ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

ADIL YAQUB

Ring-logics and certain classes of rings

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3^e série, tome 19, n^o 1 (1965), p. 101-105

<http://www.numdam.org/item?id=ASNSP_1965_3_19_1_101_0>

© Scuola Normale Superiore, Pisa, 1965, tous droits réservés.

L'accès aux archives de la revue « Annali della Scuola Normale Superiore di Pisa, Classe di Scienze » (http://www.sns.it/it/edizioni/riviste/annaliscienze/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

RING-LOGICS AND CERTAIN CLASSES OF RINGS

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 [7]. With this equational interdefinability as motivation, Foster [1; 2] introduced and studied the theory of ring-logics. Indeed, let $(R, \times, +)$ be a commutative ring with unit 1, and let $K = \{\varrho_1, \varrho_2, \ldots\}$ be a transformation group in R. The *K-logic* of the ring $(R, \times, +)$ is the (operationally closed) system $(R, \times, \varrho_1, \varrho_2, \ldots)$ whose class R is identical with the class of ring elements, and whose operations are the ring product « $\times$ » together with the unary operations $\varrho_1, \varrho_2, \ldots$ of K. The ring $(R, \times, +)$ is called a *ring-logic*, mod K if (1) the « $+$ » of ring is *equationally* definable in terms of its K-logic $(R, \times, \varrho_1, \varrho_2, \ldots)$, and (2) the « $+$ » of the ring is *fixed* by its K-logic. The Boolean theory results from the special choice, for K, of the « Boolean group », C, generated by $x^* = 1 - x$ (order 2, $x^{**} = x$). Furthermore, by choosing K to be the « natural group », N, generated by $x^\wedge = 1 + x$, Foster showed [1] that a p-ring with unit is a ring-logic, mod N. Again, by choosing K to be the « normal group », D, where the generator $x^\cap$ of D is now no longer linear, Foster [2] was able to show that a p^k-ring with unit is a ring-logic, mod D. These results naturally suggest the following question: are the groups C, N, D, in any way related, and are they the only possible transformation groups with respect to which the corresponding rings are ring-logics? It turns out that for the class of all p^k-rings (and hence, in particular, for p-rings and Boolean rings) *any* transitive $0 \to 1$ permutation of $GF(p^k)$ induces a transformation group in the corresponding p^k-ring R with respect to which R is a ring-logic.

Indeed, x^*, $x^\wedge$, $x^\cap$ above are merely examples of some transitive $0 \to 1$ permutations of $GF(2)$, $GF(p)$, $GF(p^k)$, respectively, and these in turn induce the above transformation groups C, N, D, with respect to which the corresponding rings are ring-logics.

Pervenuto alla Redazione il 31 Agosto 1964.

1. **The Finite Field Case.** Let $(F_{p^k}, \times, +)$ be a (finite) Galois field with exactly p^k elements (p prime). Then, as is well known, $F_{p^k} = \{0, \zeta, \zeta^2, \ldots, \zeta^{p^k-1} (= 1)\}$ for some ζ in F_{p^k}. We now have the following

THEOREM 1. *Let F_{p^k} be a Galois field, and let ζ be a generator of F_{p^k}. Let $\cap: x \to x^\cap$ be any permutation of F_{p^k}. Then $\cap$ is expressible as a polynomial in x over F_{p^k}.*

PROOF. Denote the elements of F_{p^k} by $x_1, \ldots, x_n$ $(n = p^k)$, and denote $x_i^\cap$ by x_i' $(i = 1, \ldots, n)$. We shall show that $x^\cap$ can be written as

$$x^\cap = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \quad (n = p^k) \tag{1.1}$$

for some $a_0, a_1, \ldots, a_{n-1}$ in F_{p^k}. Since $x_i^\cap = x_i'$ $(i = 1, \ldots, n)$, therefore, (1.1) gives n linear equations in the n unknowns $a_0, a_1, \ldots, a_{n-1}$. Now, the determinant of the coefficients of the a_i is the familiar VanderMonde determinant which, except possibly for sign, is equal to $\prod_{i,j=1, i>j}^{n} (x_i - x_j)$, and hence does not vanish since the x_i are *distinct* elements of F_{p^k}. Hence the above equations are solvable, and the theorem is proved.

We shall from now on be primarily concerned only with *transitive* $0 \to 1$ permutations of F_{p^k}. This simply means a permutation, $\cap$, of F_{p^k} such that (i) $0^\cap = 1$, and (ii) for any given elements α, β in F_{p^k}, there exists an integer r such that $\alpha^{\cap r} = \beta$, where $\alpha^{\cap r} = (\ldots((\alpha^\cap)^\cap)\ldots)^\cap$ (r-iterations). We now have the following

THEOREM 2. *Let, $\cap$, be any transitive $0 \to 1$ permutation of the Galois field F_{p^k}, and let K be the transformation group in F_{p^k} generated by, $\cap$. Then the elements of F_{p^k} are equationally definable in terms of the K-logic $(F_{p^k}, \times, \cap)$.*

PROOF. Since, $\cap$, is a transitive permutation of F_{p^k}, therefore, $F_{p^k} = \{0, 0^\cap, 0^{\cap 2}, \ldots, 0^{\cap p^k-1}\}$. A similar argument shows that, for any x in F_{p^k}, $xx^\cap x^{\cap 2} \ldots x^{\cap p^k-1} = 0$. Hence 0 (and with it $0^\cap, 0^{\cap 2}, \ldots, 0^{\cap p^k-1}$) is expressible in terms of the K-logic, and the theorem is proved.

We recall from [4] the *characteristic function* $\delta_\mu(x)$, defined as follows: for any given $\mu \in F_{p^k}$, $\delta_\mu(x) = 1$ if $x = \mu$, and 0 if $x \neq \mu$.

We now have the following

THEOREM 3. *Let F_{p^k}, K, $\cap$, be as in Theorem 2. Then the characteristic functions $\delta_\mu(x)$, $\mu \in F_{p^k}$, are equationally definable in terms of the K-logic $(F_{p^k}, \times, \cap)$.*

PROOF. Since, $\cap$, is a *transitive* $0 \to 1$ permutation of F_{p^k}, therefore, $\mu^{\cap r} = 0$ for some integer r. Now, one readily verifies that, since $y^{p^k-1} = 1$, $y \neq 0$, $y \in F_{p^k}$, $\delta_\mu(x) = (((x^{\cap r})^{p^k-1})^{\cap p^k-1})^{p^k-1}$, and the theorem is proved.

Now, let, $^{\cup}$, denote the inverse of the $0 \to 1$ transitive permutation, $\cap$, and as in [2], define $a \times_\cap b = (a^\cap \times b^\cap)^\cup$. Then, $a \times_\cap 0 = a = 0 \times_\cap a$. Hence, we have the following « normal expansion formula » [4]

$$f(x, y, \dots) = \overset{\times_\cap}{\underset{\alpha, \beta, \dots, \in F_{p^k}}{\Sigma}} f(\alpha, \beta, \dots)(\delta_\alpha(x)\,\delta_\beta(y)\dots). \tag{1.2}$$

In (1.2), $\alpha, \beta, \dots$ range independently over all the elements of F_{p^k} while $x, y, \dots$ are indeterminates over F_{p^k}. $\overset{\times_\cap}{\underset{\alpha_i \in F}{\Sigma}} \alpha_i$ denotes $\alpha_1 \times_\cap \alpha_2 \times_\cap \dots$, where $\alpha_1, \alpha_2, \dots$ are all the elements of F.

THEOREM 4. *Let,* $\cap$, *be any transitive* $0 \to 1$ *permutation of the Galois field* F_{p^k}, *and let* K *be the transformation group in* F_{p^k} *generated by,* $\cap$. *Then* $(F_{p^k}, \times, +)$ *is a ring-logic, mod* K.

PROOF. By (1.2),

$$x + y = \overset{x_\cap}{\underset{\alpha, \beta \in F_{p^k}}{\Sigma}} (\alpha + \beta)(\delta_\alpha(x)\,\delta_\beta(y)).$$

Now, by Theorem 2 and Theorem 3, the right-side of the above equation equationally definable in terms of the K-logic $(F_{p^k}, \times, \cap)$. Hence the « + » of F_{p^k} is *equationally* definable in terms of the K-logic. Next, we show that $(F_{p^k}, \times, +)$ is *fixed* by ist K-logic. Suppose that $(F_{p^k}, \times, +')$ is another ring with the same class of elements F_{p^k} and the same « $\times$ » as $(F_{p^k}, \times, +)$ and which has the *same logic* as $(F_{p^k}, \times, +)$. To prove that $+' = +$. But this follows since, up to isomorphism, there is *only one* Galois field with exactly p^k elements.

2. **The General Case.** In this section we shall extend the results of Theorem 4 to p-rings and p^k-rings by use of the familiar subdirect structure of these rings [6 ; 5]. Thus, suppose R is a commutative ring with unit 1, and suppose that p is a *prime* integer. R is called a *p-ring* [6] if $a^p = a$, $pa = 0$ for all a in R. Furthermore, R is called a *p^k-ring* [2] if (*i*) $a^{p^k} = a$, $pa = 0$ for all a in R, and (ii) R has a subring (= field) F which is isomorphic to the Galois field F_{p^k} and where $1 \in F$. (Under a somewhat broader definition, p^k-rings were first introduced by McCoy [5]). Clearly, every

p-ring R with unit is a p^k-ring ($k = 1$) (in this case (i) implies (ii) in the above definition, since F can be chosen as the prime field of R). From [5], we now recall the following fundamental subdirect structure

THEOREM 5. *A p^k-ring is isomorphic to a subdirect power of the Galois field F_{p^k}.*

We are now in a position to prove the following

THEOREM 6. *Any p^k-ring R with unit is a ring-logic, mod K, where K is the transformation group in R induced by any transitive $0 \to 1$ permutation, $^\cap$, of F_{p^k}.*

PROOF. By Theorem 5, R is isomorphic to a (not necessarily finite) subdirect power $F_{p^k}^m$ of F_{p^k}. Now, suppose $x = (x_1, x_2, \dots)$ is any element in $R\,(= F_{p^k}^m)$. Define $(x_1, x_2, \dots)^\cap = (x_1^\cap, x_2^\cap, \dots)$, and let K be the transformation group generated by, $^\cap$. We shall now show that $F_{p^k}^m$ is a ring-logic, mod K. Indeed, by Theorem 4, there exists a «logical expression» $\varphi(a, b; \times, ^\cap)$ such that $a + b = \varphi(a, b; \times, ^\cap)$ for all a, b in F_{p^k}. Since the operations are *component-wise* in $F_{p^k}^m$, therefore, for all x, y in $F_{p^k}^m\,(= R)$, we have $x + y = \varphi(x, y; \times, ^\cap)$. Hence the «$+$» of $F_{p^k}^m$ is equationally definable in terms of the K-logic. Next, we show that $F_{p^k}^m$ is fixed by its K-logic. Suppose that $(F_{p^k}^m, \times, +')$ is another ring with the same class of elements and the same «$\times$» as $(F_{p^k}^m, \times, +)$ and which has the same logic as $(F_{p^k}^m, \times, +)$. To prove $+ = +'$. Now, a new «$+'$» in $F_{p^k}^m$ defines and is defined by a new «$+_i'$» in F_{p^k} $(= i - th$ component in $F_{p^k}^m)$ such that $(F_{p^k}, \times, +_i')$ is a ring, for each i. Furthermore, the assumption that $(F_{p^k}^m, \times, +')$ has the same logic as $(F_{p^k}^m, \times, +)$ is equivalent to the assumption that each $(F_{p^k}, \times, +_i')$ has the same logic as $(F_{p^k}, \times, +)$. Since, by Theorem 4, $(F_{p^k}, \times, +)$ is a ring-logic, and hence with its «$+$» fixed, therefore, $+_i' = +$ for each i. Hence $+' = +$, and the theorem is proved.

COROLLARY 7. *Any p-ring R with unit is a ring-logic, mod K, wehere K is the transformation group in R induced by any transitive $0 \to 1$ permutation of F_p.*

This is the case $k = 1$ of Theorem 6.

It is noteworthy to observe that, since there is *only one* $0 \to 1$ (transitive) permutation of F_2, the level of generality given in Theorem 6 and Corollary 7 is not apparent in the Boolean case.

Now, by choosing $a_0, a_1, \dots, a_{p^k-1}$, in (1.1), in all of the $(p^k - 2)!$ available ways tho get *transitive* $0 \to 1$ permutations of F_{p^k}, we obtain the

corresponding transformation groups with respect to which a p^k-ring is a ring-logic. Thus, if in (1.1) we choose, $x^{\cap} = 1 - x$ ($p^k = 2^1$), we recover the generator x^* of the Boolean group C (see introduction). Similarly, if we set $x^{\cap} = 1 + x$ ($p^k = p$) in (1.1), we obtain the generator $x^{\wedge}$ of the natural group N. Finally, by selecting the a_i in (1.1) so that $0^{\cap} = 1, 1^{\cap} = \zeta$, $\zeta^{\cap} = \zeta^2, \ldots, (\zeta^{p^k-3})^{\cap} = \zeta^{p^k-2}, (\zeta^{p^k-2})^{\cap} = 0$, where ζ is a generator of F_{p^k}, we obtain the generator $x^{\cap}$ of the normal group D (see [2]). Hence, we have proved, as a further corollary of Theorem 6, the following theorem which contains Foster's results [1 ; 2] (see also [8]):

COROLLARY 8. (i) *Any Boolean ring with unit is a ring-logic, mod C;* (ii) *any p-ring with unit is a ring-logic, mod N*; (iii) *any p^k-ring with unit is a ring-logic, mod D; where C, N, D, are the Boolean group, natural group, and normal group, respectively.*

REFERENCES

1. A. L. FOSTER, *p-rings and ring-logics*, Univ. Calif. Publ. 1 (1951), 385-396.
2. A. L. FOSTER, *p^k-rings and ring-logics*, Ann. Sc. Norm. Pisa 5 (1951), 279-300.
3. A. L. FOSTER, *The indentities of — and unique subdirect factorization within — classes of universal algebras*, Math. Zeit. 62 (1955), 171-188.
4. A. L. FOSTER, *Generalized « Boolean » theory of universal algebras*, Part I, Math. Zeit. 58 (1953), 306-336.
5. N. H. MCCOY, *Subrings of direct sums*, Amer. J. Math. LX (1938), 374-382.
6. N. H. MCCOY and D. MONTGOMERY, *A representation of generalized Boolean rings*, Duke Math. J. 3 (1937), 455-459.
7. M. H. STONE, *The theory of representations of Boolean algebras*, Trans. Amer. Math. Soc. 40 (1936), 37-111.
8. A. YAQUB, *On certain finite rings and ring-logics*, Pacific J. Math. 12 (1962). 785-790.
9. A. YAQUB, *On the ring-logic character of certain rings*, Pacific J. Math. 14 (1964), 741-747.