$ for $a \equiv a' \pmod{r}$. It follows, for example, that $\epsilon_z(a) = e^{2\pi i z a/r}$ is arithmetic for any integer z.

A basic theorem proved in §2 (Theorem 1) states that every arithmetic function $f(a)$ can be expressed uniquely in the exponential form $f(a) = \sum_{z=0}^{r-1} a_z \epsilon_z(a)$, $a_z \in F$. The subject of Cauchy composition is also considered in §2. We define the Cauchy product h of two arithmetic functions f, g by the relation

$$h(n) = f \cdot g = \sum_{n \equiv a+b \pmod{r}} f(a)g(b) \qquad (0 \leq n < r), \tag{1.1}$$

where a and b range over elements of a residue system modulo r such that $n \equiv a + b \pmod{r}$. The methods of this section are completely analogous to those used in the polynomial case, but since knowledge of this case is not presupposed we include a detailed discussion of the topics in question.

In §3 arithmetic functions are considered from the underlying algebraic point of view. In particular, it is shown (Theorem 2) that the set of all such functions forms a commutative semisimple algebra $\mathfrak{A}_r(F)$ which is the direct sum of r fields each isomorphic to F. Certain subrings of $\mathfrak{A}_r(F)$ associated with exponential sums important in number theory are also considered.

In §4 a résumé of analogous results for the polynomial case is given. In §5 a general principle relating to additive congruence problems in both rational and polynomial cases is stated. A simple illustration of this principle with reference to the rational case is given, and the following quadratic problem in Ω is considered: Let P, M be polynomials of Ω, P irreducible and primary of degree π, M of degree $< \pi\lambda$, with $\alpha_1, \cdots, \alpha_{2m}$ nonzero elements of $GF(p^n)$, $p > 2$. It is then required to find the number of solutions of

$$M \equiv \alpha_1 X_1^2 + \cdots + \alpha_{2m} X_{2m}^2 \pmod{P^\lambda} \tag{1.2}$$

in polynomials X_i. It happens that this problem is a generalization of one considered by Dickson [8; §65]; the Dickson result may be obtained by specializing

Received December 5, 1951.