DĂNUŢ, MARCU — A method for finding the strongly connected components of a digraph . . . .
GH. PROCOPIUC — The equations of radiative relativistic magnetohydrodinamics Invariance groups for one-dimensional flow . . . .

NOTE

GH. GHEORGHIEV — Albert Einstein şi dezvoltarea geometriei diferenţiale . .

RECENZII . . . .

Analele ştiinţifice ale Universităţii „Al. I. Cuza" din Iaşi
Tomul XXV, s. I a, 1979, f. 2

THE NUMBER OF PRIME IDEALS OF A p-RING

BY

ALEXANDER ABIAN

Let $p > 0$ be a prime number. We recall [2, p. 144] that a p-ring R is a (necessarily commutative) ring such that.

$$x^p = x \quad \text{and} \quad px = 0 \quad \text{for every } x \in R. \tag{1}$$

Let P be a subset of a p-ring R then (it is well known) that the following statements are pairwise equivalent:

(2) *P is a prime ideal of R,*

(3) *P is a maximal ideal of R,*

(4) *$R - P$ is an ultrafilter of R (i.e., $R - P$ is closed under multiplication and is maximal w.r.t. excluding 0),*

(5) *The quotient ring R/P is isomorphic to the field $I(p)$ of integers modulo p.*

Also, it is well known that:

(6) *Every ideal of R which excludes an element r of R is a subset of a prime ideal of R which also excludes r,*

and

(7) *Every filter R (i.e., a closed under multiplication subset of R which excludes 0) which excludes an element r of R is a subset of an ultrafilter of R which also excludes r.*

Clearly, since $\{0\}$ is an ideal of R, from (6) it follows that for every nonzero element r of R there exists a prime ideal of R which excludes r. From this it follows that 0 is the only common element of all the prime ideals of R. This, in turn, implies the following well known representation theorem (which we prove since the present proof is needed for the sequel).

Theorem 1. *Let R be a p-ring and let $\{P_i\}_{i\in\alpha}$ be the set of all the prime ideals P_i of R indexed by a cardinal α. Then R is isomorphic to a ring whose elements are sequences of type α made of $0, 1, \ldots, p-1$ with addition and multiplication among sequences performed coordinatewise modulo p.*

Thus, every element of R is represented as a sequence of (finite or transfinite) type α whose terms are integers $0, 1, \ldots, p-1$.

This work is partly supported by the Iowa State University SHRI.

Proof. We construct the above mentioned representation from which the proof of the Theorem follows directly.

Let $R = \{0, a, b, c, ..., r, ...\}$ be the p-ring under consideration and let $\{P_0, P_1, P_2, ..., P_i, ...\}$ be the (not necessarily denumerable) set of all the prime ideals P_i of R with $i \in \alpha$.

On the topmost horizontal row we line up the symbols $P_0, P_1, P_2, ...$ and on the leftmost vertical column we line up all the elements $0, a, b, c, ...$ of R. Thus:

(8)

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	... P_i	...
0	0	0	0	0	0	0	0	0	... 0	...
a	m	0	0	k	q	n	n	m	... k	...
b	n	0	n	q	n	m	0	q	... m	...
c	0	q	0	0	0	0	m	0	... 0	...
.	.	.	.	.	.	.	.	.	... .	...
r	m	0	m	n	0	m	k	0	... k *iff* $r \in [k]/P_i$	
.	.	.	.	.	.	.	.	.	... .	...

Let any of the letters $k, m, n, q, ...$ stand for any of the integers $1, 2, ..., p-1$.

In view of (5), we fill in table (8) as follows:

(9) *At the intersection of the r-th row and the i-th column we put k if and only if r is an element of the coset $[k]$ of the quotient ring R/P_i.*

Thus, if $p = 5$ then R/P_i has five cosets $[0] = P_i, [1], [2], [3], [4]$. Now, if $r \in [3]$ in the quotient ring R/P_2 then at the intersection of the r-th row and the 2-nd column we put 3.

From (9) we have:

(10) *At the intersection of the r-th row and the i-th column we put 0 if and only if $r \in P_i$.*

Again, from (9) it follows (as claimed) that every element of R is represented by a sequence of type α whose terms are integers $0, 1, 2, ..., p-1$. For instance, as (8) shows:

$$0 \text{ is represented by } 0, 0, 0, 0, 0, 0, 0, 0, ..., 0, ...$$

$$a \text{ is represented by } m, 0, 0, k, q, n, n, m, ..., k, ...$$

(11) $$b \text{ is represented by } n, 0, n, q, n, m, 0, q, ..., m, ...$$

.....

$$r \text{ is represented by } m, 0, m, n, 0, m, k, 0, ..., k, ...$$

.....

From (5) it follows that the set of all the sequences thus obtained, form a ring under coordinatewise addition and multiplication modulo p,

which is homomorphic to R. However, this homomorphism is an isomorphism because from (10) and an earlier remark it follows that the zero element of R is the only element of R which is represented by the zero sequence (of type α).

Thus, the Theorem is proved.

In view of our construction, the elements of any prime ideal or any ultrafilter of R can be determined readily from inspecting the columns of table (8). Indeed, the elements of prime ideal P_i are all those elements of R whose representing sequences have 0 in the i-th column. Analogously, the elements of ultrafilter $R - P_i$ are those elements of R whose representing sequences have a nonzero entry the in i-th column. Accordingly, we have:

(12)
$$P_0 = \{0, c, ...\}, \quad P_1 = \{0, a, b, ..., r\},$$
$$P_i = \{0, c, ...\},$$
$$R - P_3 = \{a, b, ..., r, ...\}, \quad R - P_i = \{a, b, ..., r, ...\}.$$

Lemma 1. If the sequence

(13) $$r = (m, 0, m, n, 0, m, k, 0, ..., k, ...)$$

is a row in table (8) then so are the finitely many sequences:

(14) $$r_m = (m, 0, m, 0, 0, m, 0, 0, ..., 0, ...),$$

(15) $$r_n = (0, 0, 0, n, 0, 0, 0, 0, ..., 0, ...),$$

(16) $$r_k = (0, 0, 0, 0, 0, 0, k, 0, ..., k, ...),$$

where the only nonzero term of sequence r_i is the integer i which appears at all those coordinates of r_i where i appears in sequence r.

Proof. Since sequences appearing in table (8) are closed under coordinatewise addition and multiplication modulo p and since sequence r given by (13) appears in table (8), we see by (5) that each of the following sequences also must appear in table (8):

$$\begin{aligned}
r^{p-1} &= (1, \quad 0, \quad 1, \quad 1, 0, \quad 1, \quad 1, 0, ..., 1, ...)\\
kr^{p-1} &= (k, \quad 0, \quad k, \quad k, 0, \quad k, \quad k, 0, ..., k, ...)\\
s = r - kr^{p-1} &= (m-k, \quad 0, m-k, n-k, 0, m-k, \quad 0, 0, ..., 0, ...)\\
s^{p-1} &= (1, \quad 0, \quad 1, \quad 1, 0, \quad 1, \quad 0, 0, ..., 0, ...)\\
(n-k)s^{p-1} &= (n-k, \quad 0, n-k, n-k, 0, n-k, \quad 0, 0, ..., 0, ...)\\
t = s-(n-k)s^{p-1} &= (m-n-2k, 0, m-n-2k, 0, 0, m-n-2k, 0, 0, ..., 0, ...)\\
t^{p-1} &= (1, \quad 0, \quad 1, \quad 0, 0, \quad 1, \quad 0, 0, ..., 0, ...)\\
r_m = mt &= (m, \quad 0, \quad m, \quad 0, 0, \quad m, \quad 0, 0, ..., 0, ...)
\end{aligned}$$

which shows that sequence r_m given by (14) also appears in table (8).

In a similar manner we show that sequences r_n and r_k given respectively by (15) and (16) appear in table (8).

Next, we introduce two distinct notions of covering.

Definition. *We say that a set S of rows (i.e., sequences) of table* (8) *covers the nonzero entries of a row (i.e., sequence) r of table* (8) *if and only if whenever r has a nonzero entry at the i-th coordinate, there exists a row (i.e., sequence) of S which has a nonzero entry at the i-th coordinate. Also we say that a set Q of rows (i.e., sequences) of table* (8) *covers the zero entries of a row (i.e., sequence) r of table* (8) *if and only if whenever r has a zero entry at the i-th coordinate, there exists a row (i.e., sequence) of Q which has a zero entry at the i-th coordinate.*

For instance, as table (8) shows :

The set $\{a, b\}$ of rows covers the nonzero entries of row r,
The set $\{a, b\}$ of rows does not cover the zero entries of row r,
The set $\{a, c\}$ of rows covers the zero entries of row r,
The set $\{a, c\}$ of rows does not cover the nonzero entries of row r,
The set $\{a, b, c\}$ of rows covers the nonzero entries of row r,
The set $\{a, b, c\}$ of rows covers the zero entries of row r.

Lemma 2. *Let S be a set of rows and r a row of table* (8). *In the ring (coordinatewise addition and multiplication modulo p) R of all the rows of table* (8) *if r is an element of the ideal generated by S then a finite subset of S covers the nonzero entries of r.*

Proof. Let row r be an element of the ideal (of the ring R) generated by the set $S = \{u, v, w \ldots\}$ of rows of table (8). Thus, r is equal to a finite sum (coordinatewise modulo p) of finite products (performed coordinatewise) of $u, v, w, \ldots$ and rows of R. Let in this finite sum of finite products, the finitely many elements $u, v, \ldots, t$ of S be involved. But then if r has a nonzero entry at the i-th coordinate, clearly, at least one of $u, v, \ldots, t$ must have a nonzero entry at the i-th coordinate. Hence, indeed, the finite subset $\{u, v, \ldots, t\}$ of S covers the nonzero entries of r.

Remark. Based on Lemma 1 one can prove the converse of Lemma 2, however, this is not needed for our purpose.

Lemma 3. *Let Q be a set of rows and r a row of table* (8). *In the ring (coordinatewise addition and multiplication modulo p) R of all the rows of table* (8) *if r is an element of the filter generated by Q then a finite subset of Q covers the zero entries of r.*

Proof. Let row r be an element of the filter (of the ring R) generated by the set $Q = \{s, t, v \ldots\}$ of rows of table (8). Thus, r is equal to a product (coordinatewise modulo p) of finitely many elements $s, t, \ldots, w$ of Q. But then if r has a zero entry at the i-th coordinate, clearly, at least one of $s, t, \ldots, w$ must have a zero entry at the i-th coordinate (because integers modulo p form a field). Hence, indeed, the finite subset $\{s, t, \ldots, w\}$ of Q covers the zero entries of r.

Next, we prove that table (8) is compact in two distinct ways.

Theorem 2. *Let a set S of rows of table* (8) *cover the nonzero entries of a row r of table* (8). *Then a finite subset of S already covers the nonzero entries of r.*

Proof. As always, we use the same letters $0, a, b, \ldots, r, u, v, w, \ldots$ for the elements of the p-ring R and their respective representing sequences (of type α whose terms are integers $0, 1, 2, \ldots, p-1$) as constructed in table (8).

Now, let a set $S = \{a, b, \ldots, u, v, w, \ldots\}$ of rows of table (8) cover the nonzero entries of a row r of table (8). We show that a finite subset of S already covers the nonzero entries of r. Let us assume to the contrary that no finite subset of S covers the nonzero entries of r. But then by Lemma 2 we see that r is not an element of the ideal $[S]$ generated by S (in the p-ring R). Hence, by (6) the ideal $[S]$ is a subset of a prime ideal, say, P_i of R which also excludes r. Consequently,

$$S = \{a, b, \ldots, u, v, w, \ldots\} \subseteq P_i \quad \textit{and} \quad r \notin P_i. \tag{17}$$

From (17) and (10) it follows that the i-th coordinate of every one of the sequences $a, b, \ldots, u, v, w, \ldots$ is 0. On the other hand, from (17) and (9) it follows that the i-th coordinate of sequence r is a nonzero integer. But this contradicts the fact that the set $S = \{a, b, \ldots, u, v, w, \ldots\}$ covers the nonzero entries of r. Thus, our assumption is false and the Theorem is proved.

Theorem 3. *Let a set S of rows of table* (8) *cover the zero entries of a row r of table* (8). *Then a finite subset of S already covers the zero entries of r.*

Proof. Let a set $S = \{a, b, \ldots, s, t, v, \ldots\}$ of rows of table (8) cover the zero entries of a row r of table (8). Let us assume to the contrary that no finite subset of S covers the zero entries of r. But then by Lemma 3 we see that r is not an element of the filter F generated by S (in the p-ring R). Hence, by (7) the filter F is a subset of an ultrafilter, say, $R - P_i$ of R which also excludes r. Consequently,

$$S = \{a, b, \ldots, s, t, v, \ldots\} \subseteq (R - P_i) \quad \textit{and} \quad r \in P_i. \tag{18}$$

From (18) and (9) it follows that the i-th coordinate of every one of the sequences $a, b, \ldots, s, t, v, \ldots$ is a nonzero integer. On the other hand, from (18) and (10) it follows that the i-th coordinate of r is 0. But this contradicts the fact that $S = \{a, b, \ldots, s, t, v, \ldots\}$ covers the zero entries of r. Thus, our assumption is false and the Theorem is proved.

Remark. Let us recall that a finite p-ring has p^n elements and n prime ideals (where n is a positive integer). In fact, a finite p-ring with p^n elements is isomorphic to the direct product of n fields $I(p)$. On the other hand, if R is an infinite p-ring then, as shown below, R has at least as many prime ideals as it has elements (for the special case $p = 2$ (i.e., for the case of Boolean rings) this is shown in [1]). Denoting by α the cardinal number of the set of all prime ideals of an infinite p-ring R, we observe that there are p-rings R with $\alpha = \bar{\bar{R}}$ and there are p-rings R with $\alpha > \bar{\bar{R}}$. In accordance with Theorem 1, we also observe that in general, R is isomorphic only to a subring of the direct product of α fields $I(p)$.

We next prove our main Theorem.

Theorem 4. *Let R be a infinite p-ring. Then R has as many prime ideals as it has elements.*

Proof. Denoting by α the cardinal number of the set of all prime ideals of R, let us assume to the contrary that

$$\alpha < \bar{\bar{R}}. \tag{19}$$

From (19) it follows that in table (8) there are α columns and more than α (i.e., $\overline{\overline{R}}$) rows. By (3) every prime ideal P_i of R is also a maximal ideal of R. Thus,

$$(20) \qquad (P_i - P_j) \neq \varnothing \neq (P_j - P_i) \quad \textit{for every} \quad i \neq j \in \alpha.$$

From (20) and (9) it follows that for every $i \in \alpha$ and every $j \in \alpha$ with $i \neq j$ there is a row g_{ij} in table (8) such that the i-th coordinate of g_{ij} is 0 and the j-th coordinate of g_{ij} is a nonzero integer, in fact, is 1 (since in the field $I(p)$, the $(p-1)$-th power of every nonzero element is 1). Let the set G given by :

$$(21) \qquad G = \{g_{ij} \mid i \in \alpha \textit{ and } j \in \alpha \textit{ with } i \neq j\}$$

be the set of all such rows g_{ij} of table (8). Clearly (since α is infinite),

$$(22) \qquad \alpha = \overline{\overline{G}}.$$

As always, identifying the set of all the rows of table (8) (under coordinatewise addition and multiplication modulo p) with the p-ring R, we claim that the subring R_0 generated by the rows g_{ij} of table (8) is equal to R.

Since R_0 consists of the finite sums (coordinatewise modulo p) of the finite products (coordinatewise modulo p) of the elements g_{ij} of G, from (22) it follows that

$$(23) \qquad \alpha = \overline{\overline{R}}_0.$$

In order to prove that $R_0 = R$, it is sufficient to show that an arbitrary row, say, r of table (8) is an element of R_0. Let, as in (13),

$$r = (m, 0, m, n, 0, m, k, 0, ..., k, ...).$$

We have shown that r is a sum of finitely many sequences of the form (14), (15), (16), ... Thus, in order to prove that $r \in R_0$, it is enough to prove (since R_0 is a subring of a p-ring) that, say,

$$r_m = (m, 0, m, 0, 0, m, 0, 0, ..., 0, ...) \in R_0$$

or equivalently,

$$(24) \qquad e_m = (1, 0, 1, 0, 0, 1, 0, 0, ..., 0, ...) \in R$$

where e_m is obtained from r_m above, by replacing everywhere 1 for m.

Motivated by (24), for every coordinate h of e_m where e_m has 1, let us consider the following (in general, infinitely many) subsets S_h of G :

$$(24) \qquad \begin{aligned} S_1 &= \{g_{2,1}, g_{4,1}, g_{5,1}, g_{6,1}, g_{7,1}, ...\}, \\ S_3 &= \{g_{2,3}, g_{4,3}, g_{5,3}, g_{6,3}, g_{7,3}, ...\}, \\ S_6 &= \{g_{2,6}, g_{4,6}, g_{5,6}, g_{6,6}, g_{7,6}, ...\}, \\ &\cdots\cdots \\ S_h &= \{g_{2,h}, g_{4,h}, g_{5,h}, g_{6,h}, g_{7,h}, ...\}. \\ &\cdots\cdots \end{aligned}$$

In view of our definition of g_{ij} we see that S_1 covers the zero entries of e_m whereas the 1-st coordinate of e_m and that of every element of S_1 is 1. Moreover, S_3 covers the zero entries of e_m whereas the 3-rd coordinate of e_m and that of every element of S_3 is 1. In general, in (24) we have :

(25) *S_h covers the zero entries of e_m whereas the h-th coordinate of e_m and that of every element of S_h is* 1.

By Theorem 3, there exists a finite subset F_h of S_h, say,

$$(26) \qquad F_h = \{g_{2,h}, g_{7,h}, ..., g_{rh}\},$$

such that (in view of (25)) we have :

(27) *F_h covers the zero entries of e_m whereas the h-th coordinate of e_m and that of every element of F_h is* 1.

Let f_{0h} denote the product of the (finitely many) elements of F_h given in (26). Clearly, in view of (21), we see that $f_{0h} \in R_0$.

From (27) it follows that for every coordinate h of e_m where e_m has 1, the singleton $\{f_{0h}\}$ covers the zero entries of e_m whereas the h-th coordinate of e_m and that of f_{0h} is 1. Accordingly, let us consider the subset S of the subring R_0 consisting of all such f_{0h}'s. Thus,

(28) $S = \{f_{0h} \mid h \in \alpha$ *and* $\{f_{0h}\}$ *covers the zero entries of e_m and the h-th coordinate of e_m and that of f_{0h} is* $1\}$.

Obviously, S covers the nonzero entries of e_m and therefore by Theorem 2, there exists a finite subset F of S, say,

$$(29) \qquad F = \{f_{0h}, f_{0t}, ..., f_{0z}\}.$$

such that F covers the nonzero entries of e_m and (28) holds. As a result, we have the following situation (where for the sake of simplicity, we assume that F has just three elements) :

$$(30) \qquad \begin{aligned} f_{0h} &= (y, 0, y, 0, 0, y, 0, 0, 0, y, 0, y, ...) \\ f_{0t} &= (y, 0, y, 0, 0, y, 0, 0, 0, y, 0, y, ...) \\ f_{0z} &= (y, 0, y, 0, 0, y, 0, 0, 0, \ \ , 0, y, ...) \\ e_m &= (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, ...). \end{aligned}$$

From (28) it follows that in (30), above every 0 in e_m the entire column consists of 0's. Also, from (29) it follows that in (30), above every 1 in e_m at least one of the y's is 1, otherwise, y is 0 or 1.

For every element u and v of the ring R, let us denote by $L(u, v)$ the element of R defined by :

$$(31) \qquad L(u, v) = u^{p-1} + v^{p-1} + (p-1)\, u^{p-1} v^{p-1}.$$

But then, it can be easily verified, that in view of (30) we have :

$$(32) \qquad L(f_{0z}, L(f_{0t}, f_{0h})) = e_m$$

(which is valid not only for three sequences f_{0h}, f_{0t}, f_{0z} but for any finite number of sequences $f_{0h}, f_{0t}, \ldots, f_{0z}$).

From (28) it follows that the finitely many sequences $f_{0h}, f_{0t}, \ldots, f_{0z}$, given in (29), are elements of the subring R_0. Consequently, from (31) and (32) it follows that $c_m \in R_0$ and therefore $R_0 = R$, as claimed. But this, in view of (19) and (23) leads to a contradiction. Thus, our assumption in false and $\alpha \geq \bar{\bar{R}}$. Hence, the Theorem is proved.

REFERENCES

1. Makinson, D. C. — *On the number of ultrafilters of an infinite Boolean Algebra.* Zeitschr. f. math. Logik und Grundlagen d. Math. 15 (1969), 121—122.
2. Mc Coy, N. H. — *Rings and ideals,* Carus Math. Monograph No. 8. Math. Assoc. of Amer., 1948.

Received 1.III. 1979

Department of Mathematics
Iowa State University
Ames, Iowa 50011

Analele ştiinţifice ale Universităţii „Al. I. Cuza" din Iaşi
Tomul XXV, s. I a, 1979, f. 2

ON PSEUDO-IDEALS OF GROUPS

BY

M. K. SEN and T. K. DUTTA

A nonempty subset A of a semigroup S is called a left pseudo-ideal if and only if

i) $ab \in A$ whenever $a, b \in A$,

ii) $x^2A \subseteq A$, for every element $x \in S$.

The right pseudo-ideal is defined analogously. In [3], the first author has shown that: i) a left ideal of a semigroup is always a left pseudo-ideal but the converse is not true; ii) a bi-ideal [1] may not be a pseudo-ideal and a pseudo-ideal may not be a bi-ideal. Also by means of the pseudo-ideal and bi-ideal, the first author has obtained a criterion for determining the regularity of a semigroup.

Now the object of this paper is to study some more properties of pseudo-ideals, especially, in groups. The example given below shows that a group may contain pseudo-ideals. Pseudo-ideals in a group have some properties which do not hold in a semigroup. With the help of these properties of pseudo-ideals, we have obtained the criteria for determining when a semi-group will be a group. Also by using the same properties of the pseudo-ideals, we have proved the following known result:

In a finite field, every element can be expressed as a sum of two squares.

Example: R denotes the set of all non zero rational numbers. It is known that R is a multiplicative group. Suppose $A = \{r^2 \mid r \in R\}$. Then it can be shown that A is a proper pseudo-ideal of R. Again let B be a subset consisting of all the rational numbers r^2, $1/3\, r^2$, $3r^2$ where $r \in R$. Now B is also a proper pseudo-ideal of R.

The above example shows that a group may contain more than one pseudo-ideal.

We recall the following properties of pseudo-ideals. In a group a left pseudo-ideal is a right pseudo-ideal and vice-versa ([3], p. 111).

Every pseudo-ideal of a group is also a normal subgroup but the converse is not true. Hence in a group every pseudo-ideal contains 1—the identity element of the group ([3], p. 111).

Now we have the following propositions.