Equational classes of rings generated by zero rings and Galois fields

By LEE SIN-MIN in Winnipeg (Canada)

H. WERNER and R. WILLE [6] gave some characterization of those equational classes of rings in which the lattice of congruences of every ring is distributive. They showed that these are precisely the equational classes of rings generated by a finite set of Galois fields, and they also gave a set of identities characterizing these equational classes.

We give in this note a characterization of the equational class of rings generated by all zero rings and a finite number of Galois fields. A ring in such an equational class is a directed sum of its Jacobson radical $J(R)$, which is a zero ring, and its semi-simple part, $R/J(R)$. We also consider the lattice of equational subclasses of this equational class and show that it is distributive.

1. Characterization of $\mathscr{R}_g(P, N)\vee\mathscr{C}_0$.

Let π be the set of all primes, $\mathscr{N}^+$ the set of positive integers, and $\mathscr{P}(\mathscr{N}^+)$ the set of all non-empty finite subsets of $\mathscr{N}^+$.

Let P be a fixed, non-empty, finite subset of π and consider a mapping $N: P\to\mathscr{P}(\mathscr{N}^+)$, i.e., N associates with every $p\in P$ an $N(p)\in\mathscr{P}(\mathscr{N}^+)$. Denote by $\mathscr{R}_g(P, N)$ the equational class of rings generated by the set $\{GF(p^k)\,|\,p\in P,\ k\in N(p)\}$ of Galois fields.

For $S\in\mathscr{P}(\mathscr{N}^+)$ write $\Pi S=n_1\ldots n_k$ if $S=\{n_1, \ldots, n_k\}$, and define $\Pi\emptyset=1$ for the empty set $\emptyset$.

With every element x of a ring we associate the element

$$x^k=\sum_{p\in P}\Big(\prod_{q\in P-\{p\}}q\Big)^{p^{n(p)}-1}x^{p^{n(p)}},$$

where $n(p)=\Pi N(p)$.

Let $\mathscr{K}_1$ and $\mathscr{K}_2$ be two equational classes of algebras of the same type, $\mathscr{K}_1$ and $\mathscr{K}_2$ are independent if there exists a binary polynomial symbol $\mathbf{p}(x, y)=x$ is an identity in $\mathscr{K}_1$ and $\mathbf{p}(x, y)=y$ is an identity in $\mathscr{K}_2$.

G. GRÄTZER, H. LAKSER and J. PLONKA [1] showed that if $\mathscr{K}_1$ and $\mathscr{K}_2$ are independent, then every algebra in $\mathscr{K}_1 \vee \mathscr{K}_2$ (the smallest equational class of algebras containing $\mathscr{K}_1$ and $\mathscr{K}_2$) is the direct product of an algebra in $\mathscr{K}_1$ and another in $\mathscr{K}_2$. If, in addition, each algebra $\mathscr{A}$ of $\mathscr{K}_1 \vee \mathscr{K}_2$ has a modular congruence lattice then each $\mathscr{A} \in \mathscr{K}_1 \vee \mathscr{K}_2$ has, up to isomorphism, a unique representation $\mathscr{A} = \mathscr{A}_1 \times \mathscr{A}_2$ where $\mathscr{A}_1 \in \mathscr{K}_1$ and $\mathscr{A}_2 \in \mathscr{K}_2$.

Let $\mathscr{C}_0$ denote the class of all zero rings, i.e. $\mathscr{C}_0$ consists of all rings satisfying $xy=0$.

Theorem 1. *$\mathscr{R}_g(P, N)$ and $\mathscr{C}_0$ are independent equational classes of rings.*

Proof. $\mathscr{R}_g(P, N)$ is defined by the identities $x^*=x$ and $x \prod_{p\in P} \prod_{n\in N(p)} (x^{p^n}-x)=0$ (see [6]). In $\mathscr{R}_g(P, N)$, $(\Pi P)x=0$ for all $x \in R \in \mathscr{R}_g(P, N)$. Then consider the binary polynomial $\mathbf{p}(x, y)=x^*+y+(\Pi P-1)y^*$.

The object of this note is to prove the following result:

Theorem 2. *The following statements are equivalent:*

(1) $R \in \mathscr{R}_g(P, N) \vee \mathscr{C}_0$,

(2) $R \cong B \times C$, $B \in \mathscr{R}_g(P, N)$, $C \in \mathscr{C}_0$ *and this representation is unique,*

(3) *R satisfies the identities:*

(a) $xy = yx$, (b) $(\Pi P)(xy) = 0$, (c) $(xy)^* = xy$, (d) $(x-x^*)^2 = 0$,

(e) $x \prod_{p\in P} \prod_{n\in N(p)} (x^{p^n}-x) = 0$, (f) $2\left(\prod_{p\in P-\{2\}} q\right)^{2^{n(2)}-1} x^{2^{n(2)}} = 0$ (if $2 \in P$).

Proof. The equivalence of (1) and (2) follows immediately from Theorem 1 and the result of GRÄTZER, LAKSER and PLONKA [1] mentioned above, and also the fact that the congruence lattices of rings are modular.

(2)$\Rightarrow$(3) is a routine calculation.

(3)$\Rightarrow$(2). Let $B=\{x \in R \mid x^*=x\}$, $C=\{x \in R \mid x^2=0\}$. Claim: B and C are ideals of R.

Let $x, y \in B$, then

$$(x+y)^* = \sum_{p\in P} \left(\prod_{q\in P-\{p\}} q\right)^{p^{n(p)}-1} \left(x^{p^{n(p)}} + \sum_{i=1}^{p^{n(p)}-1} \binom{p^{n(p)}}{i} x^{p^{n(p)}-i} y^i + y^{p^{n(p)}}\right) =$$

$$= x^* + \sum_{p\in P} \sum_{i=1}^{p^{n(p)}-1} \left(\prod_{q\in P-\{p\}} q\right)^{p^{n(p)}-1} \binom{p^{n(p)}}{i} x^{p^{n(p)}-i} y^i + y^*.$$

Since ΠP divides $\left(\prod_{q\in P-\{p\}} q\right)^{p^{n(p)}-1} \binom{p^{n(p)}}{i}$, using (b) we have immediately $(x+y^*)= =x^*+y^*=x+y$ and hence $x+y \in B$. If $2 \in P$, then $(-x)^*=-x$ follows from (f). If $2 \notin P$, then $(-x)^{p^{n(p)}}=(-1)x^{p^{n(p)}}$ and so $(-x)^*=-x$. Therefore $-x \in B$ for any

$x \in B$. Now by condition (c) it is obvious that $rx \in B$ for any $x \in B$ and $r \in R$. Thus B is an ideal of R.

C is an ideal. For, if $x, y \in C$ and $r \in R$ then

$$(x+y)^2 = x^2 + 2xy + y^2 = 2(xy)^* = 2 \cdot 0 = 0,$$

$$rx = (rx)^* = \sum_{p \in P} \Big(\prod_{q \in P - \{p\}} q \Big)^{p^{n(p)-1}} r^{p^{n(p)}} x^{p^{n(p)}} = 0,$$

thus C is an ideal of R and it is also a zero ring.

Now for each $x \in R$ we have

$$\begin{aligned}(x^*)^* &= \Big(\sum_{p \in P} \Big(\sum_{q \in P - \{p\}} q \Big)^{p^{n(p)}-1} x^{p^{n(p)}} \Big)^* \\ &= \Big(x \sum_{p \in P} \Big(\sum_{q \in P - \{p\}} q \Big)^{p^{n(p)}-1} x^{p^{n(p)}-1} \Big)^* \\ &= x \sum_{p \in P} \Big(\prod_{q \in P - \{p\}} q \Big)^{p^{n(p)}-1} x^{p^{n(p)}-1} \quad \text{by (c)} \\ &= x^*.\end{aligned}$$

Therefore $x^* \in B$ and by condition (d) $x - x^* \in C$. Since $B \cap C = \{0\}$ and $x = x^* + x - x^*$ we have $R = B \oplus C$.

Remark. Let $n \geqq 2$. Let $P = \{p \in \pi \mid p^r - 1 \mid n-1$ for some $r \geqq 1\}$ and $N(p) = \{r \in \mathcal{N}^+ \mid p^r - 1 \mid n-1\}$ for each $p \in P$. The equational class of rings $\mathscr{R}_g(P, N)$ is defined by the identity $x^n = x$. (See L. LESIEUR [5] Théorème 6.)

We have shown in [4], the equational class $\mathscr{R}_g(P, N) \vee \mathscr{C}_0$ is defined by the identities $(x+y)^n = x^n + y^n$, $(xy)^n = xy = x^n y^n$.

2. Lattice of equational subclasses of $\mathscr{R}_g(P, N) \vee \mathscr{C}_0$.

It is an easy consequence of a result in [1] that if $\mathscr{K}_1$ and $\mathscr{K}_2$ are two independent equational classes of algebras of the same type, then the lattice $\mathscr{L}(\mathscr{K}_1 \vee \mathscr{K}_2)$ of equational subclasses of $\mathscr{K}_2 \vee \mathscr{K}_1$ is isomorphic to the direct product of $\mathscr{L}(\mathscr{K}_1)$ and $\mathscr{L}(\mathscr{K}_2)$.

Thus $\mathscr{L}\big(\mathscr{R}_g(P, N) \vee \mathscr{C}_0\big) \cong \mathscr{L}\big(\mathscr{R}_g(P, N)\big) \times \mathscr{L}(\mathscr{C}_0)$.

Now all rings in $\mathscr{R}_g(P, N)$ have distributive congruence lattices (see [4]). A well-known result of B. JONSSON [2], Corollary 4.2, states that if $\mathscr{K}$ is an equational class of algebras such that each algebra in it has distributive congruence lattice, then $\mathscr{L}(\mathscr{K})$ is distributive. We conclude that $\mathscr{L}\big(\mathscr{R}_g(P, N)\big)$ is distributive.

$\mathscr{L}(\mathscr{C}_0)$ is obviously distributive. The above results are summarized in

Theorem 3. *$\mathscr{L}\big(\mathscr{R}_g(P, N) \vee \mathscr{C}_0\big)$ is distributive and isomorphic to the direct product of $\mathscr{L}\big(\mathscr{R}_g(P, N)\big)$ and $\mathscr{L}(\mathscr{C}_0)$.*

Finally the author wishes to thank Professor G. Grätzer for his encouragement during the preparation of this note.

Bibliography

[1] G. Grätzer, H. Lakser and J. Plonka, Direct product and joins of algebras, *Bull. Canad. Math. Soc.*, **12** (1969), 741—744.

[2] B. Jonsson, Algebras whose congruence lattices are distributive, *Math. Scand.*, **21** (1967), 110—121.

[3] Lee Sin-Min, Equational classes of rings generated by all zero rings and finite number of Galois fields. *Notices of Amer. Math. Soc.*, **18** (1971), 71T—A63.

[4] Lee Sin-Min, Semigroups and rings satisfying $(xy)^n=xy=x^ny^n$, *Nanta Mathematica*, VI: 1 (January—June 1973), 21—28.

[5] L. Lesieur, Sur les anneaux tels que $x^n=x$, *Séminaire Dubreil-Pisot: Algèbre et Théorie des nombres, 19 années* (1965/66).

[6] H. Werner and R. Wille, Characterisierungen der primitiven Klassen arithmetischer Ringe, *Math. Z.*, **115** (1970), 197—200.

THE UNIVERSITY OF MANITOBA
WINNIPEG 19, MANITOBA, CANADA

Present address:
UNIVERSITÉ DE PARIS-SUD, BÂTIMENT 425
91405 ORSAY, FRANCE.

(Received February 7, 1972)