universidad nacional de cuyo
departamento de investigaciones científicas

Completo a encuadernar

revista matemática cuyana

volumen 1
1955
fasciculo 1
páginas 1-40

instituto de matemática
mendoza
argentina

REVISTA MATEMATICA CUYANA

La Revista Matemática Cuyana está destinada a la publicación de trabajos originales en los campos de la matemática pura y aplicada, y aparece en forma de fascículos sueltos sin periodicidad fija, anualmente reunidos en un volumen de 250 páginas, aproximadamente.

Castellano, inglés, alemán, francés e italiano, son los idiomas de la Revista.

Los artículos para la Revista deben ser escritos a máquina con doble espacio y enviados a nombre de uno de los miembros del Comité de Redacción, al Instituto de Matemática, Departamento de Investigaciones Científicas, Universidad Nacional de Cuyo, Mendoza, Argentina.

Los colaboradores tienen derecho a 50 tiradas aparte gratis, de sus artículos, y podrán, si lo desean, recibir hasta 150 tiradas aparte a precio de costo.

En todo lo referente a suscripciones, adquisición de números atrasados, etc., dirigirse al Director del Instituto de Matemáticas, Profesor Mischa Cotlar.

revista matemática cuyana

Imprenta y Casa Editora CONI, Perú 684, Buenos Aires

universidad nacional de cuyo
departamento de investigaciones científicas

revista matemática cuyana

volumen 1
1955
fascículo 1
páginas 1-40

instituto de matemática
mendoza
argentina

On the Theory of Unilateral equations in Associative Rings *

By ORLANDO E. VILLAMAYOR

INTRODUCTION

The first steps in the theory on unilateral equations in rings, specially those of linear systems, have been oriented towards the consideration of homogeneous systems. N. H. McCoy [12] has given, by means of determinants defined after the classical model, necessary and sufficient conditions for an homogeneous linear system (with coefficients in a commutative ring) to have a non-trivial solution in the ring. In the present article use is made of these results, after reducing the theory to the commutative case. O. Ore [21] studies the conditions under which an integral domain (non-commutative) can be embedded into a division ring by the adjunction of all formal inverses, as it is done in the commutative case, and finds that the existence of non-trivial solutions (within the ring) for all equations of the form $ax-by=O$ is a necessary and sufficient condition. He also states the problem of inquiring if any ring without zero-divisors can be embedded into a division ring. It has been proved by A. Malcev [17] that there exist non-commutative integral domains that cannot be embedded in division rings. M. Hall [10, 11] succeds in determining all linear homogeneous systems having as solutions all those of a given linear system. From this and with help of the notion of algebraic closure of ideals, as defined in section 3.*a*, he derives a group of interesting results on rings.

Other related papers, such as that of Ellis and Gaddum [6] on Boolean rings could still be mentioned, but we prefer to omit them since they are no relevant to the questions dealt with in this article.

* Received December 12, 1954.

This paper was motivated by the desire of developping a general theory of equations for associative rings. The first step, naturally, was the determination of solvability conditions, thas is, conditions for the existence of a ring extension having a solution of a given equation (or equations). The first section is devoted to this question where, in addition, it is proved that it is always possible to embed any ring into another ring having a solution for any solvable equation. The theorem on solvability of linear systems generalizes a known result on fields due to G. Birkhoff [3].

These solvability conditions require, however, the knowledge of a special extension of the ring and are of little practical value for the caracterization of solvable equations. This situation is partially remedied in the second section, where necessary and sufficient conditions for the solvability of unilateral linear equations are given in terms of the original ring only. The third section further generalizes this to linear systems.

Generalizing the notion of field, where all linear equation have solution, we introduce the notion of semi-field and complete semi-field by requiring that all solvable linear equations, or linear systems, respectively, have solutions.

These concepts are very useful for the further developement of the general theory of equations, and are not to be mistaken with the notion of semi-field introduced by A. A. Albert [2], which is a particular case of the notion given here.

Besides fields and division rings, there are still some other known examples of complete semi-fields. Such are: Boolean rings, the p-rings of McCoy and Montgomery [16], the p^k-rings of Foster [9], the Frobeniusean and quasi-Frobeniusean algebras and rings [18, 19], and the normal rings of Teichmüller [23].

In section 3, the semi-fields and complete semi-fields are also characterized by properties of ideals with regard to the closure operation defined by Hall.

Finally, in the last section, equations of higher degree are considered and some general properties of algebraic extensions are studied in the commutative case, leaving for another article the complete treatement of general equations in associative rings.

The results of this paper were presented to the Unión Matemática Argentina in the sessions of Sept. 1951 and Sept. 1952.

I. RING EXTENSIONS

1.a. General considerations. Let A be an associative ring and $W=\{X_j\}$, $(j\in J)$ a non-void set, the elements of which will be called *indeterminates*. We suppose that A and W are disjoint and β is the cardinal number of W.

If E is the ring of integers, A may be considered as an E-module. Now for every $X_j\in W$ we shall consider the one-dimensional E-module $EX_j=\{mX_j\}$. With these E-modules we form all tensorial products (1)

$$M_1 \bigcirc M_2 \bigcirc \ldots \bigcirc M_n,$$

where n is any positive integer, and the M_i are either coincident with A or with one of the $E\,X_j$, and such that not two consecutive M_i are equal to A. The (formal) terms of the elements of any of these tensorial products are called *monomials*.

We define *polinomials* as the elements of the restricted direct sum $\Gamma_\beta(A)$ of all the E-modules thus obtained (1).

To define the product of two monomials $m=(\alpha_1, \ldots, \alpha_h)$ and $m'=(\alpha'_1, \ldots, \alpha'_k)$ we must consider two cases:

1) If $\alpha_h\in A$ and $\alpha'_1\in A$, then

$$mm'=(\alpha_1, \ldots, \alpha_{h-1}, \alpha, \alpha'_2, \ldots, \alpha'_k)$$

where $\alpha=\alpha_h\alpha'_1$ (the product being defined in A)

2) Otherwise,

$$mm'=(\alpha_1, \ldots, \alpha_h, \alpha'_1, \ldots, \alpha'_k)$$

The product of two polynomials $p_1=\sum_1^h m_i$ and $p_2=\sum_1^k m'_j$ is defined by the formula

$$p_1 p_2=\left(\sum_{i=1}^{h} m_i\right)\left(\sum_{j=1}^{k} m'_j\right)=\sum_{j=1}^{h}\sum_{j=1}^{k} m_i m'_j$$

(1) This way of definition of the free extension, replacing the method originally used in [24], has kindly been suggested to the author by J. Dieudonné. The definition of tensorial product can be found, for instance in N. Jacobson, Lectures on abstract Algebra, vol 2, or in N. Bourbaki, Éléments de Mathématique, Livre 3 (Algèbre), chap. III. The restricted direct sum is the subring consisting of all formal sums with all terms but a finite number equal to zero.

The product of n polynomials is defined by induction as follows:

$$p_1 p_2 \dots p_{n-1} p_n = (p_1 p_2 \dots p_{n-1}) p_n$$

It is easily seen that the set $\Gamma_\beta(A)$ of all polynomials with the operations just defined is an associative ring, and the subset of all polynomials of the form $p_i = (a)$, $a \in A$, is a subring A' isomorphic to A, which will be called the *subring of constants*, and will be identified with A, so that, we can speak about the elements of A in $\Gamma_\beta(A)$.

$\Gamma_\beta(A)$ will be called the *free extension of A with β indeterminates*, no confusion being possible with the classical polynomial ring.

To avoid any other confusion, in the sequel, the term *polynomial* will be used only to speak about the classical polynomials; for those just defined we shall use the expression « *elements of* $\Gamma_\beta(A)$ ».

LEMMA 1.1. — *For every ring B such that $B \supseteq A$, B is a homomorphic image of $\Gamma_\beta(A)$ for a conveniently chosen cardinal number β, that is, $B = \Gamma_\beta(A)/I$, with $I \cap A = (0)$; conversely, if I is an ideal in $\Gamma_\beta(A)$ such that $I \cap A = (0)$, then $\Gamma_\beta(A)/I = B$ contains a subring isomorphic to A.*

PROOF. — Let B be an associative ring such that $B \supseteq A$. We can take W as a set with the cardinal number β of the set $B - A$, and set a one-to-one correspondence between its elements and those of $B - A$. The set of relations satisfied by the elements of $B - A$ written by means of sums and products (in these relations may appear, naturally, elements of A), has by the one-to-one elementwise correspondence just quoted a corresponding set, in $\Gamma_\beta(A)$. This set is evidently a two-sided ideal I in $\Gamma_\beta(A)$, and $B \cong \Gamma_\beta(A)/I$. Furthermore, $I \cup A = (0)$, otherwise if $a \neq 0$, $a \in A$, is in I, then $a = 0$ in B, contradicting our hypotesis $B \supseteq A$.

Conversely, given and ideal $I \subseteq \Gamma_\beta(A)$ such that $I \cap A = (0)$ since the elements of $B = \Gamma_\beta(A)/I$ are the cosets in $\Gamma_\beta(A)$ defined by I, we can put the elements of A in a one-to-one correspondence with those cosets which have (at least) one element of A, the correspondence being one-to-one since the condition $I \cap A = (0)$ implies that no more than one element of A can appear in each coset.

A ring B will be said an *extension of A* if $B \supseteq A' \cong A$

It is easily seen that the zero-element of A is also the zero-element of every free extension, hence, by the lemma just proved, it is also the zero-element of every extension. On the contrary, the

identity-element of A may be different from the identity-element of an extension (if one of them does not exist the assertion is trivial). As an example we have the ring E_6 (the residue class ring of integers reduced modulo *6*), which is an extension of E_3 (integers reduced modulo *3*), since the set $\{0_6, 2_6, 4_6\} \subseteq E_6$ form a field isomorphic to E_3, whose identity is 4_6, different from the identity element of E_6, which is 1_6.

We shall study extensions of the following types:

a) arbitrary extensions, that is, extensions over which we make no restrictions;

b) identity-preserving extensions, that is, those extensions B of A for which the identity-element *1* of A is also identity-element in B. Since $B = \Gamma_3(A)/I$, we can easily see that I must contain $1 . X_j - X_j$ and $X_j . 1 - X_j$ for every $X_j \in W$;

c) center-preserving extensions, that is, those for which the center C of A is contained into the center of B. In this case, the (two sided) above ideal I must contain $cX_j - X_j c$ for every $X_j \in W$ and every $c \in C$;

d) commutative extensions of (commutative) rings A; in this case, B must be center-preserving, furthermore, $X_i X_j - X_j X_i \in I$ for every $X_i X_j \in W$.

In section *2* and *3* we shall study only identity-preserving extensions, and in section *4*, extensions which are simultaneously commutative and identity-preserving.

To build these extensions, we can start from the (classical) polynomial ring $A[X_1, X_2 \ldots]$, which is the homomorphic image of the free extension modulo the ideal generated by all $1 . X_j - X_j$, $X_j . 1 - X_j$, $X_i X_j - X_i X_j$ and $X_j a - a X_j$ for every X_i, $X_j \in W$ and every $a \in A$.

Given an extension $B \supseteq A$, since $B = \Gamma_3(A)/I$, the image of the indeterminates in this homomorphism will be called generators of B.

DEFINITION 1.1. — *A ring B containing A, will be called a simple extension of A if there exists a single element $\theta \in B$ such that the subring generated by A and θ is the whole B.*

This is the case when B is an extension of A with a single generator θ, and it will be denoted by $B = A(\theta)$.

1. b. — Algebraic and transcendental extensions. We shall study only equations of the form $f(x, \ldots, x_n) = 0$, where $f(X_1, \ldots, X_n)$ is any element of $\Gamma_3(A)$. These will be called *equations with coefficients in A* or *A-equations*.

Speaking about extensions of type a (resp b, c, d) we shall say that $f(x_1, \ldots, x_n) = 0$ is a *trivial equation*, if $f(X_1, \ldots, X_n) \in I$ for every such an extension $B \supseteq A$, I being, as just defined, the (two-sided) ideal defined by the homomorphism $\Gamma_s(A) \to B$.

The following definitions are conditioned to the type of extensions we are studying.

DEFINITION 1.2. — *An element* x *of an extension* B *of a ring* A *is called algebraic over* A *if it satisfies at least one non-trivial equation with coefficients in* A *; otherwise, it will be called transcendental.*

DEFINITION 1.3. — *An extension* B *of a ring* A *will called algebraic if there exists a set of algebraic generators over* A.

A non algebraic extension B *of* A *will be called transcendental.*

DEFINITION 1.4. — *A transcendental extension* B *of a ring* A *is called purely transcendental if there is a set of transcendental generators over* A.

It is known that every element of an algebraic extension of a field is algebraic, but it is not true for rings in general. The following example shows it :

EXAMPLE. — Let A be the commutative ring whose elements are: a, b, $a + b$, 0, 1, $a + 1$, $b + 1$, $a + b + 1$, with $a^2 = ab = ba = b^2 = 0$ and characteristic 2. The homomorphic image of its polynomial ring $A[X]/(aX - b)$ is a proper extension of A. This is true by a theorem of solvability of first degree equations which will be proved later (Th. 2.1). The extension thus built is algebraic, because its generator X is algebraic over A (it satisfies the equation $ax = b$). If c is any element of this extension, it will be algebraic if it satisfies some non-trivial equatiou with coefficients in A, that is, if some element of the subring generated by A and c is also contained in the ideal $(aX - b)$ in $A[X]$. Since $(aX - b)$ is a principal ideal this amounts to say that some polynomial in c is divisible by $aX - b$. It may be easily proved that X^2 does not satisfy this condition, hence it is transcendental in the extension thus built.

In the commutative case we shall only deal with commutative extensions. Consequently, in such cases, we shall always start from the polynomial ring, so that a transcendental simple extension is isomorphic to the polynomial ring, and an algebraic simple extension is a proper homomorphic image.

We shall also investigate, for special types of rings, when the property (valid for fields) that every element of an algebraic extension is algebraic, holds.

For transcendental extensions the corresponding statement is false; it is very easy to find an example. Let A be a ring in which $a \neq 0$, $b \neq 0$ and $ab = 0$, and consider the element $y = bX + 1$ (1 is the identity element of A) in an identity-preserving transcendental extension of A (say $A(X)$ with X transcendental). Such an element satisfies the equation $ay = a$, hence it is algebraic over A.

Only for integral domains it is true that every element of a purely transcendental extension is transcendental.

1.c. — Solvability of equations. DEFINITION 1.5. — *An equation* $f(x) = 0$, *with coefficients in a ring* A *will be called solvable if there exists at least one extension* $B \supseteq A$ *in which the equation has a solutian. Otherwise, it will be called unsolvable.*

Let us explain brlefly this definition. Let $f(x) = 0$ be an equation with coefficients in a ring A; if there exists an element c in A such that $f(c) = 0$, we shall say that the equation *has a solution in* A. If there is one extension B of A in which $f(x) = 0$ has a solution, we shall say that the equation *admits a solution*, and in both cases it will be called *solvable*. An equation is *unsolvable* if no extension of A exists in whicb is has a solution.

Let A be a ring and B an extension of A where the equation $p(x) = 0$ has a solution. The subring generated by the elements of A and one root of the equation is also an extension of A, hence, it is a homomorphic image of the free extension of A with one generator, X; the image of the generator being the root of the equation. This homomorphism is proper, since $p(X)$, an element of the free extension, is mapped onto zero. Since the free extension is a ring, the kernel of the homomorphism is a two-sided ideal which contains $p(X)$, hence, it contains the principal two-sided ideal generated by $p(X)$.

Conversely, if we build the free extension of a ring A with one generator and consider the homomorphic image modulo an arbitrary two-sided ideal I, the ring so formed has an element (the image of X) which satisfies the equations obtained replacing in each element of I, the coefficients (elements of A) by the images of the classes containing the corresponding element of A. But, in general, this is

not an extension of A, and the equations so obtained cannot be considered as equations with coefficients in A. To exclude this difficulty, as we have seen in lemma 1.1, it is necessary and sufficient that I be disjoint with A in the free extension. We say that I and A are disjoint if they have no element in common different from zero, that is, if $A \cap I = (0)$.

Let $f(x)=0$ be an equation with coefficients in A. If the principal two-sided ideal generated by $f(x)$ (called briefly in the following $(f(x))$ in the free extension with one generator $\Gamma_1(A)$ is disjoint with A, then $\Gamma_1(A)/(f(x))$ is an extension of A in which the equation has a solution, and $f(x)=0$ is solvable.

Otherwise, no extension of A has a solution for $f(x) = 0$, and the equation is unsolvable. This proves the theorem:

THEOREM 1.1. — *The necessary and sufficient condition for an equation* $f(x) = 0$ *with coefficients in a ring* A *to be solvable, is that the ideal* $(f(X))$ *be disjoint with* A *in* $\Gamma_1(A)$.

For the special case of linear unilateral equations, we shall later give necessary and sufficient conditions which can be studied inside of A.

1.d. — Maximal and minimal extensions. For a given solvable equation $f(x) = 0$ with coefficients in a ring A (briefly, an *A-equation*), we can consider all simple extensions of A having solutions of the equation. In general, if we consider all extensions, we can study in them the subring generated by A and one root of $f(x) = 0$, which is a simple extension. By the preceding considerations, every extension is a homomorphic image of $\Gamma_1(A)$ modulo an ideal containing $(f(X))$, hence they are homomorphic images of the ring $\Gamma_1(A)/(f(X))$.

The ring $\Gamma_1(A)/(f(X))$ is, in this sense, the maximal simple extension of A in which $f(X)=0$ has a solution.

Let us consider, now, the set of all ideals of a free extension disjoint with A. These ideals can be ordered by inclusion, and the set is inductive. Then, by Zorn's lemma, every ideal is contained in a maximal disjoint ideal. Let us call M one of these maximal ideals. $\Gamma_2(A)/M$ in an extension of A and every homomorphic image of $\Gamma_2(A)/M$ is isomorphic to the homomorphic image $\Gamma_2(A)/I$, of the free extension, modulo an ideal I containing M. Since M is maximal, no proper homomorphic image of $\Gamma_2(A)/M$ is an extension of A.

In this sense, $\Gamma_\beta(A)/M$ are minimal extensions of A.

We can now prove the following additional lemma :

LEMMA 1.2. — *If* A *is a subdirectly irreducible ring, then every minimal extension of* A *is also subdirectly irreducible.*

A ring is said to be subdirectly irreducible if it cannot be considered as a subdirect sum of its proper homomorphic images. It is known that a ring is subdirectly irreducible [14] if it has a minimum ideal, that is, if it has a two-sided ideal $J \neq (0)$ such that, for every two-sided ideal I in the ring A, is $J \subseteq I$.

If B is a minimal extension of the ring A, we have $B=\Gamma_\beta(A)/M$, for suitably chosen β and M. If I is a proper two-sided in B, I is the image of a two-sided ideal I' in $\Gamma_\beta(A)$ containing M, and, since M is a maximal disjoint two-sided ideal, $I' \cap A \neq (0)$, hence $I \cap A \neq (0)$ in B.

Let J b the minimal two-sided in ideal in A. $I \cap A$ is also a two-sided ideal in A, hence it contains J, and I contains the ideal generated by J in B. This ideal J' is, then, a minimal two-sided ideal in B, thus B is subdirectly irreducible.

1.e Embedding of a ring into a ring with identity element. Let A be a ring without identity-element. We can embedd it into a ring with identity-element and with the same characteristic n, following the methods developed by J. L. Dorroh [7] and Brown and McCoy [5], which consist in taking all pairs (a, m'), with $a \in A$ and $m' \in E_n$ (the residue-class ring of the integers reduced modulo n); the sum and the product being defined by :

$$(a_1\ m'_1) + (a_2, m'_2) = (a_1 + a_2, m'_1 + m'_2)$$
$$(a_1, m'_1)\,(a_2, m'_2) = (a_1a_2 + m_1a_2 + m_2a_1, m'_1m'_2)$$

The product is uniquely defined, since n is equal to the characteristic of A ; in this case, m_ia_j is uniquely defined by m'_i (the image of m_i in E_n) and a_j.

We shall call A' the ring of all such pairs.

If $f(x)=0$ is an equation with coefficients in A, it has the form $f(x)=\sum_i a_{il}X^{il}a_{i2}X^{i2} \ldots a_{in_i} = 0$. Then, since the ring A may be identified with the subring coincident with the set of pairs $(a, 0)$ in A', we may also identify that equation with the A'-equation

$$f'(x)=\sum_i (a_{il}, 0)\, x^{il}\, (a_{i2}, 0)\, x^{i2} \ldots (a_{in_i}, 0) = 0$$

We wish now to prove the following theorem:

THEOREM 1.2. — *If $f(x) = 0$ is a solvable A-equation, it is also a solvable A'-equation.*

If this theorem is true, we see that the embedding of a ring A into a ring A' does not change the solvability of the equations in A. This is important, because in general an arbitrary embedding may change the character of some equations.

The converse of the theorem is trivial.

Proof: We suppose that $f(x)=0$ is a solvable A-equation, that is, the two-sided ideal generated by $f(X)$ in the free extension of A is disjoint with A.

To prove the theorem we shall consider two cases, namely, solutions with no condition imposed and commutative solutions, that is, solutions in the center of the extension. In both cases, we suppose the solvability of the A-equation.

First case: Let us suppose that

$$f(x)=\sum_i a_{il}x^{il}a_{i2}x^{i2}\ldots a_{in_i}=0$$

is a solvable A-equation, that is, $(f(X))\cap A=(0)$ in $\Gamma_1(A)$

The elements of $(f(X))$ have the form

$$g(X)=\sum_{i'} p_{i'}(X)\cdot f(X)\cdot q_{i'}(X)+mf(X)$$

and, if we write

$$p_{i'}(X)=\sum_j b_{jli'}X^{jli'}\ldots b_{jmi'}$$

and

$$q_i(X)=\sum_k c_{kli'}X^{kli'}c_{k2i'}X^{k2j}\ldots c_{kmki'}$$

we have

$$g(X)=\sum_i\sum_{i'}\sum_j\sum_k b_{j1i'}X^{j1i'}\ldots b_{jmji'}\cdot a_{i1}X^{i1}\ldots a_{in_i}\cdot c_{k1i'}X^{k1i'}\ldots c_{knki'}+mf(x)$$

by our assumptions, $g(X)\in A$ implies $g(X)=0$.

Let us write, now, $f(x)=0$ as an A'-equation $f'(x)=0$, that is

$$f'(X)=\sum_i (a_{i1},0)X^{i1}(a_{i2},0)\ldots(a_{in_i},0)$$

The elements of $(f'(X))\subseteq\Gamma_1(A')$ have the form

$$g'(X)=\sum_i\sum_{i'}\sum_j\sum_k (b_{j1i'}\cdot h_{j1i})X^{j1i'}\ldots(b_{jmji'}\cdot h_{jmji'})\cdot(a_{i1}\cdot 0)X^{i1}\ldots$$
$$\ldots(a_{in_i},0)\cdot(c_{k1i'},l_{k1i'})X^{k1i'}\ldots(c_{kmki'},l_{kmki'})$$

Now, if $g'(X) \in A'$, since

$$(b_{jm_ji}, h_{jm_ji})\,(a_{is}, 0) = (b_{jm_ji}, 0)\,(a_{is}, 0) + h_{jm_ji}\,(a_{is}, 0)$$

and

$$(a_{ik}, 0)\,(c_{jli}, t_{jli}) = (a_{ik}, 0)\,(c_{jli}, 0) + t_{jli}\,(a_{ik}, 0)$$

we have $g'(X) = d \in A$, and we can choose $p_{i'}(X)$ and $q_{i'}(X)$ in $\Gamma_1(A)$ such that

$$g(X) = \sum_i p_{i'}(X) \cdot f(X) \cdot q_{i'}(X) = d \in A\,;$$

then, $d = 0$, and the theorem is proved.

Second case — If we want X to commute with every (a, n) in A', and the extension to be unit-preserving, then, the residue-class ring of the free extension modulo de ideal of the elements giving trivial equations, is isomorphic to the (classical) polynomial ring, and, then, we can start from such a polynomial ring. Furthermore, the free extension of A, for X in the center, may be reduced to the ring of all formal sums

$$\sum_0^h a_i X_i + \sum_1^h m_i X_i,$$

with m_i integers and $a_i \in A$.

Let $f(x) = \sum_0^h a_i x^i = 0$ be a solvable A-equation, then $(f(X)) \subseteq \Gamma_1(A)$ is the set of all sums

$$g(X) = \sum_0^n \left(\sum_0^{h'} b_j X^j + \sum_0^{h'} m_j X^j\right)\left(\sum_0^h a_i X^i\right)\left(\sum_0^{h''} c_k X^k + \sum_0^{h''} m_k X^k\right),$$

while the principal ideal generated by $f'(X)$ in the polynomial ring of A' is the set of sums

$$g'(X) = \sum_0^n \left(\sum_0^{h'} (b_j, m_j)\, X^j\right)\left(\sum_0^h (a_i, 0)\, X^i\right)\left(\sum_0^{h''} (e_k, m_k)\, X^k = \right.$$
$$= \sum_0^n \left(\sum_0^{h'} (b_j, 0)\, X^j + \sum_0^{h'} m_j X^j\right)\left(\sum_0^h (a_i, 0)\, X^i\right)\left(\sum_0^{h''} (c_k, 0)\, X^k + \sum_0^{h''} m_k X^k\right).$$

Then, if $g'(X) = (d, m) \in A'$, we must have $g'(X) = (d, 0) \in A \subseteq A'$. In addition, we can choose in the reduced free extensión of A an element $g(X) = d \in A$, so that, by our hypetesis on the solvability of $f(x) = 0$, we have $d = 0$. Thus from $g'(X) \in A'$ we arrive to $g'(X) = 0$, and the theorem is proved.

The commutative case (starting from commutative rings) is a particularization of the second case, hence, the theorem is proved above, but it is not a special case of the first, because of the additional conditions imposed on the solutions.

Since this embedding process does not change the solvability of equations, from now on we shall confine our attention only to rings with identity-element, and to their identity-preserving extensions.

2. UNILATERAL LINEAR EQUATIONS AND SEMI-FIELS

2.a The solvability of the unilateral linear equation. Let a be a given element of a ring (with identity) A. The set of all $x \in A$ such that $xa=0$ (resp. $ax=0$) will be called the left- (resp. right-) annihilator of a and denoted by 0_a^l (resp. 0_a^r). It is clear that a right- (left-) annihilator is a right- (left-) ideal [20].

We shall prove now the following theorem:

THEOREM 2.1. — $0_a^r \subseteq 0_b^r$ *is a necessary and sufficient condition for a left-linear equation* $xa = b$ *to be solvable in a ring* A *with identity.*

The condition is evidently necessary, because, if the equation is solvable, there exists at least one extension B of A in which there is an element c such that $ca = b$, hence, for every y in B (in particular in $A \subseteq B$ such that $ay = 0$, we will have $by = cay = 0$, hence $0_a^r \subseteq 0_b^r$.

To prove the sufficiency we shall use our theorem 1.1, that is, we shall consider the ideal $(f(X))$ in the free extension $\Gamma_1(A)$.

We must show that, under the condition $0_a^r \subseteq 0_b^r$, the element $Xa-b$ cannot be reduced to a non-zero constant by multiplication and addition.

To simplify the proof, we shall see first that

$$g(X)=p(X)\,(Xa-b)\,q(X) \in A \text{ and } 0_a^r \subseteq 0_b^r \text{ imply } g(X)=0$$

Let

$$p(X)=\sum_i c_{i1}X^{i1}c_{i2}X^{i2}\ldots c_{in_i}$$
$$q(X)=\sum_j d_{j1}X^{j1}d_{j2}X^{j2}\ldots d_{jn_j}$$

and let us suppose that $g(X) \neq 0$ and $g(X) \in A$. Then, there will be in $p(X)$ and $q(X)$, respectively, terms of the form c_{00} and d_{00} such that $c_{00}bd_{00} \neq 0$. Hence, $bd_{00} \neq 0$, and, by our hypothesis, $ad_{00} \neq 0$.

Therefore, $g(X)$ must contain $c_{00}Xad_{00}$, and, since $g(X)\epsilon A$, the term of first degree in $g(X)$ must vanish, that is,

$$c_{10}Xbd_{00}+c_{00}bXd_{10}+c_{00}Xad_{00}=0,$$

and, since $c_{00}Xad_{00}\neq 0$, at least one of the terms $c_{10}Xbd_{00}$ or $c_{00}bXd_{10}$ must be different from zero, implying $c_{10}X\neq 0$ or $c_{00}b\neq 0$, respectively.

From $c_{00}b\neq 0$ follows $c_{00}a\neq 0$, and in both cases a term of second degree, either $c_{10}XaXd_{00}$ or $c_{00}aX^2d_{10}$ does not vanish.

In any case, the condition $g(X)\epsilon A$ implies, by the same argument, the existence of (at least) one non-vanishing term of third degree in $g(X)$, and so on. This is in contradiction with the fact that the degree of a polynomial is finite.

Then, our assertion is proved.

Furthermore, $\sum_i c_iX^jad_i=0$ implies that $\sum_i c_iX^jad_i$ can be reduced to a single term $c'X^jad'$. This reduction must be made by termwise succesive elimination.

One term $c_rX^jad_r$ can be reduced if at least one of the following conditions holds;

1) $c_r=\sum_{i\neq r}\lambda_i c_i$ (λ_i integers), in which case

$$\sum_i c_iX^jad_i=\sum_{i\neq r}c_iX^ja\,(d_i+h_id_r)$$

2) $ad_s=\sum_{i\neq s}\lambda_i ad_i$, implying $\sum_i c_iX^jad_i=\sum_{i\neq s}(c_i+\lambda_i c_s)\,X^jad_i$

In any case, the same reduction can be performed on $\sum_i c_iX^kbd_i$ — (the first is trivial and the second follows from $ad_s=\sum_{i\neq s}\lambda_i ad_i\rightarrow$

$$\rightarrow\sum_i\lambda_i ad_i=0\ (\lambda_s=-1)\rightarrow a\,(\sum_i\lambda_i d_i)=0\rightarrow b\,(\sum_i\lambda_i d_i)=0\ \rightarrow$$

$\rightarrow bd_s=\sum_{i\neq s}\lambda_i ad_i$), and their sum is, respectively,

$$\sum_i c_iX^kdb_i\,d_i=\sum_{i\neq r}c_iX^kb\,(d_i+\lambda_i d_r)$$

or

$$\sum_i c_iX^kbd_i=\sum_{i\neq s}(c_i+\lambda_i c_s)\,X^kbd_i.$$

Then, $\sum_i c_iX^jad_i=c'X^jad'$ implies $\sum_i c_iX^kbd_i=c'X^kbd'$, and from $c'X^jad'=0$ follows either $c'=0$ or $ad'=0$, and in both cases $c'X^kbd'=0$.

Since an element *of* $I=(Xa-b)$ is a sum of expressions all similar to $g(X)$, that is, every element of I has the form

$$f(X)=\sum_i p_i(x)\,(Xa-b)\,g_i(X)$$

we can write $f(X)=\sum_i g_i(X)\,\epsilon\,\mathrm{I}$.

To prove our theorem by contradiction, let us suppose that $f(X) \in A$ and $f(X) \neq 0$. Then, there exists c_{i00} and d_{i00} in $p_i(X)$ and $q_i(X)$, respectively, such that

$$\sum_i c_{i00} b d_{i00} \neq 0,$$

which, by the above argument, with c_{i00} and d_{i00} in place of c_i and d_i, implies $\sum_i c_{i00} b d_{i00} \neq 0$.

The proof proceeds now as in our simplified case.

We can establish a similar condition for commutative extensions of commutative rings, but the proof differs from the preceeding one. In commutative rings, $0_a^r = 0_a^l$ will be written 0_a.

THEOREM 2.2.— *If A is a commutative ring, the equation* $ax - b = 0$ *admits a commutative solution if and only if* $0_a \subseteq 0_b$.

We say that the equation admits a commutative solution if there exists at least one commutative extension in which it has a solution.

We have seen that commutative identity-preserving extensions of commutative rings are homomorphic images of the (classical) polynomial ring. Since A has an identity-element (otherwise the theorem is not appliable) we must prove that

$$(aX - b)\, p(X) \in A \text{ implies } (aX - b)\, p(X) = 0$$

Let $p(X) = \sum_1^n c_i X^i$. Suppose the condition of the theorem is fulfilled and assume $(aX - b)\, p(X) = d \in A$.

Then $(aX - b)\, p(X) = ac_n X^{n+1} + \sum_1^n (ac_{i-1} - bc_i) X^i - bc_0 = d$ implies

$$\begin{aligned} ac_n &= 0 \\ ac^{i-1} = bc_i &= 0 \quad (n \geq i \geq 1) \\ -bc_0 &= d \end{aligned}$$

From the first two equations and by $0_a \subseteq 0_b$, succesively follows $bc_{i-1} = 0$ $(i = n, n-1, \ldots, 1)$, finally arriving to $bc_0 = d = 0$. Thus, the condition is sufficient.

The necessity being obvious, the theorem is proved.

To show that in general the theorem is not valid without assuming the existence of an identity-element, we have the following example: Let A be a trivial ring, that is, a ring for which $A^2 = (0)$, hence, for every $a \in A$, $aA = (0)$, the ring is commutative and $0_a = A$. Since $0_0 = A$, the equation $0x = a$, evidently unsolvable, satisfies the conditions of the theorem.

Remark: In view of theorems 2.1 and 2.2, we can assert that, if A is a commutative ring with identity, every solvable linear equation admits (or has) a commutative solution.

2.b. — An open question: the compatibility of equations. As we have seen in the previous section, given an equation $fx = 0$, with coefficients in a ring A, every extension of A containing a solution has a subring B, simple extensión of A, which is a homomorphic image of the free extension of A with one generator, modulo an ideal containing $f(X)$, and hence, containing the (two-sided) ideal $(f(X))$. Let us suppose two solvable equations $f(x) = 0$ and $g(x) = 0$ are given in A. If we «solve» the first, that is, if we build some extension of A containing at least one root of $f(x)=0$, it may happen that we introduce new elements which make $g(x)=0$ unsolvable in the extension.

If $g(x)=0$ is a solvable A-equation, unsolvable in every extension of A containing a root for $f(x) = 0$, we shall say they are incompatible. The general theorem for extensions says that two equations are compatible if and only if the (two-sided) ideal $(f(X), g(Y))=I$ verifies that $I \cap A = (0)$ in the free extension with two generators X, Y.

Now the following question is open: is every set of solvable equations, compatible? The question is not yet answered. Only for special cases we have an affirmative answer.

In general, we say that a set of equations is compatible if there exists an extension of the original ring in which all the equations have solution. For sets of only one equation, compatibility is equivalent to solvability.

In fields, it is known that there are extensions where all solvable equations can be simultaneously solved, hence they all form a compatible set.

We can prove the following theorem, due to R. Ricabarra, on the compatibility of linear equations.

We recall that a ring is called semisimple if there exists a set of prime (2) two-sided ideals with zero intersection.

THEOREM 2.3 (*Ricabarra*). — *In a semisimple ring, the set of all linear solvable equations is compatible*

(2) A two sided ideal P is called prime if, as in the commutative case, $ab \in P$, a not in P implies $b \in P$.

By definition, a semisimple ring is a subdirect sum of rings without proper zero-divisors. By theorem 2.5, whose proof is independent of these considerations, each of these rings can be embedded in a quotient ring ([3]).

In the commutative case, it is equivalent to say that it has no nilpotent elements. We find, in this case, a commutative extension in which every solvable linear equation of the original ring has a solution.

In the general case, we only consider unilateral linear equations, since no conditions are known for the general linear equation $\sum_{i=0}^{n} a_{i1} x a_{i2} = b$ to be solvable.

We can consider, now, our original ring A, as a subring of the direct sum of the division rings obtained from the (not necessarily commutative) integral domains, homomorphic images of A. That direct sum will be called C.

Given the set $\Omega = \{\alpha\}$ of all prime ideals in A, each element of C may be considered as a function defined on the set Ω and taking values in the quotient rings extensions of A/α [14]. Hence, the set of all elements of A is a subset of the whole set of such functions.

We shall call *projection* of an element $a \in A$ on the quotient ring R_α (containing $A\alpha$) the image a_α of a by the homomorphism $A \to A/\alpha$.

We shall call *projection* of an equation $ax = b$, with coefficients in A, on the quotient ring R_α, the equation $a_\alpha x = b_\alpha$ in R_α, where a_α and b_α are the projections of a and b, respectively, on R_α. It is worth noticing that the equation $cd = 0$, viewed in the function ring C means that for every α either c_α or d_α is zero.

As it has been said above, each element of A may be considered as a function of the ring C Let $ax = b$ (or $xa = b$) be a solvable A-equation. If Λ_a, is the set of all prime ideals containing a, and Λ_b that of all prime ideals containing b, then the equation is precisely unsolvable at the points $\alpha \in \Lambda_a - \Lambda_b$. Thus, to keep the solvability of $ax = b$ we must take as identical functions differing on points of $\Lambda_a - \Lambda_b$ only, that is to say, we must identify with the zero-function all those fnnctions taking values diefferent from zero only at points of $\Lambda_a - \Lambda_b$. These functions wil be called *trivial functions*.

([3]) The classical method of embedding a commutative integral domain into a field by adjunction of all formal inverses does noc hold, in general, in the non-commutative case. O. Ore [21] has given necessary and sufficient conditions for the ring so obtained to be a quotient ring. The quotient ring may be defined as the minimal extension (sec. 1*d*) by adjunction of the solutions of all equations $ax = 1$ ($xa = 1$).

In the following lemmas we shall show that the class of all trivial functions corresponding to all left- (or right-) linear equations is a (two-sided) ideal I disjoint with A in C, and consequently that C/I is an extension of A preserving the solvability of the given linear equations.

In the homomorphic image of C the equation $ax=b$ (and $xa=b$) is not only solvable but can also be solved. Its solution is found by solving the projected equations in each quotient ring R_α, α not in $\Lambda a - \Lambda b$, and taking as a solution any class of functions modulo I containing a function that for α not in $\Lambda a - \Lambda$ coincides with the solutions of the projected equations. In fact, for such a function x_α, $ax_\alpha - b$ is a trivial function because it vanishes outside of $\Lambda a - \Lambda b$, hence passing to the classes $a\{x_\alpha\} - b = 0$. In general the solution is not unique because arbitrary values in R_α can be assigned to the function at points where $a_\alpha = b_\alpha = 0$, the difference of two functions thus obtained not being a trivial function in general.

Having proved that in C any solvable linear A-equation can be solved we haven shown that there are no sets of incompatible equations in A.

Let $\Omega = \{\alpha\}$ designate the class of all prime ideals in A. By the semi-simplicity there is, for every non-zero $a \in A$, an ideal not containing a, hence $\bigcap_{\alpha \in \Omega} \alpha = (0)$. (4)

We introduce now a notion of closure for all subsets of Ω, in the following way: The closure $\overline{\Lambda}$ of a subset $\Lambda \subseteq \Omega$ is the set of all prime ideals containing the elements of A that simultaneously belong to all $\alpha \in \Lambda$ that is, $\overline{\Lambda}\{\alpha \mid \alpha \supseteq \bigcap_{\beta \in \Lambda} \beta\}$. It is easily verified that the operation thus defined has all properties of a topological closure: *i)* $\overline{\Lambda} \supseteq \Lambda$, *ii)* $\overline{\Lambda_1 \quad \Lambda_2} = \overline{\Lambda_1} \cup \overline{\Lambda_2}$, *iii)* $\overline{\overline{\Lambda}} = \overline{\Lambda}$. The only property requiring a proof is the second one, the other two are trivial. Moreover, $\overline{\Lambda_1 \cup \Lambda_2} \supseteq \overline{\Lambda_1} \cup \overline{\Lambda_2}$ is an immediate consecuence of *i)* and *iii)*, so it is enough to prove $\overline{\Lambda_1 \cup \Lambda_2} \subseteq \overline{\Lambda_1} \cup \overline{\Lambda_2}$. This we do by showing that any γ in $\overline{\Lambda_1 \cup \Lambda_2}$ and not in $\overline{\Lambda_2}$ must be in $\overline{\Lambda_1}$. We notice first that γ not in $\overline{V_2}$ implies the existence of a b in the intersection of all ideals of $\overline{\Lambda_2}$ not contained in γ. Further, for every a in the intersection of all ideals of $\overline{\Lambda_1}$, the product ab is in the intersection of all

(4) In all considerations that follows it is enough to take, instead of Ω, any subclass having the same intersection property.

ideals of $\overline{\Lambda_1} \cup \overline{\Lambda_2}$, hance in γ. Since b is not in γ, it follows that $a \in \gamma$, which by the arbitrariness of a implies $\gamma \in \overline{\Lambda_1}$ as we wanted to prove.

A closed set is a set coinciding with its closure ($\Lambda = \overline{\Lambda}$). It is easily proved that the intersection of any number of closed sets, and the union of a finite number, is closed.

A set of ideals Λ such that the intersection of all ideals not belonging to it is the ideal (0) is called a *redundant set of ideals*. It is clear that a set Λ is redundant if and only if $\overline{\Omega - \Lambda} = \Omega$.

LEMMA 2.1. *The set of all points (ideals) where a trivial function is different from zero is contained in a closed redundant set.*

PROOF. — The solvebility condition $0_a^l \subseteq 0_b^l$ simply means that every ideal not containing b contains the intersection of all ideals not containing a. In other terms, $\Omega = \Lambda_b \subseteq \Omega - \Lambda_a$ where Λ_a and Λ_b are the sets of all ideals containing a and b respectively. Moreover the set of points where a trivial functions is different from zero is contained in $\Lambda_a - \Lambda_b = \Lambda_a \cap (\Omega - \Lambda_b)$ hence, contained in $\Lambda_a \cap \overline{(\Omega - \Lambda_b)}$. This set, as the intersection of two closed sets, is closed. La addition, it is redundant because

$$\overline{\Omega - (\Lambda_a \cap \overline{(\Omega - \Lambda_b)})} = \overline{(\Omega - \Lambda_a) \cup (\Omega - \overline{(\Omega - \Lambda_b)})} \supseteq \overline{\Omega - \Lambda_a} \cup (\Omega - \overline{(\Omega - \Lambda_a)}) = \Omega.$$

LEMMA 2.2. — *The union of two closed redundant sets is redundant* [5].

PROOF. — We have to prove that $\overline{\Lambda_i} = \Lambda_i$ and $\overline{\Omega - \Lambda_i} = \Omega$, $i = 1, 2$, imply $\overline{\Omega - (\Lambda_1 \cup \Lambda_2)} = \Omega$.

Let $F = \overline{\Omega - (\Lambda_1 \cup \Lambda_2)}$. Obviously F is closed and $F \supseteq \Omega - (\Lambda_1 - \Lambda_2)$. Hence $F \cup \Lambda_1 \supseteq \Omega - \Lambda_2$, and it follows $F \cup \Lambda_1 = \overline{F \cup \Lambda_1} = \overline{F \cup \Lambda_1} \supseteq \overline{\Omega - \Lambda_2} \supseteq \Omega$ which succesively implies $F \supseteq \Omega - \Lambda_1$, $F \supseteq \overline{\Omega - \Lambda_1} = \Omega$. That is, $F = \Omega$.

LEMMA 2.3. — *The set of all trivial functions generates in C a two-sided ideal disjoint with A.*

PROOF. — 1) If f is a trivial function, hence, a function vanishing outside of a redundant set, then all finite products containing f will also vanish outside of the same set.

[5] In the topological terminology this lemma expresses the fact that the union of two closed nowhere dense sets is nowhere dense.

2) If f and g are functions vanishing outside of clased redundant sets Λ_f and Λ_g respectively, then the function $f-g$ will vanish outside of the set $\Lambda_f \cup \Lambda_g$, which by lemma 2.2 is also redundant.

3) As the two-sided ideal I generated by a set of elements of a ring (in this case the trivial functions) is the set of all finite sums of finite products containing at least one element of the given set, it follows that all functions belonging to such an ideal will vanish outside of a closed redundant set.

4) Since by definition no element of A is contained in all ideals not belonging to a redundant set, it follows that the functions associated with elements of A are not functions of the ideal I. Hence $A \cap I = (0)$, and C/I is an extension of A (6).

2.c. The « conditional » theory of compatible sets. Given a compatible set of equations, which can also be of some special type, a.e. linear right-, linear left-, linear, we wish to prove that it is always contained in a maximal compatible set of the same type. Clearly, if there is no set of incompatible equations, a maximal compatible set should be understood as the set of all equations. We must make a convenient construction to define chains of sets and apply Zorn's lemma.

We shall say *p-equations* or *equations of type p* whenever we speak about sets of equations having some property p.

We shall prove here the following theorem :

THEOREM 2.4. — *Every compatible set of p-equations is contained in a maximal compatible set of p-equations.*

Naturally, we say that C is a maximal compatible set of p-equations if, adding to it any other arbitrary p-equation, the new set is always incompatible.

It is trivially true that, if in a set there is an unsolvable equation, it is incompatible. So, we may restrict our attention to sets of solvable equations only.

Let C be the set of all solvable p equations in an arbitrary ring (not necessarily with identity element) A, and let β be the cardinal number of C. We can build the free extension of A with β generators

(6) In the commutative case we can, in addition say that C/I is also commutative and semisimple. This easily proved by showing that there are no nilpotent elements in C/I.

and establish a one to-one correspondence between the generators and the equations of C. We associate, then, the i^{th} p ecuation of C with the i^{th} generator of the free extension, that is, $p_i(x) = 0 \rightarrow X_i$.

A subset $S \supseteq C$ is compatible if and only if the ideal

$$\alpha_S = (\{p_i(X_i)\,;\ i \in S\}) \text{ verifies } \alpha_s \cap A = (0)$$

This ideal will be called the ideal *associated* with S.

It is evident that $S \subseteq S'$ is equivalent to $\alpha_s \subseteq \alpha_{s'}$.

We say that the family $\{S\}$ is a chain if ond only if it is linearly ordered by inclusion in the family of subsets of C. Hence, the associated ideals form also a chain.

We have a chain of compatible sets $\{S\}$ of p-equations if and only if their associated ideals form a chain $\{\alpha_S\}$ with $\alpha_S \cap A = (0)$. It is known that, in this case, the set of ideals associated with every subset of C constitutes an inductive system. Thus, Zorn's lemma can be applied and the theorem is proved.

2.d. — The embedding of a ring in a p-closed ring. We say that a ring A is *p-closed* if every solvable p-equation in it has at least one solution in A.

Let B_0 be a ring which is not p-closed (obviously, if B_0 is p-closed, no proper embedding is necessary), S_0 a maximal compatible set of p-equations in B_0, and α_0 the associated ideal of S_0 in the free extension of B_0 with a set of generators with the same cardinal number as S_0. Let B_1 be the homomorphic image of that free extension modulo α_0. Since S_0 is a maximal compatible set of p-equations, no other p-equation solvable in B_0 remains solvable in B_1; furthermore, B_1 has solutions for every solvable p-equation of S_0. B_1 has the same properties if we replace α_0 by another ideal α'_0 such that $\alpha'_0 \supseteq \alpha_0$ and $\alpha'_0 \cap B_0 = (0)$.

If B_1 is p-closed the process is finished; otherwise, we repeat the process with S_1 in place of S_0 (we can also remove from S_1 those p-equations having solutions in B_1) and find a B_2 which has the solutions of all p-equations of B_1, solvable in B_2. The process may be repeated indefinitely.

If we arrive to a p-closed ring in a finite number of steps, the embedding of B_0 in B_n (the last ring so obtained) is the one desired. If no B_i is p-closed, we define B_∞ as the join (set theoretical) of all B_i (i 1, 2, 3,...). It is well known that B_∞, defined as the join of

a chain of rings is also a ring. Furthermore, if $p(x) = 0$ is a solvable p-equation with coefficients in B_∞, its coefficients are elements of rings B_i, and, since there is only a finite number of them, there is a B_n eontaining all coefficients. Thus $p(x) = 0$ is a solvable p-equation in B_n, and, since it is also solvable in B_∞, it remains solvable in B_{n+1}, hence it has a solution in B_{n+1} and therefore in B_∞. This proves B_∞ is p-closed. It is true, then, that:

THEOREM 2.5. — *Every ring may be embedded in a p closed ring.*

2.e. — Semi-fields. DEFINITION 2.1. — *A ring A will be said a right- (left-) semi-field if every solvable right- (left-) linear equation has a solution in A.*

DEFINITION 2.2. — *A ring A will be said a semi-field if it is simultaneously a right- and left semi-field.*

DEFINITION 2.3. — *A ring A will be said an absolute semi-field if every solvable linear equation has a solution in A.*

In commutative rings, our three definitions coincide.

As a corollary of theorem 2.5, we have:

COROLLARY 2.1. — *Every ring may be embedded:*

a) *in a right- (left-) semi-field,*
b) *in a semifield,*
c) *in an absolute semi-field.*

3. ISOLATERAL LINEAR SYSTEMS AND COMPLETE SEMIFIELDS

DEFINITION 3.1. — *A set of unilateral equations will be said isolateral if every equation is a left (or right) one.*

The purpose of this section is to establish solvability conditions for isolateral linear systems.

3.a. The common solution of a set of isolateral linear equations. If A is an associative ring, we call A' (resp. A'') the A-left- (resp. A-right-)module underlying A, and A'_α (resp. A''_α) the direct sum of α A modules all isomorphic to A' (resp. A'').

The elements of A'_α (resp. A''_α) will be called left-vectors (resp. right-vectors); they are the α-tuples $[a_1, a_2, \ldots]$, and their sum is defined by adding the elements which lie in the same place, and the left- (resp. right-) product by an element of A by multiplying on the left (resp. on the right) every element of the α-tuple by the element of A.

Given two elements, $\bar{a}_l = [a_1, a_2 \ldots] \in A'_\alpha$ and $\bar{b}_r = [b_1, b_2, \ldots] \in A''_\alpha$ their inner product is defined by $(a_l, b_r) = \sum a_i b_i$; if α is infinite, all but a finite number of $a_i b_i$ must be zero, a nd the summation extended to those non-zero products.

If $\bar{a}_l \in A'_\alpha$, the set of all $\bar{x}_r \in A''_\alpha$ such that $(\bar{a}_l, \bar{x}_r) = 0$ will be called the right-annihilator of $\bar{a}_l$ and denoted by $0^r_{\bar{a}_l}$. It is an A-right-submodule of A''_α.

For right-vectors $\bar{b}_r$ we can define, in a similar fashion, the left-annihilator $0^l_{\bar{b}_r} \subseteq A'_\alpha$.

If a system of n equations $a_i x = b_i$ $(1 \leqq i \leqq n)$ is given, we shall call the right-vectors $\bar{a}_r = [a_1, a_2, \ldots, a_n] \in A''_n$ and $\bar{b}_r = [b_1, b_2, \ldots, b_n]$ its corresponding vectors.

THEOREM 3.1. — *The necessary and sufficient conditions for a set of* n *isolateral linear equations* $a_i x = b_i$ *(resp.* $x a_i = b_i$*) in a ring with identity element, to admit a common solution, is that* $0^l_{\bar{a}_r} \subseteq 0^l_{\bar{b}_r}$ *(resp.* $0^r_{\bar{a}_l} \subseteq 0^r_{\bar{b}_l}$*) for the corresponding vectors of the system.*

The proof is similar to that of theorem 2.1. Here we must consider the ideal generated by the given set of equations in the free extension with *one* generator (one generator because we wish a common solution).

If the ideal has an infinite basis, since only finite sets heve been used in the proof, we can give a more general theorem:

THEOREM 3.2. — *The necessary and sufficient condition for an arbitrary set of isolateral linear equations* $a_i x = b_i$ $(x a_i = b_i)$ *in a ring with identity element to admit a common solution is that* $0^l_{\bar{a}_r} \subseteq 0^l_{\bar{b}_r}$ $(0^r_{\bar{a}_l} \subseteq 0^r_{\bar{b}_l})$ *holds for the corresponding vectors of every finite subset of equations.*

3. b. — The equation with several variables. Let $\sum_l^m a_i x_i = b$ (resp. $\sum_l^m x_i a_i = b$) be an unilateral linear equation with m variables. We shall establish conditions for solvability in identity-preseving extensions (in general no center-preserving-ones).

THEOREM 3.3. — *A necessary and sufficient condition for an unilateral equation* $\sum_1^m a_i x_i = b$ (*resp.* $\sum_1^m x_i a_i = b$) *in a ring with identity element to be solvable is* $\cap\, 0_{a_i}^l \subseteq 0_b^l$ (*resp.* $\cap\, 0_a^r \subseteq 0_b^r$).

PROOF. — To study the solvability of the linear equation $\sum_l^m x_i a_i = b$ we must start from the free extension with m indeterminates X_i, and consider there the ideal $I = (\sum_l^m X_i a_i - b)$, which is the set of all sums.

$$f(X_1, \ldots X_m) = \sum_j p_j (X_1 \ldots X_m)\ (\sum_l^m X_i a_i - b)\ q_j (X_1, \ldots, X_m)$$

If the given equation were not solvable, there would be an element $f(X_1, \ldots, X_m) \in I$ such that $f(X_1, \ldots, X_m) \in A$ and $f(X_1, \ldots, X_m) \neq 0$. Hence, there would be elements c_{j00} in p_j and d_{j00} in q_j such that

$$\sum_j c_{j00}\, d b_{j00} \neq 0$$

If for every i, $\sum_j c_{j00} X_i a_i d_{j00} = 0$, then $\sum_j c_{j00} X_i a_i d_{j00} = c' X_i a_i d'$, and by considerations similar to those of theorem 2.1, $\sum_j c_{j00} b d_{j00} = c' b d'$.

Now, $c' X_i a_i d' = 0$ $(1 \leqq i \leqq m)$ implies $c' = 0$ or $a_i d' = 0$ $(1 \leqq i \leqq m)$, and in any case it follows $c' b d' = 0$. Hence, there is at least one index i for which $\sum_j c_{j00} X_i a_i d_{j00} \neq 0$, and the proof proceeds as in theorem 2.1.

For commutative rings the situation is quite different. Evidently, if we look for general extensions (identity-preserving) we are in a particular case of the previous theorem, but if we want commutative extensions the conditions while being necessary, are no longer sufficient, as the following example shows:

Example: Let $E_2[X, Y, Z]$ be the polynomial ring over the Boolean field E_2 and consider the quotient ring $E_2[X\ Y\ Z]/(X^2\ Y^2, XYZ, XZ^2, YZ^2, Z^3)$. If a, b and c are the homomorphic images of X, Y, and Z respectively, the equation $ax + by + c = 0$ satisfies the conditions of the theorem, and is unsolvable, since $(ax + by + c)(ax + by + c) = c^2 = 0$.

We have seen in theorem 2.2 that the conditions of theorem 3.3 are sufficient in commutative rings if $m = 1$. We shall now another such case; the case when b is not a zero-divisor.

THEOREM 3.4. — *If* b *is not a zero-divisor, a necessary and sufficient condition for an equation* $\sum_1^m a x_i = b$ *to admit a commutative solution in a commutative ring with identity element is that* $\bigcap 0a_i = (0)$.

We shall prove the theorem by using some results of McCoy [13] which state that a system of homogeneous linear equations has a non-trivial solution if and only if the rank of the matrix (7) is less than the number of unknowns. In the considerations of that paper, it is also established that every non-zero solution annihilates every m by m determinant (8).

We shall give the proof in a special case, the generalization is immediate but laborious.

Let $ax + by = 0$ be an equation fullfilling the conditions of the theorem, and $p(X, Y)$ a polynomial such that $p(X, Y) . (aX + bY - c) \in A$. If $p(X, Y)$ is a constant, siuce pa and pb must be zero, the hypothesis implies that pc is also zero, and so that p is zero. We proceed now by induction on the degree of $p(X, Y)$. Let us suppose that for every $p(X, Y)$ of degree $n - 1$, the fact that the above product is in A implies that it is zero, and take a polynomial $p(X, Y)$ of degree n such that $p(X, Y)\ (aX + bY - c)$ is a constant. Let us call $z^i\ (0 \leqq i \leqq n)$ the coefficients of $X^{n-i}Y^i$ in the polynomial. Setting equal to zero the terms of degree $n+1$ of the product we must have $az_0 = 0$; $bz_{i-1} + az_i = 0\ (1 \leqq i \leqq n)$; $bz_n = 0$. Clearly, to prove $p(X, Y) = 0$ it is enough, by the induction hypothesis, to prove that all z_i vanish.

The above conditions form a system of $n+2$ equations with $n+1$ unknowns (the z_i). By McCoys results, $z_i (0 \leqq i \leqq n)$ annihilates all determinants of $n+1^{st}$ degree, which in this case coincide with the totality of products of $n+1^{st}$ degree in a and b.

Since a and b have no common annihilator, the amnihilation of all products of degree $n+1$ implies the annihilation of all products of degree n ; in its turn this implies the annihilation of all products of degree $n-1$, and so on. One finally gets to the annihilation of

(7) McCoy defines the rank of a matrix with coefficients in a commutative ring R, as follows : The matrix M is said of renk r if the determinants of all square minors of M of order $r+1$ admit a common anihilator in R but not those of order r. M is of rank zero if all elements of M are annihilated by a fixed element of R.

(8) The usual theorems on expansions of a determinant are valid if the elements lie in an arbitrary commutative ring, see McCoy [15].

products of the first degree, that is of a and b. Thus all z_i are annihilators of a and b, hence they all vanish, as we wanted to prove.

In another particular case, the stated conditions are also sufficient, as is indicated in the following theorem:

THEOREM 3.5. — *A necessary and sufficient conditions for a linear equation* $\sum_1^m a_i z_i = b$ *in a commutative principal ideal ring to admit a commutative solution is* $\bigcap 0_{a_i} \subseteq 0_b$.

PROOF: Let $\sum_1^m a_i x_i = b$ be an equation satisfying the conditions of the theorem. We call c the basis of the ideal generated by all a_i. We wish to prove now that $0_c = \bigcap 0_{a_i}$. Since $(c) = (a_i)$, we must have: $c = \sum_1^m a_i d_i$, $a_i = c e_i$. Thus any x annihilating all a_i's annihilates c and conversely, and our assertion is proved.

Now the conditions of the theorem say that $0_c \subseteq 0_b$, so that, $cy = b$ is a solvable equation (with commutative solution). Replacing c by $\sum_1^m a_i d_i$ the theorem is proved.

No other particular case will be studied here, instead we turn our attention to the search of necessary and sufficient conditions. The leading idea is the embedding of an arbitrary commutative ring into another for which the stated conditions are sufficient (see section 3. *c*)

LEMMA 3.1. — *Let* $\{a_i\}$ *be a set of elements of a commutative ring A; if an element* b *does not belong to the ideal generated by the* a_i's, *then* bX *does not belong to the ideal gerated by the* $a_i X$'s *in the (classical) polynomial ring* A [X] (9).

PROOF. If $bX = \sum_i a_i X . p_i(X)$, the terms of degree higher than one cancel mutually, and $bX = \sum_i aX . c_i = (\sum_i a_i c_i) X$. Consequently, $b = \sum_i a_i c_i$, that is $b \in (a_i)$.

LEMMA 3.2. — *If in a commutative ring* A *with identity element* b *is not in the ideal generated by a set* $\{a_i\}$, *there is an extension of* A *in which there exists an element* c *such that* $cb \neq 0$ *and* $ca_i = 0$ *for every i.*

PROOF. — We take the residue-class ring of the polynomial ring modulo the ideal generated by the set $\{a_i X\}$ as the extension of A. If we call c the image of X in this homomorphism, then by lemma 3.1, c satisfies all required conditions.

The converses of lemmas 3.1 and 3.2 are trivial.

(9) See remark at the end of this section.

We have now another method to embed a ring into a semi-field, namely, by introducing annihilator elements such that, for every b which is not in (a), there is at least one x with $ax = 0$ and $bx \neq 0$.

By example, starting from the integers and using the method of section 2, we can arrive to the rationals, and using this method we arrive to the direct sum of E_p (we know that the ring of integers is a subdirect sum of an infinite number of E_p, p prime). Both methods give us semi-fields, but in the first one a maximal set of solvable equations is also solvable and has solution, and with the second, the equations which remain solvable are only those which had solution in the first ring.

3.c. — Isolateral linear systems with a finite number of unknowns. We shall use here the terminology of 3.a.

If $\mathfrak{a}_l = \{\bar{a}_i\}$ is a set of left vectors in A'_α, its right annihilator is the set of all $\bar{x} \in A''_\alpha$ such that $(\bar{a}_i, \bar{x}) = 0$ for every i. This right-annihilator will be denoted by $0^r_{\mathfrak{a}}$. Clearly, $0^r_{\mathfrak{a}} = \cap\, 0^r_{\mathfrak{a}_i}$.

Given a system of n equations $\sum_{j=1}^{m} a_{ij}x_j = b_i$ $(1 \leqq i \leqq n)$, we shall call the right-vectors

$$\mathfrak{a}_r = \{[a_{1j}, a_{2j}, \ldots, a_{nj}]\}\ (1 \leqq j \leqq m) \text{ and } \{\bar{b}_r\} = \{[b_1, \ldots, b_n]\}$$

its corresponding sets of vectors.

Then, following similar lines as in the proofs of theorems 2.1, 3.1 and 3.3, we cam show :

THEOREM 3.6. — *A necessary and sufficient conditions for a system of* n *isolateral linear right- (left-) equations with* m *unknowns, to be solvable in a ring with identity is that that* $0^l_{\mathfrak{a}} \subseteq 0^l_{\mathfrak{b}}$ $(0^r_{\mathfrak{a}} \subseteq 0^r_{\mathfrak{b}})$ *for the corresponding sets of vectors of the system.*

THEOREM 3.7. — *A necessary and sufficient condition for an infinite system of isolateral linear right- (left-) equations with* m *unknowns, to be solvable is that* $0^l_{\mathfrak{a}} \subseteq 0^l_{\mathfrak{b}}$ $(0^r_{\mathfrak{a}} \subseteq 0^r_{\mathfrak{b}})$ *for the corresponding sets of vectors of every finite subsystem.*

3.d. — Homomorphisms and algebraic closure. Let I be a left-ideal in a ring (with identity) A (that is, an A-left-module) and σ an A-left-homomorphism of I into A, then $I_0 = \sigma(I)$ is also a left-ideal in A. If $\{a_i\}$ is a basis for I, then $\{\sigma(a^i)\}$ is a basis for I_0.

For every finite set $\{y_i\}$ with $\sum y_i a_i = 0$, it follows $\sum y_i \sigma(a_i) = 0$; therefore, the (non-necessarily finite) isolateral linear system $a_i x = \sigma(a_i)$ is solvable, (th. 3.2). Conversely, if an isolateral linear system $a_i x = b_i$ is solvable, then A can be embedded into another ring having an element θ which satisfies $a_i\theta = b_i$ for every i, and the mapqing $c \to c\theta$ is an A-left-homomorphism of I (the left-ideal generated by the set $\{a_i\}$ in-A) onto the left-ideal generated by the set $\{b_i\}$.

Hence, we have:

LEMMA 3.3. — *A left-ideal I_0 is an A-left-homomorphic image of a left-ideal I (in a ring A with identity) if and only if for an arbitrary basis $\{a_i\}$ for I and a conveniently chosen basis $\{b_i\}$ for I_0 the system $a_i x = b_i$ is solvable.*

Let us call, as in 3.a, A' and A'', respectively, the A-left-module and the A-right-module underlying A, and A'_α (resp. A''_α) the direct sum of α A-left-modules all isomorphic to A' (resp. A''), that is, the set of all α-tuples $[a_1\ a_2, \ldots, a_n, \ldots]$ with $a_j \in A'$ (resp. A'').

By similar considerations one can prove:

LEMMA 3.4. — *A left-ideal I is an A-left-homomorphic image of an A-left-submodule $M_n \subseteq A'_n$ if and only if for an arbitrary basis $\{[a_{i_1}, a_{i_2}, \ldots, a_{in}]\}$ for M_n and a conveniently chosen basis $\{b_i\}$ for I, the system $\sum_j a_{ji} x_j = b$ is solvable.*

If $[a_1, \ldots, a_n] \in A'_n$ and $[c_1, \ldots c_n] \in A''_n$, we have called $\sum a_i c_i \in A$ their inner product.

To say that the linear system $\sum_{j=1}^{n} a_{ji} x_j = b\ (i \in \Lambda)$ has a solution in A, is equivalent to say that the homomorphism σ defined by $\sigma([a_{1i}, \ldots, a_{ni}]) = b_i\ (i \in \Lambda)$ may be carried out by an inner product. In particular, if $n = 1$, the existence of a solution for the system $a_i x = b_i$ is equivalent to the fact that the homomorphism σ defined by $\sigma(a_i) = b_i$ may be carried out by a right-multiplication. In both cases the homomorphisms must be seen as A-left-homomorphisms of the A-left-submodules of A'_n and A', respectively, generated by the sets of left-vectors just indicated.

Let $M_\alpha = \{[a_{i_1}, \ldots, a_{in}, \ldots]\}$ be a left-submodule of A'_α; its right-annihilator is the submodule $0^r_{M_\alpha} \subseteq A''$, defined in 3.c.; the left annihilator of $0^r_{M_\alpha}$ will be called, according to M. Hall [11], the *closure* of M_α, and will be denoted by $\overline{M}_\alpha$.

In view of theorems 2.1, 3.1 and 3.2, we have:

THEOREM 3.8. — *Every solvable right-linear system* $\sum_1^n a_{ij}x_i = b$ $(1 \leqq j \leqq m)$ *of (at most)* α *equations with* k *unknowns has a solution in a ring (with identity) A if and only if every right-submodule of* A''_k *generated by (at most)* α *vectors is closed.*

If M_n is the A-left-submodule of A'_n generated by the set $\{[a_{i1}, \ldots, a_{in}]\}$ $(i \in \Lambda)$, we shall call the A-right-submodule $M'_\alpha \subseteq A''_\alpha$ (when α is the cardinal number of Λ) generated by the set $\{[a_{ij}, a_{2j}, \ldots, a_{mj}, \ldots]\}$ $(1 \leqq j \leqq n)$, its *reciprocal submodule.*

Lemma 3.4 and theorem 3.8 give us a generalization of a result of Ikeda and Nakayama [12] as follows:

COROLLARY 3.1 — *Every A-left-homomorphism of an A-left-submodule* $M_n \subseteq A'_n$ *into A may be carried out by an inner product if and only if the reciprocal submodule is closed.*

DEFINITION 3.2. — *A ring A will be called a right- (left-) complete semi-field if every solvable right- (left-) linear system of equations with only one unknown has a solution in A; A will be called a complete semi-field if it is a right- and a left-complete semi-field.*

By the results of Ikeda and Nakayama ([12], p. 16, th. 1 *iii*)) and corollary 3.1, the conditions of def. 3.2. imply the existence of solutions of solvable linear right-equations with an arbitrary (finite) number of unknowns. Recent results [25] show that this is true also for (finite or infinite) right-linear systems.

We can now state the following results, immediate consequences of the previous ones:

COROLLARY 3.2. — *A ring A with identity element is a right-semi-field if and only if every principal left-ideal is closed.*

COROLLARY 3.3. — *A ring A with identity-element is a complete right-semi-field if and only if every cyclic left-submodule of* A''_α *is closed for every* α.

The method presented in section 2.*d* does not ensure the possibility of embedding any ring into a complete semi-field. Under weaker conditions, such as that any finite solvable system of unilateral linear equations have a solution, this may howevsr be possible (10).

(10) The assertion, in [24], that every ring may be embedded into a complete semi-field, is not proved.

3.e. — Invariant ideals. The fundamental idea is that of invariance relative to an extension, as was given by M. Cotlar [6, p. 129] for some special sets in lattice theory. We shall give now an ideal-theoretical definition :

DEFINITION 3.3. — *If a ring* B *is an extension of a ring* A, *I an ideal in* A, *we shall say I is invariant relative to* B *if the intersection of* A *with the ideal I' generated by the elements of I is* B, *is precisely I.*

We shall give now some results for the (classical) polynomial extension of a ring :

THEOREM 3.9. — *In a ring* A *with identity, every two-sided ideal is invariant relative to the polynomial ring.*

If I_x is the ideal generated by the elements of I in the polynomial ring, it is evident that $I_x \cup A \supseteq I$.

We now prove the reverse inclusion. Let $I = (a_i)$, then $I^x = (a_i)^x$ $I^x = \sum_i (\sum_j p_{ij} a_i q_{ij})$ with $p_{ij} = \sum_l c_{ijl} X^l$, $q_{ij} = \sum_k d_{ijk} X^k$, but $\sum_i (\sum_j p_{ij} a_i q_{ij}) = b$, hence $b \in (a_i)$, and $(a_i)^x \cap A = (a_i)$.

The reasoning applies also to an infinite basis because only a finite number of a_i's appear in each expression.

COROLLARY 3.4. — *The lattice of all two-sided ideals of a polynomial ring (with coefficients in a ring* A) *contains a sublattice isomorphie to the lattice of all two-sided ideals of* A.

Thoorem 3.9 and corollary hold also for one-sided ideals.

If $0'_a$ is the annihilator in the polynomial ring of a constant a, and $(0_a)^x$ is the ideal generated in $A[X]$ by the annihilator 0_a of a in A, then :

THEOREM 3.10. — $0'_a = (0_a)^x$, *in the polynomial ring of a commutative ring A with identity.*

PROOF : 1) If $0_a = (\{b_i\})$, every $p \in (0_a)_x$ has the form $p = \sum b_i p_i$, $p_i \in A[X]$. Then $pa = \sum b_i a p_i = 0$, and $p \in 0'_a$. This shows that $(0_a)^x \subseteq 0'_a$. 2) Let $p \in 0'_a$, then $p = \sum c_i X^i$, hence $ap = 0$ implies $ac_i = 0$ for every i. Therefore $c_i \in 0_a \subseteq A$, and $p \in (0_a)^x$. Thus $0'^a \subseteq (0_a)^x$, and the proof is completed.

THEOREM 3.11. — *If a right-ideal I in* A *is closed, so is the ideal* I^x *generated by* I *in the free extension of* A.

PROOF. — Let I be a right-ideal in A, and suppose it is closed. The right-ideal generated by I is $I^x = \{\sum a_i p_i\}$, $(a_i \in I)$ where the p_i are in the free extension. A polynomial annihilates I^x if and only if it has the form $\sum q_i b_i$ with $b_i \in 0_I^1 \subseteq A$ (left-annihilators). Further, an element of the free extension annihilates them on the right if it can be expressed as $\sum c_i q'_i$ with $c_i \in \bar{I}_r \subseteq$ A. Since $I = \bar{I}$, then, $c_i \in I$, $\sum c_i q'_i \in I^x$, or $\bar{I}_x = I_x$, and I_x is closed.

DEFINITION 3.4. — *We shall say an ideal I is invariant if it is invariant relatively to every extension of* A.

We can study the relations between invariance and closure.

Let I be a right-ideal in A. If an element $b \in A$ is in the right-ideal generated by I in some extension B of A, then there exists a set of elements of I, say $\{a_i\}$, such that $b = \sum a_i q_i$, with $q_i \in B$; hence, by the previous considerations, b is in the closure of $\{a_i\}$. Conversely, if b is in the closure of a finite set $\{a_i\}$, there is an extension B of A in which there exists a set of solutions for the equation $\sum a_i x_i = b$, and b is in the ideal generated by $(\{a_i\})$ in B.

This proves the following:

THEOREM 3.12. — *A necessary and sufficient condition for a given right- (left-) ideal I to be invariant in* A *is that I contain the closure of all its finite subsets.*

Evidently, if I has finite basis, this is equivalent to say that I must be closed.

We can now assert:

COROLLARY 3.5. — *In a complete right- (left-) semifield, every right- (left-) ideal is invariant.*

REMARK. — The following statement, analogous to that of lemma 3.1, generalizes it to the non-commutative case, so that all assertions and considerations there derived are also valid here.

LEMMA 3.5. — *In any associative ring* A, *if an element* b *does not belong to the right- (left-) ideal generated by a finite set of elements* $\{a_i\}$, *then* Xb (*resp.* bX) *does not belong to the two-sided ideal generated by the set* $\{Xa_i\}$ (*resp.* $\{a_iX\}$) *in the free extension* Γ_1 (A) *with one generator* X.

PROOF. — Let us prove it by contradiction, and assume that $Xb \in (\{a_i X\})$. Then Xb has the form

$$Xb = \sum_{i,j} p_{ji}(X) \cdot (Xa_i) \cdot q_{ji}(X),$$

all terms of degree higher than one cancelling mutually on the right, so

$$Xb = \sum_{i,j} p_{ij} X a_i d_{ij}.$$

This says that the sum on the right can be reduced to a single term. In any case, the coefficients on the right of X belong to the right ideal generated by the set $\{a_i\}$, thus $b \in (\{a^i\})$, contradicting the hypothesis.

4. GENERAL EQUATIONS IN COMMUTATIVE RINGS

This section will be devoted to the study of commutative extensions (also identity-preserving) of commutative rings. Generalizations not requiring commutativity will be developed in a later paper.

4.a. Polynomials of minimal degree. We shall say that an ideal I is *solvable* in the polynomial ring $A[X]$ if it satisfies the condition $I \cap A = (0)$. It is evident that, if $p(X)$ is in I, then $p(X) = 0$ is a solvable equation that is,

$$(p(X)) \cap A = (0).$$

Since the polynomials of an ideal have a positive degrec (this ideal need not be solvable), that is since the degree of all polynomials of I are natural integers, there must be in I at least one polynomial whose degree is minimal in this set. This will be called a *polynomial of minimal degree* in I (briefly, a *m-d-polynomial*).

THEOREM 4.1. — *If* $f(X) = \sum_0^n a_i X^i$ *is a m-d-polynomial in an ideal* I, *then* $0_{a_n} \subseteq 0_{a_i}$ *for every* i.

PROOF. — Let c be an element such that $ca_n = 0$ (0 is one such c). Hence, $cf(X)$ has a degree lower that $f(X)$ and is in I. Thus, $f(X)$ being a m-d-polynomial, $cf(X) = 0$, and $ca_i = 0$ for every i.

This condition, which is necessary, is not sufficient, as the following example shows : The ideal $(X - a)$ contains the polynomial

$X^2-2aX+a^2$, which satisfies evidently the conditions of theorem 4.1, but is not an m-d-polynomial in *1*.

But the sufficiency is restricted to the following case:

THEOREM 4.2. — *If* $0_{a_n} \subseteq 0_{a_i}$ *for every* i, *then* $f(X) = \sum_0^n a_i X^i$ *is a m-d-polynomial in* $(f(X))$.

PROOF. — The ideal $(f(X))$ is the set of all $f(X)p(X)$ for every $p(X)$ in $A[X]$. Let us suppose that a product $f(X)p(X)$ is of lower degree than $f(X)$ Then, if $p(X) = \sum_0^m b_j X^j$, $a_n b_m = 0$, and by hypothesis $a_i b_m = 0$. Then the leading term of $f(X)p(X)$ would be $a_n b_{m-1} X^{n+m-1}$, and by similar considerations $a_n b_{m-1} = 0$, implying $a_i b_{m-1} = 0$ for every i, and so on. Therefore, $f(X)p(X) = 0$ and $f(X)$ is a minimal degree polynomial in $(f(X))$.

Following the usual definitions, we shall call *leading coefficient* the coefficient of the term of maximal degree in a polynomial, and a polynomial *monic* if its leading coefficient it the identity 1.

Since the conditions of theorem 4.1 are necessary and sufficient for the solvability of the equations $a_i = a_n x_i$, in a semifield we can find element d_i such that $a_i = a_n d_i$; then, the $f(X)$ above, can be written as $f(X) = \sum_0^n a_n d_i X^i$, with $d_n = 1$. Hence, $f(X) = a_n \sum_0^n d_i X^i = a_n m(X)$, where $m(X)$ represente a monic polynomial, and we have proved

COROLLARY 4.1. — *In a semi-field, every m-d-polynomial is the product of a monic polynomial by a constant.*

There can be more than one m-d-polynomial in an ideal, all them multiple of monic ones. Yet, for complete semi-fields it is true that

COROLLARY 4.2. — *In a complete semi-field, all m-d-polynomials of an ideal I in its polynomial ring, are multiples of a single monic polynomial.*

PROOF. If $p_i(X) = \sum_0^n a_{ji} X^j$ are the m-d-polynomials of I, then, every finite linear combination $\sum_0^m c_i p_i(X) \in I$ is either of the same degree or it is zero. If $\sum_0^m c_i a_{ni} = 0$, then $\sum_0^m c_i p_i(X)$ being of lower degree than n, it is zero, hence $\sum_0^m c_i a_{ji} = 0$ for every j. This is the necessary and sufficient condition, in a complete semi-field, for the linear systems $a_{ji} = x_j a_{ni}$, to have a common solution, that is, for the existence of a set of d_j such that $a_{ji} = d_j a_{ni}$ for every i. Clearly, this is equivalent to our assertion.

For every polynomial ring (over a commutative ring but not necessarily a semi-field) the following theorem is valid :

THEOREM 4.3. — *If a m-d-polynomial* f(X) *of an ideal* I *is monic,* I = (f(X)).

We must prove here that every element of I is a multiple of $f(X)$. Since the leading coefficient of this m-d-polynomial is the identity, the division algorithm can be applied, and the remainder, having degree lower than $f(X)$, must be zero.

The theorem is also true if the leading coefficient of the m-d-polynomial has an inverse (see a.e., Albert [1], p. 24), but in this case, no generalization is introduced, because by multiplying by such an inverse one obtains a monic polynomial of the same degree

The principal ideal generated by a monic polynomial will be called a *monic ideal.*

Since in a complete semi-field, all m-d-polynomials of an ideal are multiples of a (single) monic polynomial of the same degre (hence, if the ideal is solvable the monic polynomial is different from the identity *1*) we might think that every equation could be studied in an extension $A[X]/(m(X))$ for a convenient monic $m(X)$, in other terms, that the monic divisor of all the m-d-polynomials of I generates an ideal $(m(X))$ which contains I. But this is not true, as we can see in the following example :

EXAMPLE : An equation having no monic divisors different from the identity : Let A be a Boolean ring (which is a complete semi-field) with more than two elements and identity, and a an element such that $a \neq 0$, $a \neq 1$. Consider the equation $ax^2 + x + 1 = 0$; we shall see that it is solvable

PROOF: Let $g(X) = \sum_0^n b_i X^i$ be a polynomial such that $f(X)\,g(X) \in A$, with $f(X) = aX^2 + X + 1$ From the se conditions follows : $ab_n = 0$, $ab_{n-1} + b_n = 0$, $ab_{i+2} + b_{i-1} + b_i = 0$ $(n \geqq i \geqq 2)$, $b_0 + b_1 = 0$. From the second equation we have : $a(ab_{n-1} + b_n) = ab_{n-1} + ab_n = 0$, and from the first $ab_{n-1} = 0$, hence $b_n = 0$. By the same reasoning all $b_i\,(i \geqq 1)$ are zero, and by the last condition $b_0 = 0$, hence $g(X) = 0$ and $f(X)\,g(X) = 0$, that is, $(f(X)) \cap A = (0)$ and the equation is solvable. We can see at the same time that $f(X)\,g(X)$ is of lower degree than $f(X)$ if and only if $g(X)$ is a constant polynomial b with $ab = 0$, then $b \,.\, f(X) = bX + b$. In a Boolean ring, $ab = 0$

implies that b is a multiple of $1-a$. The $bX + b$ are precisely the m-d-polynomials of $(f(X))$. All these polynomials are divisible by $X + 1 + c$ with $bc = 0$ for every b. Since the set of the $b's$ contains $1-a$ and every b is a multiple of $1-a$ the conditions $bc=0$ for every b amounts to $c(1 - a) = 0$, that is, to $ca = c$. If $f(X)$ has a monic divisor, the divisor must be also a divisor of every m-d-polynomial of $(f(X))$, hence it must be one of the $X + 1 + c$ just obtained. By the division algorithm, $aX^2 + X + 1 / X + 1 + c$ is uniquely determined for each d, and, as it is easily seen, its reimainder is always equal to a. This proves that $f(X)$ has no monic divisors, hence that $(f(X))$ is not contained in any (solvable) monic ideal, and, a fortiori, that no ideal containing $f(X)$ is contained in a monic ideal.

4. b. Algebraic simple extensions of semi-fields. If B is a simple extension of a semi-field A, we shall say that B is a monic extension if there is a monic ideal I such that $B=A[X]/I$.

If B is a simple extension of a semi-field A, B is isomorphic to a homomorphic image of the polynomial ring $A[X]$, modulo some ideal I. If $I = (0)$ the extension is transcendental, and if $I \neq (0)$, B is an algebraic extension of A. Considering only the polynomials appearing in I, we have proved that every m-d-polynomial is a multiple of (at least) one monic polynomial, which is not necessarily an element of I.

We can consider B as an A-module, and, if the m-d-polynomials of I are of degree n, we can choose a set of n linearly independent elements of B such that the set of these, together with some other element of B, is always dependent.

If $p=\sum_0^n a_iX^i$ is a such m-d-polynomial in I, we will have (writing a for a_n) $p = ap' = a(X^n + \sum_0^{n-1} c_iX^i)$, where $ac_i = a_i$. For every polynomial in $A[X]$, we write : $q(X) = p'(X)s(X) + r(X)$, where $r(X)$ has smaller degree than n.

The set $\{1, X, X^2, \ldots, X^{n-1}\}$ has no linear combination in I, for otherwise, I would have a polynomial of lower degree than n; hence, their images in B are linearly independent.

Let q be an element of B, that is, the image of some $q(X)$ in the polynomial ring. We can write then $aq(X) = ap'(X)s(X) + ar(X)$. But $ar(X)$ is a linear combination of the set $\{X^i\}$ $(0 \leq i \leq n-1)$, and, since $ap'(X) = p(X) \in I$, we have in B: $aq = \sum_0^{n-1} d_iX^i$ (the X^i in B representing the inages of the X^i in $A[X]$). We have proved our assertion.

If B is a monic extension of A, then $a = 1$, and every element of B is a linear combination of X^i's. Furthermore, since the remainder in the division algorithm is unique, this representation is unique. In this case, B is a vector space over A.

We have seen in section 1, that there may be transcendental elements in an algebraic extension of a ring. We wish to prove now that this is not true for semi-fields, that is, that in a simple algebraic extension af a semi-field every element is algebraic.

THEOREM 4.4. — *Every element of a simple algebraic extension* B *of a semi-field* A *is algebraic over* A.

PROOF. — Let A be a semi-field, $A(\theta)$ a simple extension isomorphic with $A[X]/I$ (I a proper ideal in $A[X]$), n the degree of an m-d-polynomial in I, and a the leading coefficient of such polynomial. Hence, we may express the powers of every $\alpha \epsilon A(\theta)$ linearly in terms of the θ^j's :

$$a\alpha^i = a\left(\sum_{j=0}^{n-1} b_{ij}\theta^j\right), \quad 1 \leqq i \leqq n, \tag{1}$$

Let Δ be the determinant $|b_{ij}|$ $(1 \leqq i \leqq n-1;\ 1 \leqq j \leqq n-1)$ and Δ_{ij} the cofactor of b_{ij} in Δ. Then, multiplying the $n-1$ first expressions (1) by Δ_{ij} (with j fixed), and adding :

$$a\sum_{i=1}^{n-1} \Delta_{ij}\alpha^i = a\Delta\theta^j + a\sum_{i=1}^{n-1} \Delta_{ij}b_{i0} \quad (1 \leqq j \leqq n-1). \tag{2}$$

If we multiply the n^{th} identity in (1) by Δ and replace the $\Delta\theta_j$ by their expression obtained from (2), we get :

$$a\Delta\alpha^n - a\sum_{i=1}^{n-1} \Delta_{ij}b_{nj}\alpha^i = a\Delta b_{n0} - a\sum_{i=1}^{n-1} \Delta_{ij}b_{i0}, \tag{3}$$

in which no power of θ appears. If $a\Delta \neq 0$, then (3) is an equation of degree n satisfied by α, hence α is algebraic over A. If $a\Delta = 0$, (2) gives us a set of equations of degree lower than n satisfied by α, unless all $a\Delta_{ij}$ are zero.

The Δ_{ij} are, then, determinants of order $n-2$ obtained from the $n-1$ first expressions (1) by neglecting the colunm b_{i0}.

We consider now the determinants of order $n-2$ of the first $n-2$ equations (1) obtained by omitting one arbitrary column (besides the constants). Let Δ_1 and Δ_2 be two such determinants, and let $b_{i(1)}$ be the elements appearing in Δ_1 and not in Δ_2, and, conversely, $b_{i(2)}$ those appearing in Δ_2 but not in Δ_1. The cofactors (now called Δ_{iz})

of $b_{i(1)}$ in Δ_1 are, up to the sign, respectively equal to the cofactors of $b_{i(2)}$ in Δ_3.

Multiplying each of the firs $n-2$ expressions (1) by Δ_{iz} and adding we have :

$$a \sum_{i=1}^{n-2} \Delta_{iz} \alpha^i = a \sum_{i=1}^{n-2} \Delta_{iz} b_{i0}, \qquad (4)$$

since Δ_1 and Δ_2 are zero by our previons hypothesis.

But here, since we have imposed no restriction on the selection of the columns of $b_{i(1)}$ and $b_{i(2)}$, (4) gives us a set of equations of degree lower than $n-1$ satisfied by α, unless every determinant of order $n-3$ obtained from the $n-2$ first equations (1), is orthogonal to a.

In this case, we consider the first $n-3$ equations of (1) and repeat the operation. If we have some Δ' such that $a\Delta' \neq 0$, then there is an equation in A solved by α. Otherwise, our process continues until to arrive to an equation solved by α, or until all the determinants are of order 1. In the latter case the determinants are the coefficients of the first equation (1), hence $a\alpha = 0$, and α always satisfies an A – equation. The theorem is proved.

Since this theorem is true for simple extensions, a new problem appears : Which are necessary and sufficient conditions for a simple extension of a semi-field to be also a semi-field ?

It is known, under which conditions an extension of a field is a field. It is however easy to prove that every simple extension of a field is a semi-field. It is a particular case of the following theorem.

THEOREM 4.5. — *If* B *is a monic simple extension of a complete semi-field, then* B *is also a complete semi-field.*

If B is a monic extension of a complete semi-field A, θ the image of X in the homomorphism $A[X] \to A[X]/I = B$, and $\sum_{i=0}^{n} m_i X^i$ the monic ($m_n = 1$) basis of I, then, in B :

$$\theta^n = \sum_{k=0}^{n-1} H_k^0 \theta_k, \text{ with } H_k^0 = - m_k \qquad (1)$$

By our previous considerations, every element of B is a linear combination of θ^j's ($0 \leqq j \leqq n-1$), with coefficients in A. In particular, for θ^{n+1} we have the following recurrence formula :

$$\theta^{n+1} = \sum_{k=0}^{n-1} H_k^i \theta^k \text{ with } H_k^i = H_{k-1}^{i-1} + H_{n-1}^{i-1} H_k^0$$

To prove it by induction, notice that if

$$\theta^{n+i-1} = \sum_{k=0}^{n-1} H_k^{i-1}\,\theta^k, \text{ then}$$

$$\theta^{n+i} = (\sum_{k=0}^{n-1} H_k^{i-1}\,\theta^k)\,\theta = H_{n-1}^{i-1}\theta^n + \sum_{k=0}^{n-1} H_{k-1}^{i-1}\,\theta^k,$$

where $H_{k-1}^{j} = 0$ if $k = 0$; now, replacing θ^n by its expression (1)' one has

$$\theta^{n+i} = \sum_{i=0}^{n-1} (H_{k-1}^{i-1} + H_{k-1}^{i-1} H_k^0)\,\theta^k,$$

as we wanted to prove.

We shall now show how to express the product of two arbitrary elements of B as a linear combination of the θ^k's.

Let $\pi = \sum_{t=0}^{n-1} p_t\theta^t$ and $\rho = \sum_{s=0}^{n-1} r_s\theta^s$ be two arbitrary elements in B, then

$$\pi\rho = \sum_{j=0}^{2n-2} (\sum_{t+s=j} p_t r_s)\,\theta^j$$

and replacing the θ^j's ($n \leqq j \leqq 2n-2$) by their expressions in terms of the H_j^i's, we arrive to:

$$\pi\rho = \sum_{k=0}^{n-1} \theta^k\,[\sum_{t=0}^{k} p_t r_{k-t} + \sum_{t=1}^{n-1} p_t\,(\sum_{i=0}^{t-1} H_k^i r_{n+i-t})],$$

or

$$\pi\rho = \sum_{k=0}^{n-1} \theta^k\,[p_0 r_k + \sum_{t=1}^{k} p_t\,(r_{k-t} + \sum_{i=0}^{t-1} H_k^i\, r_{n+1-t}) + \\ + \sum_{t=k+1}^{n-1} p_t\,(\sum_{i=0}^{t-1} H_k^i\, r_{n+i-t})].$$

Remembering that, in general, $n = \sum_{k=0}^{n-1} y_k\theta^k = 0$ implies $y_k = 0$ for every k, we can assert that, if $\alpha = \sum_{k=0}^{n-1} a_k\theta^k$ and $\gamma = \sum_{k=0}^{n-1} c_k\theta^k$, then $\gamma\alpha = 0$ if and only if

$$0 = c_0 a_k + \sum_{t=1}^{k} c_t\,(a_{k-t} + \sum_{i=0}^{t-1} H_k^i a_{n+i-t}) + \sum_{t=k+1}^{n-1} c_t\,(\sum_{i=0}^{t-1} H_k^i\, a_{n+i-t}) \quad (2)$$

for every $k\,(0 \leqq k \leqq n-1)$.

To prove the theorem it is sufficient to show that B is a semi-field. A slight generalization of the proof shows that it is also a complete semi-field.

If $\alpha x = \beta$ is a solvable equation, then, for every γ, $\gamma\alpha = 0$ implies $\gamma\beta = 0$; hence conditions (2) imply similar conditions with the b_r's in place of the a_r's.

In particular, the $(n-1)^{st}$ expression (2) becomes:

$$c_0 b_{n-1} + \sum_{t=1}^{n-1} c_t\,(b_{n-1-t} + \sum_{i=0}^{t-1} H_{n-1}^i\, b_{n+i-t}) = 0. \quad (3)$$

Let C_i^k be the coefficient of c_i in the k^{th} expression (2) and C_i^b the coefficient of c_i in (3). Then the solvability of $\alpha x = \beta$ is equivalent to the solvability of the set

$$C_i^b = \sum_{k=0}^{n-1} C_i^k x_k^{(i)},$$

which, if solvable, must have a common system of solutions X_k, that is,

$$C_i^b = \sum_{k=0}^{n-1} C_i^k x_k$$

We shall now construct a solution for our original solvable equation $\alpha x = \beta$.

If $\delta = \sum_{k=0}^{n-1} d_k \theta^k$ is such a solution, its coefficients d_k must solve the set

$$a_k d_0 + \sum_{t=1}^{k} (a_{k-t} + \sum_{i=0}^{t-1} H_k^i a_{n+i-t})\, d_t + \sum_{t=k+1}^{n-1} (\sum_{i=0}^{t-1} H_k^i a_{n+i-t})\, d_t = b_k.$$

Thus, taking

$$d_{n-1} = X_0 \text{ and } d_{n-t-1} = X_t - \sum_{i=0}^{t-1} H_{n-1}^i\, d_{n+i-1},$$

δ is the solution.

The following counter-example shows that there are simple extensions of a complete semi-field which are not semi-fields.

Let A be a Boolean ring with four elements: 0, a, $b = a+1$, 1, and B the simple extension $B = A[X]/(aX^2 - aX)$. For the element $m(\theta) = \theta^2 + \theta$, and any $q(X) = \sum_{i=0}^{n} c_i x^i$.

$m(X) \cdot q(X) = c_n X^{n+2} + \sum_{i=0}^{n} (c_{i-1} + c_i) X^{i+1}$ belongs to $(aX^2 - aX)$ if $c_n = a$, and, if all c_i are equal to zero or to a, so that, $q(X) \in (a)$ and $q(\theta) \in (a)$ in B. Conversely, for every $r(\theta) \in (a) \subseteq B$, $r(X) \in (a) \subseteq A[X]$, and $m(X)\, r(X) \in (aX^2 - aX)$. Hence $m(\theta) \cdot r(\theta) = 0$, that is, $0_{m(\theta)} = (a)$.

Now, for the element $b \in B$, we have: $bq(X) \in (aX^2 - aX)$ implies $b \cdot q(X) \in (a)$, and, since $b = a+1$, $q(X) \in (a)$. Conversely, for $r(X) \in (a)$, since $ab = 0$, $b \cdot r(X) = 0 \in (aX^2 - aX)$, and $0_b = (a)$.

Hence, $m(\theta) \cdot x = b$ is a solvable equation in B. Moreover for every $s(\theta)$ in B we have in $A[X]$: $s(X) = \sum_{i=0}^{n} s_i X^i$ and

$$m(X) \cdot s(X) = \sum_{i=0}^{n} s_i (X^2 + X), \text{ implying}$$
$$(m(X),\, aX^2 - Xa) \cap A = (0).$$

Hence, no multiple of $m(\theta)$ is different from zero in A, that is $m(\theta) . x = b$ has no solution in B, and B is not a semi-field.

Added in proof. It can be shown that in unrestricted or identity preserving extensions (types *a*) and *b*), section 1*b*) any family of right (left) solvable equations is compatible. Yet, the problem remains of finding out if this is true for commutative extensions for which the theorem of Ricabarra is still valid.

REFERENCES

1. A. A. Albert, *Modern Higher Algebra,* Chicago, 1937.
2. A. A. Albert, *On cyclic algebras,* Annals of Mathematics, 39 (1938) 669-682.
3. G. Birkhoff, *On the structure of abstract algebras,* Proc. Cambridre Phil. Society, 31 (1935) 433-454.
4. R. Brauer, *Theory of rings,* Class notes, Michigan University.
5. B. Brown and N. H. McCoy, *Rings with unit-element which contains a given rings,* Duke Math. Journal 13 (1946) 9-20.
6. M. Cotlar, *Un método de construcción de estructuras...,* Revista Univ. Nac. de Tucumán, serie A, 4 (1944) 105-157.
7. J. L. Dorroh, *Concerning adjunctions to algebras,* Bull. Am. Math, Society, 38 (1932) 85-88.
8. D. O. Ellis & J. W. Gaddum, *On solutions of systems of linear equations in a Boolean algebra,* Bull. Am. Math. Society, Abst. 448 t, 56 (1950) 474.
9. A. Foster, *p^k-rings and ring logics,* Annali Scuola Norm. Sup. Pisa, 5 (1951) 279-300.
10. M. Hall, *Group rings and extensions I,* Annals of Math., 39 (1938) 220-234.
11. M. Hall, *A type of algebraic closure,* Annals of Math., 40 (1939) 360-369.
12. M. Ikeda and T. Nakayama, *On some characteristic properties of quasi-Frobenius and regular rings,* Proc. Amer. Math. Soc., 5 (1954) 15-19.
13. N. H. McCoy, *Remarks on divisors of zero,* Amer. Math. Monthly, 49 (1942) 286-295.
14. N. H. McCoy, *Subdirectly irreducible commutative rings,* Duke Math. Journal, 12 (1945) 381-387.
15. N. H. McCoy, *Concerning matrices with elements in a commutative ring,* Annals of Math., 32 (1931) 463-477.
16. N. H. McCoy and D. Montgomery, *A representation of generalized Boolean rings,* Duke Math. Journal, 3 (1937) 455-459.
17. A. Malcev, *On the inmersion of an algebraic ring into a field,* Math. Annalen, 113 (1936) 686-691.
18. T. Nakayama, *On Frobeniusean algebras,* Annals of Math., 40 (1939) 611-633.
19. T. Nakayama and M. Ikeda, *Supplementary remarks on Frobeniusean algebras,* Osaka Math. Journal, 2 (1950) 7-12.
20. J. von Neumann, *On regular rings,* Proc. Nat. Acad. Sci. U.S.A., 22 (1936) 707-713.

21. O. Ore, *Linear equations in non-commutative fields,* Annals of Math., 32 (1931) 463-477.
22. E. Snapper, *Completely primary rings II,* Annals of Math., 53 (1951) 463-477.
23. O. Teichmueller, *Multiplikation zyclischer Normalringe,* Deutsche Math., 1 (1936) 92-102 und 192-328.
24. O. E. Villamayor, *Sur les équations et les systèmes linéaires dans les anneaux associatifs,* C. R. Acad. Sci. París, 240 (1955) 1681-1683 et 1750-1751.
25. O. E. Villamayor and E. Gentile, *On the homomorphisms and algebraic closure in associative rings* (to appear in this magazine).

Instituto de Matemática
Departamento de Investigaciones Científicas
Universidad Nacional de Cuyo, Mendoza.

ESTE FACSÍCULO

SE TERMINÓ DE IMPRIMIR EL 31 DE OCTUBRE DE 1955

EN LA IMPRENTA Y CASA EDITORA «CONI»

CALLE PERÚ 684, BUENOS AIRES

CONTENIDO

ORLANDO E. VILLAMAYOR, On the theory of unilateral equations in associative rings.