ON CERTAIN FINITE RINGS AND RING-LOGICS

ADIL YAQUB

Introduction. Boolean rings $(B, \times, +)$ and Boolean logics (=Boolean algebras) $(B, \cap, {}^*)$ though historically and conceptionally different, are equationally interdefinable in a familiar way [6]. With this equational interdefinability as motivation, Foster introduced and studied the theory of ring-logics. In this theory, a ring (or an algebra) R is studied modulo K, where K is an arbitrary transformation group in R. The Boolean theory results from the special choice, for K, of the "Boolean group", generated by $x^* = 1 - x$ (order 2, $x^{**} = x$). More generally, in a commutative ring $(R, \times, +)$ with identity 1, the *natural group* N, generated by $x^\frown = 1 + x$ (with $x^\smile = x - 1$ as inverse) proved to be of particular interest. Thus, specialized to N, a commutative ring with identity $(R, \times, +)$ is called a *ring-logic*, mod N if (1) the $+$ of the ring is equationally definable in terms of its N-logic $(R, \times, {}^\frown, {}^\smile)$, and (2) the $+$ of the ring is *fixed* by its N-logic. Several classes of ring-logics (modulo suitably chosen groups) are known [1; 2; 7], and the object of this manuscript is to extend further the class of ring-logics. Indeed, we shall prove the following:

THEOREM 1. *Let R be any finite commutative ring with zero radical. Then, R is a ring-logic, mod N.*

1. The finite field case. Let $(R, \times, +)$ be a commutative ring with identity 1. We denote the generator of the natural group by $x^\frown = 1 + x$, with inverse $x^\smile = x - 1$. Following [1], we define $a \times_\wedge b = (a^\frown \times b^\frown)^\smile$. It is readily verified that $a x_\wedge b = a + b + ab$.

Let $(F_{p^k}, \times, +)$ be a finite field with exactly p^k elements (p prime). We now have the following:

THEOREM 2. *$(F_pk, \times, +)$ is a ring logic (mod N). Indeed, the ring (field) $+$ is given by the following N-logical formula:*

$$x + y = \{(x(yx^{p^k-2})^\frown)\} \times_\wedge \{y((x^{p^k-1})^\smile)^2\} . \tag{1.1}$$

Proof. It is well known that in the Galois field F_{p^k}, we have

$$a^{p^k-1} = 1, a \in F_{p^k}, a \neq 0 . \tag{1.2}$$

we now distinguish two cases:

Received August 29, 1961.