N. C. A. da Costa
A. A. M. Rodrigues

Definability and Invariance

Abstract. In his thesis *Para uma Teoria Geral dos Homomorfismos* (1944), the Portuguese mathematician José Sebastião e Silva constructed an abstract or generalized Galois theory, that is intimately linked to F. Klein's Erlangen Program and that foreshadows some notions and results of today's model theory; an analogous theory was independently worked out by M. Krasner in 1938. In this paper, we present a version of the theory making use of tools which were not at Silva's disposal. At the same time, we tried to keep in mind, so much as possible, the gist of his standpoint.

Keywords: Definability, Invariance, Galois Theory, Generalized Galois Theory, Model Theory.

Contents

Introduction **2**

1 Types, scales and structures **3**

2 Two classes of abstract languages **5**

3 Expressible elements **6**

4 Isomorphism, equivalence and closed sets **11**

5 Logical bases **18**

6 Fundamental theorems **20**

7 Strong isomorphisms and orbits **23**

8 Some results of generalized Galois theory **25**

9 Axiomatic systems **28**

10 Final Remark **29**

References **29**

Presented by **Daniele Mundici**; *Received* April 1, 2006

Studia Logica (2007) 86: 1–30
DOI: 10.1007/s11225-007-9049-6
© Springer 2007

> Das Aufsuchen der Invarianten ist eine schöne, ja sogar die schönste Aufgabe der Mathematik, aber noch mehr, es ist sogar ihre einzige Aufgabe. Und auch damit ist es noch nicht genug: es ist einzige Aufgaben aller Wissenchaften überhaupt.
>
> L. Kronecker

Introduction

In this paper we present the basic ideas and results of a thesis whose author was the Portuguese mathematician José Sebastião e Silva (1914-1972). The thesis was written in Portuguese around 1944, when Silva was in Italy with a scholarship of the *Instituto para a Alta Cultura*, Lisbon, to complete a dissertation for the Doctorate in Portugal; he developed his researches at the *Instituto Nazionale di Alta Matematica*, Rome, getting in touch with several Italian mathematicians, such as F. Enriques, F. Severi and L. Fantappié. The thesis was never published during Silva's life nor submitted for the Doctorate degree; in fact, he wrote another dissertation, inspired by Fantappié's work on functional analysis. The thesis appeared only in 1985 in the first volume of *Obras de José Sebastião e Silva* [12]. However, he published a note in Italian in 1945 [13], summarizing his work. An English version of this note appeared in 1985 ([14]; the introduction, by A. J. Franco de Oliveira, gives an outline of Silva's life and accomplishments).

Silva's thesis is important not only for its originality, but also because it foreshadows various concepts and results of higher-order model theory (see [14]). In addition, in other works Silva made applications of his theory, called today generalized Galois theory, to functional analysis and to the theory of distributions.

Nonetheless, Silva's exposition, in his thesis as well as in his note [13], is neither rigorous nor sufficiently precise by present day standards. One of our aims is to correct its shortcomings; another is to contribute to make historical justice to a relevant subject, although not well-known; finally, the third is to present a reference work on generalized Galois theory, which will surely interest a wide range of persons, for instance in the fields of logic, geometry, algebra and functional analysis.

It deserves to be remarked that, independently of Silva, the Russian-French algebraist Mark Krasner developed an analogous theory (cf., for ex-

ample, [6] and [7]). (In a certain sense, Krasner's theory can be reduced to Silva's.) Similar ideas were considered by Tarski (see his posthumous paper [11]).

One of the basic objectives of the theory is the study of certain connections between two central logico-mathematical notions: that of invariance under a group of transformations and that of definability in an appropriate (abstract) language. From this point of view, generalized Galois theory is related to Klein's Erlangen Program, and constitutes one of its possible extensions. On these notions and their importance Hodges writes that,

> The twenty-three year old Felix Klein in his famous Erlanger Programm (1872) proposed to classify geometries by their automorphisms. He hit on something fundamental here: in a sense, *structure is whatever is preserved by automorphisms*. One consequence—if slogans can have consequences—is that a model-theoretic structure implicity carries with it all the features which are set-theoretically definable in terms of it, since these features are preserved under all automorphisms of the structure.
> There is a rival model-theoretic slogan: *structure is whatever is definable*. Surprisingly, this slogan points in the same direction as the previous one. For example, if we have a field K, we can define the projective plane over K. But precisely because the projective plane is definable from K, any automorphism of K will induce an automorphism of the plane too. Either way, the plane comes with the field; in some abstract sense it is the field, but looked at from an unusual point of view. (Hodges [4], p. 93)

1. Types, scales and structures[1]

The underlying theory of our exposition is ZFC, i.e., Zermelo-Fraenkel system with the axiom of choice. So, the basic language of this paper is that of ZFC; nonetheless, the exposition will be informal, though rigorous (and precise).

The set T of types is the least set satisfying the following conditions:

[1]Silva's use of the term "type" clashes with current usage of it in present-day model theory, so that some other term like "sort" should be used instead in this section. However, here we keep Silva's usage to do justice to him, who employed the term in a sense that was not common in logic even at his time.

1. The symbol i belongs to T;
2. If $a_0, a_1, \ldots, a_{n-1} \in T$, then $\langle a_0, a_1, \ldots, a_{n-1}\rangle \in T$, $1 \leq n < w$, where $\langle a_0, a_1, \ldots, a_{n-1}\rangle$ is the finite sequence of n terms, composed by $a_0, a_1, \ldots, a_{n-1}$.

Given $a \in T$, the order of a, in symbols $\mathrm{ord}(a)$, is defined as follows:

1. $\mathrm{ord}(i) = 0$;
2. $\mathrm{ord}(\langle a_0, a_1, \ldots, a_{n-1}\rangle) = \max\{\mathrm{ord}(a_0), \mathrm{ord}(a_1), \ldots, \mathrm{ord}(a_{n-1})\} + 1$.

Let D be a set; it is then possible to introduce the function t_D or, to simplify the notation, only t, whose domain is T, by means of the clauses:

1. $t(i) = D$;
2. If $a_0, a_1, \ldots, a_{n-1} \in T$, then $t(\langle a_0, a_1, \ldots, a_{n-1}\rangle) = \mathbb{P}(t(a_0) \times t(a_1) \times \cdots \times t(a_{n-1}))$, where $\mathbb{P}$ and $\times$ are the symbols for power-set and for Cartesian product, respectively.

If $a \in T$, then the objects (or elements) of $t(a)$ are said to be of type a. The elements of $t(i)$, which are of type i, are also called individuals.

The function t_D is named a scale based on D. The set $\cup\mathrm{range}\ (t_D)$ is denoted by $\varepsilon(D)$. The objects of $\varepsilon(D)$ having types whose orders are greater than zero are relations of finite rank, in particular unary relations or sets. If $a = \langle a_0, a_1, \ldots, a_{n-1}\rangle$, $1 \leq n < w$, is a type, any relation belonging to $t(a)$ is a relation of degree or rank n. Sometimes we identify t with $\varepsilon(D)$.

A sequence is a function whose domain is an ordinal number, finite or infinite. Here, family has the same meaning as sequence. The sequence $a_0, a_1, \ldots$, whose domain is the ordinal λ, will be written $(a_\iota)_{\iota\in\lambda}$ or a_ι, $\iota \in \lambda$, or, to simplify, a_ι, if the domain is clear by the context.

$\mathbb{P}^{(n)}(D)$ denotes the set $\mathbb{P}(\mathbb{P}(\ldots \mathbb{P}(D)\ldots))$, where the symbol $\mathbb{P}$ appears n times, $1 \leq n < \omega$.

The cardinal k_D associated to the scale $\varepsilon(D)$ is introduced as follows:

$$k_D = \sup\{\overline{D}, \overline{\mathbb{P}(D)}, \overline{\mathbb{P}^{(2)}(D)}, \overline{\mathbb{P}^{(3)}(D)}, \ldots\}.$$

A structure e on the basic set D is an ordered pair of the form

$$e = \langle D, r_\iota\rangle,$$

where r_ι is a sequence of elements of $t(D)$. D is the domain of e and r_ι is the family of its primitive elements (we identify individuals with their unit sets). $\varepsilon(D)$ and k_D are the scale and the cardinal associated with e respectively.

We suppose that the domain of the family r_ι is strictly less than k_D.

The order of a relation is the order of its type. The order of a structure $e = \langle D, r_\iota \rangle$, denoted by $\mathrm{ord}(e)$, is defined as follows: if there is the greatest order of the relations r_ι, then $\mathrm{ord}(e)$ is that greatest order; otherwise, $\mathrm{ord}(e) = \omega$.

The usual mathematical structures can be reduced to structures according to the above definition. Sometimes it is a complex task to make such a reduction, for example in the case of differentiable manifolds, but it is always possible, normally in various alternative ways. In addition, there is no difficulty to develop a theory of structures with several domains of individuals (basic sets), say i_0, i_1, ..., i_{m-1}, $m \in \omega$; however, this is theoretically dispensable since such structures are reducible to the standard structures here defined.

On the other hand, the structures of mathematical practice in which there are relations of infinite degree are interesting, but such structures are also reducible to our standard structures, as it is not difficult to verify. However, in a few passages we employ infinitary relations as obvious abbreviations.

Anyhow, the main results below can be adapted to structures with several basic sets or with relations of infinite degree.

2. Two classes of abstract languages

We shall employ two kinds of language: $L^\omega_{\omega\omega}(R)$ and $L^\omega_{\omega\kappa}(R)$.

$L^\omega_{\omega\omega}(R)$ or simply $L^\omega(R)$ possesses the following primitive symbols:

1. Connectives: $\rightarrow$ (implication), $\wedge$ (conjunction), $\vee$ (disjunction) and $\neg$ (negation); $\leftrightarrow$ (equivalence) is introduced by the common definition.
2. Quantifiers: $\exists$ (there exists) and $\forall$ (for all).
3. For each type a, a denumerably infinite set of variables of this type.
4. For each type a, a family of constants of type a; some families may be empty. All constants form the set R.
5. For each type a, the symbol $=_a$ of equality between elements of type a; usually, we suppress the subscript a.
6. Parentheses.

Russell's description symbols ι is introduced by contextual definition. The notions of term, formula, sentence (formula without free variables), term free for a variable in a formula, etc. are easily defined in the standard way.

$L^{\omega}(R)$ is a language of type theory or of higher-order logic. If R is composed by objects of $\varepsilon(D)$, the scale of $e = \langle D, r_{\iota}\rangle$, then one can cannonically interpret $L^{\omega}(R)$ in $\varepsilon(D)$ and, if R is the range of r_{ι}, also in $e = \langle D, r_{\iota}\rangle$. Therefore, it is clear how to define truth for sentences of $L^{\omega}(R)$, interpreted in $\varepsilon(D)$ or in e.

We shall implicitly suppose that when a formula is described or written, it satisfies the ordinary restrictions imposed by the theory of types.

When a sentence S of $L^{\omega}(\text{range}(r_{\iota}))$ is true in $e = \langle D, r_{\iota}\rangle$, we write

$$e \vDash S.$$

A relation r of type $a = \langle a_0, a_1, \ldots, a_{n-1}\rangle$ of $\varepsilon(D)$ is definable in $e = \langle D, r_{\iota}\rangle$ if there exists a formula $F(x_0, x_1, \ldots, x_{n-1})$ of $L^{\omega}(\text{range}(r_{\iota}))$, whose only free variables are $x_0, x_1, \ldots, x_{n-1}$, of types $a_0, a_1, \ldots, a_{n-1}$ respectively, such that, in the language $L^{\omega}((\text{range}(r_{\iota})) \cup \{r\})$, the formula

$$\forall x_0 \forall x_1 \ldots \forall x_{n-1}(r x_0 x_1 \ldots x_{n-1} \leftrightarrow F(x_0, x_1, \ldots, x_{n-1}))$$

is true in $\varepsilon(D)$.

Let κ be an infinite cardinal greater than ω. $L^{\omega}_{\omega\kappa}(R)$ is a language like $L^{\omega}_{\omega\omega}(R)$ to which we add infinite conjunctions ($\wedge$) and disjunctions ($\vee$) of families of formulas whose domains are ordinals strictly less than κ. In $L^{\omega}_{\omega\kappa}(R)$, any block of quantifiers is finite (i.e., has length less than ω).

Precisely as in the case of $L^{\omega}(R)$, we can interpret $L^{\omega}_{\omega\kappa}(R)$ in a given structure $e = \langle D, r_{\iota}\rangle$, introduce the concept of true sentence, etc. But when we do that, we suppose that $\kappa_D \leq \kappa$, κ_D being the cardinal associated with $e = \langle D, r_{\iota}\rangle$.

Definability in $L^{\omega}(R)$ will here be called *definability in the strict sense*; definability in $L^{\omega}_{\omega\kappa}(R)$ is called *definability in the wide sense* or *determination*.

Let s_{α} be a sequence of elements of $\varepsilon(D)$. It is obvious how to characterize the concept of strict definability (or of determination) of a certain object of $\varepsilon(D)$ in $e = \langle D, r_{\iota}\rangle$, with the help of s_{α} and $L^{\omega}(R)$ (or of $L^{\omega}_{\omega\kappa}(R)$).

It seems worthwhile to remark that the concepts of definability, as presented above, are essentially due to Tarski (see, for instance, [15], chapters VI and X).

3. Expressible elements

We denote by $e = \langle D, r_{\iota}\rangle$ a structure, by $\varepsilon(D)$ its scale, by s an element of $\varepsilon(D)$ and by l_{μ} ($\mu < k_D$) a sequence of objects of $\varepsilon(D)$. Under these

conditions, we define by induction the relation 's is expressible in ℓ_μ in the structure e' through the following clauses, such that, in any case, the application of every clause is under the range of action of finitely many applications of the clauses:

1. s is definable in the strict sense in the structure e to which we added the terms of ℓ_μ as new primitive relations;
2. if s is not an individual, then s is expressible in ℓ_μ in the structure e when every element of s is expressible in ℓ_μ in e;
3. if s is expressible in the sequence b_α of elements of $\varepsilon(D)$ in the structure e and every element of b_α is expressible in ℓ_μ in the structure e, then s is expressible in ℓ_μ in the structure e.

The element s of $\varepsilon(D)$ is expressible in the set S (of elements of $\varepsilon(D)$) in the structure e if s is expressible in a sequence b_α, whose range is S, in e. When it is clear what is the structure we are considering, instead of s is expressible in the sequence b_α (or the set S) in the structure e, we simply write that s is expressible in b_α (or in S).

Now, we pass to the question of establishing the connection that exists between expressibility and definability in the wide sense.

THEOREM 3.1. *In $e = \langle D, r_\iota \rangle$, the object $s \in \varepsilon(D)$ is definable in the wide sense in e with the help of the sequence ℓ_μ of elements of $\varepsilon(D)$ iff s is expressible in e with respect to ℓ_μ.*

PROOF. We note that, if F is a formula which defines s in the wide sense, then we have:

1. any subformula of F contains at most a finite number of free variables;
2. there are in F only finite blocks of contiguous quantifiers;
3. any subformula of F is in the scope of a finite number of logical symbols.

The implication from left to right is proved by induction on the construction of F in $L^{\omega}_{\omega\kappa}(R)$, R containing all primitive relations of the structure and all ℓ_μ. We show that any subformula of F defines in the wide sense a relation which is expressible; in particular, s, defined in the wide sense by F, is expressible.

If F is atomic, then the relation defined by F is expressible, taking into account clause 1 of the characterization of expressibility. If F is a finite propositional combination of formulas already proved to determine objects of $\varepsilon(D)$ which are expressible (and definable), then F defines the object that

is also expressible, by clauses 1 and 3. Similarly, if F is of the form $\exists x G$. Finally, when F is of the form $\bigvee_{j \in J} G_j$, with J infinite, we may suppose that all G_j, $j \in J$, have the same free variables $x_1, x_2, \ldots, x_n$, $n \in \omega$. Each of the already expressible $G_j(x_1, x_2, \ldots, x_n)$ in fact expresses a relation of type $\langle t_1, t_2, \ldots, t_n \rangle$, t_i being the type of x_i, $1 \leq i \leq n$. Therefore, the set of all those relations is expressible by clause 2, and its union is also expressible by clauses 1 and 3.

So, if s is definable in the wide sense by F, then it is expressible.

The implication from right to left is proved by induction on the application of the clauses of the concept of expressibility.

The object s, being expressible by clause 1, is evidently definable in the wide sense by a formula of $L^{\omega}_{\omega\kappa}(R)$. If s is expressible because any of its elements is expressible (and definable), then by considering finite or infinite disjunctions, there obviously exists a formula of $L^{\omega}_{\omega\kappa}(R)$ that defines s. The third clause of notion of expressibility is treated on the basis of a kind of rule of substitution: replacing some or all constant terms of a formula by constant descriptions, the resulting expression is also a formula (the description $\iota x H(x)$ is constant if x is the sole free variable of $H(x)$); thus, if s is expressible and therefore definable in terms of α_i and α_i is expressible and so definable in terms of β_j, s is expressible and clearly definable in terms of β_j. ∎

When s is definable in the wide sense in terms of ℓ_λ, there exists, in an obvious sense, an operator ϕ that expresses s in function of ℓ_λ; we are then allowed to write $s = \phi(\ell_\lambda)$. If ℓ'_λ is another sequence such that, for every λ, the types of ℓ_λ and ℓ'_λ are the same, then ϕ also relates s' to ℓ'_λ, where $s' = \phi(\ell'_\lambda)$.

Language $L^{n}_{\omega\omega}(R)$ (or $L^{n}_{\omega\kappa}(R)$), $1 \leq n < \omega$, is called a language of order n; it contains only types of order $\leq n$ and quantification of variables of types having order $\leq n - 1$. The interpretation of such languages are restricted to structures of order n. Their semantic counterparts are easily developed. $L^{\omega}_{\omega\omega}(R)$ and $L^{\omega}_{\omega\kappa}(R)$ are said to be of order ω.

There exists, associated with $e = \langle D, r_\iota \rangle$ and its scale $\varepsilon(D)$, a first-order structure e' characterized by the following conditions:

1. the domain of e' is $\varepsilon(D)$;
2. in e' there are four kinds of primitive elements:
   2.1 for any type t, the unary relation T_t, formed by the elements of $\varepsilon(D)$ of type t;

2.2 for any type $t = \langle t_0, t_1, \ldots, t_{n-1}\rangle$, $0 < n < \omega$, the $n+1$-ary relation E_t such that, for all $p, v_0, v_1, \ldots, v_{n-1}$ in $\varepsilon(D)$, $E_t\, p\, v_0\, v_1\, \ldots\, v_{n-1}$ is true if $\langle v_0, v_1, \ldots, v_{n-1}\rangle \in p$;

2.3 the relation of equality with its usual meaning;

2.4 the family r_ι, whose range is now formed by individuals of e' (though they have *inicial* types in e).

If R and R' denote the sets of primitive elements of e and e', then the languages $L^\omega_{\omega\kappa}(R)$ and $L^1_{\omega\kappa}(R')$ are interpretable in e and e' in an obvious way. Hence, any sentence of $L^\omega_{\omega\kappa}(R)$ and of $L^1_{\omega\kappa}(R')$ has a definite truth-value.

To each sentence φ of $L^\omega_{\omega\kappa}(R)$ there corresponds a sentence φ^* of $L^1_{\omega\kappa}(R')$ which can be obtained in three steps:

First step: Every variable x_t of φ is univocally replaced by a variable x of $L^1_{\omega\kappa}(R')$ restricted by T_t; distinct variables of φ must be replaced by distinct variables of $L^1_{\omega\kappa}(R')$;

Second step: Afterwards, any subformula of form $p\, v_0\, v_1\, \ldots\, v_{n-1}$ is replaced by $E_t\, p\, v_0\, v_1\, \ldots\, v_{n-1}$, where the type of p is $t = \langle t_0, t_1, \ldots, t_{n-1}\rangle$ and the types of the terms $v_0, v_1, \ldots, v_{n-1}$ are $t_0, t_1, \ldots, t_{n-1}$, respectively;

Third step: Finally, subformulas of form $a \underset{t}{=} b$ are replaced by $a = b \wedge T_t(a) \wedge T_t(b)$.

When the object a of type t of $\varepsilon(D)$ is defined in the wide sense by formula $\varphi(x_t)$ of $L^\omega_{\omega\kappa}(R)$, we have that

$$\forall x_t (x_t \underset{t}{=} a \leftrightarrow \varphi(x_t))$$

is true in e. Therefore, by the construction of $\varphi(a)^*$, a is the only object of the domain of e' that satisfies $\varphi(x)^* \wedge T_t(x)$ in e', and

$$\forall x (x = a \leftrightarrow \varphi(x)^* \wedge T_t(x))$$

is true in e'. In other words, a is definable in the wide sense in e'.

Now, let us consider a sentence ψ of $L^1_{\omega\kappa}(R')$. It is associated with the formula ψ^+ of $L^\omega_{\omega\kappa}(R)$, that is built according to the following procedure:

First step: Every subformula of ψ of form $\forall x A(x)$ $(\exists x A(x))$ is replaced by $\bigwedge\limits_{t\in T} \forall x_t A(x_t)$ $(\bigvee\limits_{t\in T} \exists x_t A(x_t))$, x_t being a variable of type t of $L^\omega_{\omega\kappa}(R)$, and distinct variables of $L^1_{\omega\kappa}(R')$ are replaced by distinct variables of $L^\omega_{\omega\kappa}(R)$. So, any term in the resulting expression has a type;

Second step: If $E_t\, p\, v_0\, v_1 \ldots v_{n-1}$ appears in the expression obtained in the previous step, then there are two cases to consider:

1. $E_t\, p\, v_0\, v_1 \ldots v_{n-1}$ satisfies the restrictions of the type hierarchy: in its place we put $p\, v_0\, v_1 \ldots v_{n-1}$, where t is the type that p has to have according the first step;
2. $E_t\, p\, v_0\, v_1 \ldots v_{n-1}$ does not satisfy such restrictions: we write $\neg\forall y\ (y = y)$ in its place, y being a fixed variable of $L^{\omega}_{\omega\kappa}(R)$;

Third step: Afterwards, any expression of form $T_t(v)$ is replaced by $v = v$ if v is a term of type t, and by $v \neq v$ otherwise;

Fourth step: Accomplished third step, every occurrence of $a = b$ is replaced by formula $a \underset{t}{=} b$ if both a and b are of type t; otherwise, it is replaced by $\neg\forall y(y = y)$.

Then, if an object a of type t is determined in e' by formula $\psi(x)$, a is the sole element of the domain of e' that satisfies $\psi(x)$ and $\psi(a)$ is true in e'. Hence, denoting by $\psi(x_t)^+$ the formula $\psi(a)^+$ in which we substitute x_t for a, the sentence

$$\forall x_t(x_t = a \leftrightarrow \psi(x_t)^+)$$

has to be true in e, taking into account its method of construction. Therefore, a is definable in the wide sense in e.

We have, then, proved the proposition that follows:

THEOREM 3.2. *If $e = \langle D, r_\iota\rangle$ and $a \in \varepsilon(D)$, then a is definable in the wide sense in e if and only if a is definable in the wide sense in e', the first-order structure associated with e.*

The preceding theorem remains valid for expressibility with reference to a sequence (or set); it is important because it shows that definitions in higher-order structures can be reduced to definitions in first-order structures.

REMARK. Any sequence is a function whose domain is a finite or infinite ordinal. In certain situations, where the terms of the sequence belong to a given type and the domain of the structure we are considering is infinite, we define, as usual, relations of infinite degree (infinitary relations) as sets of sequences possessing the same ordinal as their common domain. Since here we may restrict such ordinals, without loss of generality to the case in which they are less than a fixed ordinal strictly less than the cardinal associated to the structure, we may identify these ordinals to objects of determined type of the corresponding scale. Thus, infinitary relations on

objects of the same type are identified to sets of sequences belonging to the scale (the axiom of choice is clearly involved in this process). But we don't need infinite blocks of quantifiers in the languages introduced in this paper. For structures with finite domains, we don't need infinitary relations, at least in this work. Nonetheless, we are free to employ arbitrary sequences of objects when necessary or convenient.

Silva employed in some passages of his work an informal notation susceptible of rigorous formulation. We suppose that our infinitary language of type theory, which we denote by L, is interpreted in a structure $e = \langle D, r_\iota \rangle$. Let $(x_\lambda)_{\lambda \in \mu}$ (or simply x_λ) be a sequence of variables of L, all of the same type (i.e., a syntactical sequence of symbols of L); then, an expression like $\exists x_\lambda \varphi(x_\lambda)$, where $\varphi(x_\lambda)$ is a formula of L, in which the variables x_λ may appear free, abbreviates a formula of L of the following form: $\exists h(\psi(h) \wedge \varphi(h(\lambda)))$, such that:

1. h refers to a sequence of elements of $\varepsilon(D)$, elements of the same type as that of x_λ, satisfying obvious conditions that are expressed by $\psi(h)$ (the domain of h is μ, etc.);
2. $\varphi(h(\lambda))$ is the formula obtained from $\varphi(x_\lambda)$ by the replacement of each occurrence of x_λ by $h(\lambda)$. For example, the expression $\exists y_\lambda(z_\lambda = \iota z \phi_{z_\lambda}(z, y_\lambda) \wedge \rho(y_\lambda))$ means $\exists h[\psi(h) \wedge z_\lambda = \iota z \phi_{z_\lambda}(z, h(\lambda)) \wedge \rho(h(\lambda))]$.

4. Isomorphism, equivalence and closed sets

Let $e = \langle D, r_\iota \rangle$ and $e' = \langle D', r'_\lambda \rangle$ be two similar structures, that is, the ordinals of the sequences r_ι and r'_λ are the same, and the types of the corresponding elements coincide. If h is a bijection of D on D', then h may canonically be extended to $\varepsilon(D)$ and $\varepsilon(D')$. We get this way a new function $\overline{h}$ of $\varepsilon(D)$ onto $\varepsilon(D)$, which is also a bijection. We normally identify $\overline{h}$ to h.

Under these conditions, h is an isomorphism of e on e' if we have, for any r_ι, supposed to be of degree n, $0 < n < \omega$, that

$$r_\iota(x_0, x_1, \ldots, x_{n-1}) \leftrightarrow r'_\iota(h(x_0), h(x_1), \ldots, h(x_{n-1})),$$

for all $x_0, x_1, \ldots, x_{n-1}$ of appropriate types, that is, we have $r'_\iota = h(r_\iota)$, for all r_ι (and r'_ι); in addition, when r_ι is an individual, we have that $h(r_\iota) = r'_\iota$.

In particular, in case that $e = e'$, an isomorphism is called an automorphism. The automorphisms of a structure form a group, in an obvious sense, and this group is the Galois group of the structure.

From now on, the structure $e = \langle D, r_\iota \rangle$ in which r_ι is a finite sequence, say $r_0, r_1, \ldots, r_{n-1}$, will sometimes be written as follows:

$$e = \langle D, r_0, r_1, \ldots, r_{n-1} \rangle.$$

When the Galois group of a structure is only composed by the identity function, the structure is said to be undeformable (or rigid); otherwise, it is deformable (or non rigid). The field of reals, for example, is rigid, while a real vector space is not.

The structures $e = \langle D, r_\iota \rangle$ and $e' = \langle D, r'_\lambda \rangle$ are called equivalent when the primitive relations of each of them are definable in the wide sense in terms of the primitive relations of the other. In this case we write $e \equiv e'$; otherwise, $e \not\equiv e'$.

In order to introduce some well-know geometric structures, that will be used in various examples and counter-examples, P will stand for a set of points, and $Rt(x, y, z)$, $Tr(x, y, z)$ and $Eg(u, v, x, y)$ will represent the relations, defined on P, "x, y and z are colinear", "y is between x and z" and "the distance from u to v is equal to the distance from x to y", respectively. These relations are supposed to have the ordinary properties to characterize the three dimensional structures

$$g = \langle P, Rt, Tr \rangle \quad \text{and} \quad g' = \langle P, Rt, Eg \rangle.$$

which are the real affine space and the ordinary Euclidean space. If we add to g' the distance function d as a new primitive relation, we get the strict Euclidean space

$$g'' = \langle P, Rt, Eg, d \rangle,$$

where the points of a straight line with a fixed unit segment play the role of the real numbers. (In fact, the number of dimensions of g, g' and g'' is here irrelevant.)

Some examples are in order:

1. The automorphisms of a topological space are the homeomorphisms of the space on itself. The Galois groups of g, g' and g'' are the groups of affinities, of similarities and of rigid motions respectively. The structure $\mathcal{N} = \langle N, suc \rangle$, where N is the set of natural numbers and suc is the sucessor operator, is rigid. The field of complex number is deformable.
2. If N is the set of natural numbers and the symbols suc, $<$, $+$, $\times$ and $\circ$ (zero) have their common interpretations, then one has:

$$\langle N, suc \rangle \equiv \langle N, < \rangle \equiv \langle N, +, \circ \rangle \equiv \langle N, \circ, < \rangle$$

and

$$\langle N, x \rangle \not\equiv \langle N, suc \rangle.$$

3. If $\mathbb{R}$ denotes the set of reals and the other symbols have their usual meanings, then

$$\langle \mathbb{R}, +, 1, < \rangle \equiv \langle \mathbb{R}, +, \times, < \rangle \equiv \langle \mathbb{R}, +, \times \rangle \equiv \langle \mathbb{R}, +, \times, <, 1 \rangle$$

and

$$\langle \mathbb{R}, + \rangle \not\equiv \langle \mathbb{R}, +, \times \rangle.$$

4. In the case of the complex number, $\mathbb{C}$, we have:

$$\langle \mathbb{C}, + \rangle \not\equiv \langle \mathbb{C}, \times \rangle \quad \text{and} \quad \langle \mathbb{C}, + \rangle \not\equiv \langle \mathbb{C}, +, \times \rangle$$

5. The structures $\langle \mathbb{C}, +, \times \rangle$, $\langle \mathbb{R}, < \rangle$, $\langle \mathbb{R}, +, < \rangle$ and $\langle \mathbb{R}, \times, < \rangle$ are not rigid.

It is clear that the notion of equivalence between structures can be extended to structures with different domains.

The following proposition is true:

THEOREM 4.1. *Two equivalent structures have isomorphic Galois groups.*

Given structure $e = \langle D, r_\iota \rangle$, it is easy to define the concept of substructure of e, by restricting the relations of e to a subset of D. Anyhow, when some of the relations of e are envisaged as operations (or operators), it is usual to suppose that the substructure is closed under the operations. Analogously, we introduce the concept of extension (or superstructure) of a given structure. If e is isomorphic to a substructure of the structure e', we write $e \leq e'$; $e \approx e'$ means that e is isomorphic to e'. We have: 1) $e \leq e$; 2) $e \leq e'$ and $e' \leq e''$ imply that $e \leq e''$.

THEOREM 4.2. *$e \leq e'$ and $e' \leq e$ does not entail that $e \approx e'$.*

PROOF. It suffices to take into account the structures $e = \langle (0, 1], \leq \rangle$ and $e' = \langle [0, 1), \leq \rangle$, substructures of $\langle \mathbb{R}, \leq \rangle$. In fact, e is isomorphic to a substructure of e' and e' is isomorphic to a substructure of e, but e and e' are not isomorphic. ∎

THEOREM 4.3. *Let us suppose that $e = \langle D, r_\iota \rangle$ and $e' = \langle D, r'_\iota \rangle$ are two similar structures, that s_ι is a sequence of constants such that the type of s_ι is that of r_ι (or of r'_ι) and that R is the range of s_ι in $L^\omega(R)$; thus, $L^\omega(R)$ is canonically interpretable in e and e', and we denote by T_e and $T_{e'}$ the sets of true sentences of $L^\omega(R)$ in e and e' respectively. Then, $e \approx e'$ implies that $T_e = T_{e'}$, but not conversely.*

PROOF. $e \approx e'$ clearly implies that $T_e = T_{e'}$. However, if $l = \langle D, s\rangle$ is a structure whose domain is the set $\mathbb{R}$ of reals and s is a well ordering, then the set of true sentences of $L^w(\{s\})$ in l, T_l, is denumerable. Therefore, there exist structures $l_1 = \langle D, s_1\rangle$ and $l_2 = \langle D, s_2\rangle$, where s_1 and s_2 are well orderings on D, satisfying the conditions that $T_{e_1} = T_{e_2}$ and $l_1 \not\approx l_2$. ■

The converse of the preceding proposition is true if instead of simple type theory an infinitary language $L^{\omega}_{\omega\kappa}(R)$ is employed, containing an appropriate family R of constants.

The following four propositions are trivially true:

THEOREM 4.4. *$\langle D, r_\iota\rangle \approx \langle D, r'_\iota\rangle$ implies that $\langle D, r_\iota\rangle \equiv \langle D, r'_\iota\rangle$, but not conversely.*

THEOREM 4.5. *$e \leq e'$ implies that e' is isomorphic to an extension of e.*

THEOREM 4.6. *There are non isomorphic structures which have the same Galois group.*

THEOREM 4.7. *If e and e' are finite structures, i.e., their domains are finite, then one has: $T_e = T_{e'}$ if and only if $e \approx e'$, in a finitary language.*

A subset K of the domain of $e = \langle D, r_\iota\rangle$ is logically closed or, to simplify, closed, if any element of D that is expressible in terms of the members of K belongs to K. (Analogous definitions apply to subsets of any type.)

If $X \subset D$, then $\widetilde{X}$ denotes the logical closure of X, that is, the intersection of all closed sets that contain X.

The operator $\sim$ has the properties that follow:

$$X \subset \widetilde{X}; \quad X \subset Y \rightarrow \widetilde{X} \subset \widetilde{Y}; \quad \text{and} \quad \widetilde{\widetilde{X}} \subset \widetilde{X},$$

where X and Y are any subsets of D.

Sometimes, we refer to $\widetilde{X}$ as the set generated by X.

THEOREM 4.8. *In $e = \langle D, r_\iota\rangle$, an element d of D is expressible in (the elements of) the set $X \subset D$ iff $d \in \widetilde{X}$.*

THEOREM 4.9. *If X is a subset of D, then X is closed iff $X = \widetilde{X}$.*

EXAMPLES

1. In g, the affine space, the closed sets are the linear (affine) varieties;
2. In g', the logically closed sets are still the linear varieties;

3. In g'', with four noncoplanar fixed points, there is only one closed set, the total space (such structure is rigid);
4. The closed subsets of a field F are subfields of F, but there may exist subfields that are not closed (this happens with $\mathbb{Q}(\sqrt[3]{2})$, where $\mathbb{Q}$ is the field of rationals;
5. If E is a topological space, the logically closed sets are topologically closed, though there may exist topologically closed sets which are not logically closed. The topological closure is contained in the logical closure;
6. In a real vector space, the closed subsets of vectors are the subspaces of the space.

It is possible to extend the notions of expressibility, closure, etc. in such a manner that they can be applied to subsets of $\varepsilon(D)$ containing objects of different types.

It is clear that if $e = \langle D, r_\iota \rangle$ and $e' = \langle D, r'_\theta \rangle$ are such that the extensions of their closure operators to $\varepsilon(D)$ coincide, then $e \equiv e'$.

THEOREM 4.10. *In $e = \langle D, r_\iota \rangle$, the set K of all elements of D which are invariant under the action of a subgroup G of the Galois group of e is closed. However, it may happen that several subgroups of the Galois group give rise to the same closed set of invariant elements.*

PROOF. Supposing that $d \in D$ is definable in the wide sense in terms (of the members) of K, there exists a sequence k_μ of elements of K and a formula $\varphi(x; k_\mu)$ of $L^\omega_{\omega\kappa}(\Sigma)$, where Σ is composed by the elements of r_ι and of k_μ, such that $d = \iota x \varphi(x; k_\mu)$. Therefore, for $\theta \in G$, we get: $\theta d = \iota x \varphi(x; \theta k_\mu)$, and, since $\theta k_\mu = k_\mu$, it follows that $d = \theta d$, and $d \in K$.

Now, let us pay attention to the case of the strict Euclidean space. A straight line l is invariant under the group H of rotations around it, which is a subgroup of the group of rigid motions; but it is then obvious that there are several subgroups of H which have l invariant (i.e., the points of l are invariant). ∎

In $e = \langle D, r_\iota \rangle$, if $Y \subset X \subset D$, a logical basis of X with respect to Y is any set $K \subset X$ such that every element of X is expressible in terms of $K \cup Y$; when $Y = \emptyset$, K is called a logical basis of X. To abbreviate, we may simply say basis of X/Y (X over Y) instead of logical basis of X with respect to Y.

In case that $d \in D$ is expressible in terms of $K \subset D$, there is a formula $\varphi(x; k_\mu)$ of $L^{\omega}_{\omega\kappa}(R \cup K)$ satisfying the condition

$$d = \iota x \varphi(x; k_\mu),$$

where k_μ is a sequence of elements of K.

Then, any automorphism θ of e can be applied to both sides of that equality, and we get

$$\theta d = \iota x \varphi(x; \theta k_\mu).$$

So, the expression $\iota x \varphi(x; k_\mu)$ characterizes an operator whose domain is the set of all sequences θk_μ, for all θ in the Galois group of e.

Examples

1. In $e = \langle \mathbb{R}, \leq \rangle$, where $\leq$ is the ordinary ordering of the real numbers, the set generated by ϕ is ϕ;
2. In Euclidean space, the set generated by two (distinct)points is the line determined by these points; but two distinct points of the two-sided elliptic plane, p and q, may be such that $\widetilde{\{p, q\}} = \{p, q\}$;
3. In the field $\mathbb{R}$, any real number is definable in the wide sense, and the same is true in connection with any of its subsets (therefore $\mathbb{Q}$ is not logically closed in $\mathbb{R}$);
4. In the ordinary three-dimensional affine space, put $K = \{p, q\}$, p and q being two distinct points; if P is the set of all points, then a basis for P/K is any set $\{a_1, a_2\}$ such that the lines $a_1 p$ and $a_2 q$ have no point in common, as well as lines $a_1 q$ and $a_2 p$.

Let $e = \langle D, r_\iota \rangle$ be a structure, X a subset of D and s a first-order relation of degree n, $1 \leq n \leq \omega$. Relations s is called irreducible in X whenever we have:

1. s is expressible in e in terms of X;
2. if s' is another n-adic, first-order relation, expressible in e in terms of X and such that $s \cap s' \neq \varnothing$, then $s \subset s'$. In particular, when $X = \varnothing$, s is said to be irreducible. The empty relation is irreducible.

Clearly, the concept of an irreducible relation (with or without reference to a set) can be extended to relations of any type.

THEOREM 4.11. *In $e = \langle D, r_\iota \rangle$, the predicate (i.e., set) of type $\langle a \rangle$ "to be an object of type a definable in the wide sense in e" is definable in the wide sense in e.*

PROOF. Immediate by the properties of the notion of expressibility, which is equivalent to definability in the wide sense. ∎

THEOREM 4.12. *If $e = \langle D, r_\iota \rangle$ and $d \in D$, then there is an irreducible predicate P such that d satisfies P.*

PROOF. The intersection of all expressible predicates of type $\langle i \rangle$ satisfied by d is the irreducible set to which d belongs. ∎

The above proposition is true for all relations of any type whatever; any such relation belongs to an irreducible set.

EXAMPLES

1. In affine plane, the predicate "x is a polygon" isn't irreducible. However the predicate "x is an ellipse" is irreducible;
2. In strict Euclidean plane "x is a circle" isn't irreducible, but "x is a circle of radius $\sqrt{2}$" is;
3. "x is a conic" is irreducible in the projective plane, although it is not in Euclidean plane; the predicate "$x = 1$" is irreducible in the field of reals;
4. Irreducibility entails expressibility.

The solutions of a relation r of degree n, $1 \leq n < \omega$, are the sequences $\langle a_0, a_1, \ldots, a_{n-1} \rangle$ that satisfy r. If the type of r is $t = \langle t_0, t_1, \ldots, t_{n-1} \rangle$, then the types of $a_0, a_1, \ldots, a_{n-1}$ must be $t_0, t_1, \ldots, t_{n-1}$, respectively.

Given $e = \langle D, r_\iota \rangle$, it is immediate how the restriction (or relativization) of e to a subset K of D can be introduced: it is the structure $e_K = \langle K, r'_\iota \rangle$, where r'_ι is r_ι relativized to K, and so $r'_\iota \in \varepsilon(K)$. We normally suppose that if a relation is an operator (or operation), then it is closed under its relativization.

Let A and B be subsets of D in structure $e = \langle D, r_\iota \rangle$, and θ a bijection of A on B; then,

I) θ is called a weak isomorphism (or w-isomorphism) of A on B iff it preserves all primitive relations of e relativized to A;

II) θ is called a strong isomorphism (or s-isomorphism) of A on B iff it preserves all relations definable in the wide sense in e, relativized to A.

Examples

1. In $\mathbb{R}^3$, envisaged as a topological space, a paraboloid of revolution is s-isomorphic to a plane, though not to a disc (without the border); however, it is w-isomorphic to the disc (that is, homeomorphic to the disc);
2. In the structure $z = \langle \mathbb{Z}, \leq \rangle$, where $\mathbb{Z}$ is the set of rational integers and $\leq$ has its usual meaning, the only irreducible set is $\mathbb{Z}$ and any two finite intervals with the same number of elements are s-isomorphic; but structure $z' = \langle \mathbb{Z}, \leq, \circ \rangle$ is rigid and distinct intervals are never s-isomorphic (or w-isomorphic).

The propositions that follow, easy to prove, generalize and complete the preceding explanation of irreducibility.

Theorem 4.13. *In any structure, an object of type a belongs to one and only one irreducible relation of type $\langle a \rangle$; the set of irreducible relations of any type of order ≥ 1 is never empty.*

Theorem 4.14. *In any structure, a relation of type a is irreducible iff it is the intersection of all expressible relations whose intersections with it are not empty. The irreducible relations of type $\langle a \rangle$ constitute a partition of the objects of type a.*

Theorem 4.15. *In all structures, an expressible relation is the union of a unique set of irreducible relations of its type, and conversely.*

Theorem 4.16. *Two equivalent structures are such that their sets of irreducible relations of any type coincide.*

5. Logical bases

From now on, sets will often be supposed to be well ordered and presented as sequences; so, instead of set A, we shall normally write (a_λ) or simply a_λ, the subscript ranging over an ordinal that is kept implicit. In the case of structures, the domains of sequences are always strictly less than the cardinal associated to it. Moreover, taking into account the final remark of section 3, such sequences belongs to the scale of the structure.

With reference to structures and scales, given a relation r and an infinite sequence a_λ, $r(a_\lambda)$ means that the sequence a_λ, envisaged as an element of the scale, satisfies r. However, we are free to imagine $r(a_\lambda)$ as a relation r

of infinite degree applied to an infinite sequence a_λ of objects of the scale. We sometimes write $r(x_\lambda)$ instead of r.

It is convenient to represent the range of sequence a_λ by $\widehat{a}_\lambda$.

In $e = \langle D, r_\iota \rangle$, let A be a subset of D and B a subset of A. We say that the sequence k_λ of elements of A is a logical basis of A with respect of B, if any member of A is expressible, in e, in terms of k_λ and of elements of B. To abbreviate, we say that k_λ is a logical basis of A/B. If $B = \varnothing$, k_λ is called a logical basis of A. (This is a reformulation of the preceding notion of logical basis of a set.)

For example, if field E is a finite extension of field K, i.e.,

$$E = K[a_0, a_1, \ldots, a_{n-1}],$$

then $a_0, a_1, \ldots, a_{n-1}$ is a finite logical basis of E/K. Another example: in affine three dimensional geometry, a logical basis of $P/\{p, q\}$, where P is the set of all points and p and q are two distinct elements of P, is constituted by two points a_1 and a_2, such that:

1. lines $\overline{a_1 p}$ and $\overline{a_2 q}$ have no point in common;
2. lines $\overline{a_2 p}$ and $\overline{a_1 q}$ also have no point in common.

The concept of logical basis can be extended to any type. It is easily seen that, if A and B are subsets of D, with $B \subset A$, in $e = \langle D, r_\iota \rangle$, one has: under the condition that a_λ is a logical basis of A/B, there exists an irreducible relation $r(x_\lambda)$ in B such that a_λ is a *solution* of $r(x_\lambda)$ or, in other words, we have that $r(a_\lambda)$.

If $A \subset D$ is closed and all solutions of r, just considered, belong to A (i.e., the ranges of these solutions are contained in A), we say that A is a normal extension of B. The set of all s-isomorphism of A that leave invariable the elements of B is called the Galois group of A with respect to B or the Galois group of A/B; r is a Galois resolvent of A with respect to B.

If $e = \langle D, r_\iota \rangle$, then the Galois group of D with respect to the empty set is the Galois group of e already defined. The connection between the above ideas and those of classical Galois theory are clear. On the other hand, the extension of such ideas to higher-order types is immediate.

Examples (in an informal formulation)

1. Let E be the root field of the polynomial $p(x)$, separable and irreducible on the field F; then E is a normal extension of F, and $p(x) = 0$ is a Galois resolvent of E with respect to F;

2. The set of rational integers $\mathbb{Z}$ constitutes a normal extension of $\{-1, 0, 1\}$; a basis of $\mathbb{Z}$ with respect to $\{-1, 0, 1\}$ is $\varnothing$, which is also a Galois resolvent.

6. Fundamental theorems

In this section, we state and prove some of the basic propositions of Galois generalized theory (cf. Silva [12], chapter III).

V and W being two subsets of the domain D of $e = \langle D, r_\iota \rangle$ and a_λ a basis of V/W, we have: for any v in V, there is a formula $\phi_v(x; x_\lambda)$ of $L^{\omega}_{\omega\kappa}(\widehat{r}_\iota \cup \widehat{a}_\lambda)$ whose distinct free variables are x and x_λ, κ being the cardinal associated to $\varepsilon(D)$, such that $v = \iota x \phi_v(x; a_\lambda)$ (this fact is established with the help of the axiom of choice).

From now on we shall employ a compact notation which is self-explanatory.

THEOREM 6.1. *Let us suppose that V and V' are two subsets of the domain of structure $e = \langle D, r_\iota \rangle$, with $V \cap V' = W$, a_λ is a basis of V/W, ρ is the irreducible relation in W of which a_λ is a solution, and θ is a mapping of V on V'. Then, a necessary and sufficient condition for θ to be a s-isomorphism of V on V', that leaves invariant the elements of W, is that, for any $v \in V - W$, $v = \iota x \phi_v(x; a_\lambda)$ entails that $\theta v = \iota x \theta_v(x; b_\lambda)$, where b_λ is a solution of ρ, and that, for $v \in W$, $\iota x \phi_v(x; a_\lambda)$ be the identity mapping.*

PROOF. Since a_λ is a logical basis of V/W, then for every $v \in V$, we have: $v = \iota x \phi_v(x; a_\lambda)$, i.e., v is expressible in terms of $\widehat{a}_\lambda \cup W$. Therefore, θ is a s-isomorphism implies that $\theta v = \theta \iota x \phi_v(x; a_\lambda) = \iota x \phi_v(x; \theta a_\lambda) = \iota x \phi_v(x; b_\lambda)$, where $b_\lambda = \theta a_\lambda$; but b_λ is a solution of ρ because $(\theta\rho)(a_\lambda) \leftrightarrow \rho(\theta a_\lambda) \leftrightarrow \rho(b_\lambda)$, taking into account that ρ is expressible in terms of W in e and that the members of W remain fixed under θ.

Moreover, if $v, u \in V$ and $v \neq u$, we cannot have

$$\iota x \phi_v(x; b_\lambda) = \iota x \phi_u(x; b_\lambda).$$

In effect, otherwise it would follow that

$$\iota x \phi_v(x; \theta a_\lambda) = \iota x \phi_u(x; \theta a_\lambda),$$

hence

$$\iota x \phi_v(x; a_\lambda) = \iota x \phi_u(x; a_\lambda),$$

what is absurd, since the relation

$$\iota x \phi_v(x; x_\lambda) = \iota x \phi_u(x; x_\lambda),$$

expressible in W, would have the solution b_λ, but not a_λ, and ρ would not be an irreducible relation.

Thus, θ is such that it transforms

$$v = \iota x \phi_v(x; a_\lambda)$$

in

$$\theta v = \iota x \phi_v(x; b_\lambda).$$

Conversely, if for every $v \in V$, $v = \iota x \phi_v(x; a_\lambda)$ implies that $\theta v = \iota x \phi_v(x; b_\lambda)$, we shall show that θ is a s-isomorphism from V on V'.

First of all, it is easy to prove that θ is a bijection of V on V'.

Now, we suppose that r is an expressible relation and, to simplify, that it is a first-order relation. If $r(u_1, u_2, \dots)$ is true, where $u_1, u_2, \dots$ belong to V, then $r(\theta u_1, \theta u_2, \dots)$ has to be true in V'. In fact, $r(u_1, u_2, \dots)$ true and $r(\theta u_1, \theta u_2, \dots)$ false would imply that the relation

$$r(\iota x \phi_{u_1}(x; x_\lambda), \iota x \phi_{u_2}(x; x_\lambda), \dots),$$

expressible in W, would be satisfied by a_λ, but not by b_λ, what is impossible because ρ is satisfied by a_λ and b_λ.

The reasoning above can be extended to expressible relations of any type whatever by the application of theorem 3.2 of section 3. ∎

THEOREM 6.2. *Under the conditions of the preceding proposition, if $V = V'$ and all solutions of ρ are formed by elements of V, then every s-isomorphism of V on itself, that leaves invariant the elements of W, constitutes a bijection of V on V', such that, for every $v \in V$, $v = \iota x \phi_v(x; a_\lambda)$ implies that $\theta v = \phi_v(x; b_\lambda)$, b_λ being a solution of ρ, and conversely.*

PROOF. Immediate consequence of the previous theorem. ∎

THEOREM 6.3. *Under the hypotheses of the previous theorem, plus the extra condition that V is logically closed, if θ is a mapping of V in V such that for all $v \in V$, $v = \iota x \phi_v(x; a_\lambda)$ entails that $\theta v = \iota x \phi_v(x; b_\lambda)$, then θ is a s-isomorphism of V on itself.*

PROOF. By hypothesis, V is closed, all the terms of solutions of ρ belong to V and a_λ is a basis of V/W.

Since a_λ is a logical basis, every solution of ρ, say b_λ, is expressible in V in terms of a_λ. We may express this circumstance by writing

$$b_\lambda = \iota x B_{b_\lambda}(x; a_\lambda)$$

But let us put

$$r(x_\lambda) \leftrightarrow \exists y_\lambda (x_\lambda = \iota x B_{b_\lambda}(x, y_\lambda) \wedge \rho(y_\lambda)),$$

where the meaning of the abbreviate symbolism is clear (see remark at the end of section 3).

Relation r is expressible in W and has b_λ as a solution. Hence, ρ being also expressible in W and irreducible, $r(a_\lambda)$ is true and it results that

$$a_\lambda = \iota x B_{b_\lambda}(x; c_\lambda), \tag{1}$$

c_λ being a solution of ρ.

As a_λ is a logical basis, we get that

$$c_\lambda = \iota x \phi_{c_\lambda}(x; a_\lambda) \tag{2}$$

However, (1) and (2) entail that

$$c_\lambda = \iota x \phi_{c_\lambda}(x; \iota x B_{b_\lambda}(x; c_\lambda)) \tag{3}$$

In the expression (3), replacing c_λ by x_λ, we obtain another expression which defines a relation expressible in W, having a solution c_λ, which is also a solution of ρ. Therefore,

$$a_\lambda = \iota x \phi_{c_\lambda}(x; \iota x B_{b_\lambda}(x; a_\lambda)),$$

and, in consequence,

$$a_\lambda = \iota x \phi_{c_\lambda}(x; b_\lambda)$$

what means that b_λ is a logical basis of V/W.

So, if $f \in V$, then

$$f = \iota x F_f(x; b_\lambda),$$

and there exists $v \in V$ such that

$$v = \iota x F_f(x; a_\lambda),$$

because V is closed; thus, we have that

$$\theta v = \theta \iota x F_f(x; a_\lambda) = \iota x F_f(x; \theta a_\lambda) = \iota x F_f(x; b_\lambda) = f$$

and θ is a surjection, in effect a bijection of V on V. ∎

THEOREM 6.4. *In $e = \langle D, r_\iota \rangle$, with $W \subset V \subset D$ and $m \in V$, we have: m is invariant under all s-isomorphisms of V that preserve the elements of W iff m belongs to the logical closure of W. In particular, when W is closed, m is invariant under the s-isomorphisms of V which preserve the elements W iff $m \in W$.*

PROOF. If m belongs to the logical closure of W, then m is expressible in terms of W in e, and so it is invariant under the s-isomorphisms of V that leave fixed the members of W.

Conversely, let us suppose that m is invariant as it is stated in the theorem. Then, we have that $m = \iota x \phi_m(x; a_\lambda)$, a_λ being a basis of V/W. Hence,

$$\exists y_\lambda (m = \iota x \phi_m(x; y_\lambda) \wedge \rho(y_\lambda)),$$

where ρ is the irreducible relation defined in W that is satisfied by a_λ.

But m is invariant under all s-isomorphisms of V which leave fixed the members of W, and so the formula

$$\exists y_\lambda (x = \iota x \phi_m(x; y_\lambda) \wedge \rho(y_\lambda))$$

has one and only one solution in the variable x. In conclusion,

$$m = \iota x \exists y_\lambda (x = \iota x \phi_m(x, y_\lambda) \wedge \rho(y_\lambda)),$$

and so m is expressible in terms of W in the structure e, belonging to the closure of W. ∎

THEOREM 6.5. *Let r_ι be a sequence of elements of a set D and of relations of $\varepsilon(D)$. Then, a necessary and sufficient condition for any relation $r \in \varepsilon(D)$ or individual $d \in D$ to be expressible in terms of r_ι is that r be invariant under the Galois group of $e = \langle D, r_\iota \rangle$.*

PROOF. Immediate consequence of theorem 6.4. ∎

7. Strong isomorphisms and orbits

We have:

THEOREM 7.1. *Let $e = \langle D, r_\iota \rangle$ be a structure, V and V' subsets of D with $V \cap V' = W$, and θ a s-isomorphism between V and V', keeping fixed the elements of W. Then θ can be extended to an automorphism θ' of e that leaves fixed the members of W.*

PROOF. There is a basis a_λ of V/W, whose irreducible relation in W is ρ. On the other hand, there also exists a basis c_β of D/V. In consequence, $c_\beta \oplus a_\lambda$ (notation whose meaning is concatenation: in $c_\beta \oplus a_\lambda$, a_λ follows c_β, the domain of $c_\beta \oplus a_\lambda$ is $\beta + \lambda$, etc.) is a basis of D/W; the irreducible relation corresponding to $c_\beta \oplus a_\lambda$ is $h(x_\beta \oplus x'_\lambda)$.

If $b_\lambda = \theta a_\lambda$, then there is an automorphism θ' which transforms $c_\beta \oplus a_\lambda$ in $c'_\beta \oplus b_\lambda$, $c' \oplus b_\lambda$ being a solution of h; in effect, otherwise the relation $\exists y_\beta h(y_\beta \oplus x_\lambda)$ would be satisfied by a_λ but not by b_λ, what is absurd since $\rho(x_\lambda)$ is irreducible and would have more solutions than $\rho(x_\lambda) \wedge \exists y_\beta h(y_\beta \oplus x_\lambda)$. Hence, θ' transforms $c_\beta \oplus a_\lambda$ in $c'_\beta \oplus b_\lambda$.

However, if we put, for $u \in D - V$,

$$u = \iota x \phi_u(x; c_\beta \oplus a_\lambda)$$

and, for $v \in V$,

$$v = \iota x \phi_v(x; a_\lambda),$$

θ' has the property that

$$\theta' u = \iota x \phi_u(x; c'_\beta \oplus b_\lambda)$$

and

$$\theta' v = \iota x \phi_v(x; b_\lambda).$$

Therefore, θ' is an automorphism of e that extends θ. ∎

As far as the end of this section, we will be talking about a structure $e = \langle D, r_\iota \rangle$.

Two elements x and y of D are G-equivalent, where G is the Galois group of e, if there is $g \in G$ such that $y = gx$. This relation induces a partition in D and its classes of equivalence are the orbits of e.

The next three propositions are easily provable.

THEOREM 7.2. *Every orbit is an invariant set and every invariant set is a union of orbits.*

THEOREM 7.3. *Any irreducible set is a union of orbits.*

THEOREM 7.4. *Any irreducible set is invariant.*

We have already proved that a set is invariant if and only if it is expressible (in e).

THEOREM 7.5. *Orbits and irreducible sets are expressible.*

PROOF. In fact, invariance entails expressibility. ∎

We know that every expressible set is a union of irreducible sets. Then, we obtain the following proposition:

THEOREM 7.6. *Every orbit is a union of irreducible sets.*

PROOF. All orbits are invariant and, in consequence, expressible. Hence, any orbit is a union of irreducible sets. ∎

THEOREM 7.7. *A set is an orbit if and only if it is irreducible.*

PROOF. As we proved, any orbit θ is a union of irreducible sets and any irreducible set I is a union of orbits.

Therefore, if orbit θ were not irreducible, it would be a union of disjoint orbits, since any irreducible set is a union of disjoint orbits, and this would be absurd.

Analogously, I is an orbit. ∎

The propositions of the present section can immediately be generalized to any type whatever, as well as in many other ways.

8. Some results of generalized Galois theory

We shall now outline some fundamental results of generalized Galois theory.

THEOREM 8.1. *In any structure $e = \langle D, r_\iota \rangle$ there exists a finite logical basis of $D/\varnothing$ composed by first-order predicates (sets).*

PROOF. By the axiom of choice, there exists a bijection between D and an ordinal λ (the cardinal of D). But any ordinal can be defined in the wide sense with the help of a finite number of predicates of first-order such as addition and multiplication of ordinals. Hence, every member of λ and, as a consequence, of D, can be defined in the wide sense by the means of a finite number of first-order predicates. ∎

It deserves mention the fact that, with the help of the last proposition, it is possible to give a direct proof of theorem 6.5

THEOREM 8.2. *If G is a group of permutations of set D, then there is a structure $e = \langle D, r_\iota \rangle$, with only one predicate of order 2, whose Galois group is G.*

PROOF. Let $u_1, u_2, \ldots, u_n$ be the finite basis of $D/\varnothing$ constructed in the previous proof. The second-order predicate Q, which is satisfied only by the n-tuples $gu_1, gu_2, \ldots, gu_n$, i.e. $Q(gu_1, gu_2, \ldots, gu_n)$ if and only if $g \in G$, has the property that the Galois group of $e = \langle D, Q\rangle$ is G. ∎

THEOREM 8.3. *Let G be a subgroup of the Galois group of structure $e = \langle D, r_\iota\rangle$; then, there exists a second-order predicate which, joined to the primitive relations of e, transforms e into a structure whose Galois group is G.*

PROOF. Corollary to the preceding theorem. ∎

As far as the end of this section, we will be considering an arbitrary but fixed structure $e = \langle D, r_\iota\rangle$.

If $A \subset D$ is a logically closed set, then there is the group G_A of all automorphisms which leave fixed the members of A, and A is the only closed set in this condition, that is, whose members remain invariable under G. Clearly, G is a subgroup of the Galois group of e.

However, the following statement is not true in the present, general setting: To each subgroup H of the Galois group of e, there corresponds a closed set V, such that the group of automorphisms that leaves invariant the members of V is precisely H.

Counter-example: In strict three-dimensional Euclidean space, let us consider the group Σ of all rotations around a straight line t. Evidently, Σ leaves invariant all points of t, which is closed. But several subgroups of Σ leave the points of t invariable.

W and V being subsets of D, $V\|W$ will denote the group of all s-automorphisms of V which leave fixed the elements of W.

THEOREM 8.4. *If $W \subset V \subset D$ and $\theta \in D\|W$, then $\theta(D\|V)\theta^{-1} = D\|\theta(V)$.*

PROOF. If $g \in D\|V$ and $a \in V$, then we have: $\theta g\theta^{-1}(\theta a) = \theta g(a) = \theta a$.

But, if $h \in D\|\theta(V)$ and $a \in V$, we have that $h\theta(a) = \theta a$ and $\theta^{-1}h\theta(a) = a$, i.e., $\theta^{-1}h\theta \in D\|V$, and $h = \theta g\theta^{-1}$, with $g \in D\|V$. ∎

THEOREM 8.5. *If W and V are closed subsets of D, then V is a normal extension of W iff $D\|V$ is a normal subgroup of $D\|W$.*

PROOF. To begin with, we prove that $D\|V$ is a normal subgroup of $D\|W$ entails that V is a normal extension of W.

Clearly, $W \subset V$, and we denote by ρ the irreducible relation in W that is satisfied by a basis b_λ of V/W, whose terms belong to V. Since V is closed, it is enough to show that any solution c_λ of ρ has all its terms in V. But

there exists $\theta \in D\|W$ such that $c_\lambda = \theta b_\lambda$; hence, for $h \in D\|V$, it follows that $\theta h \theta^{-1}(c_\lambda) = \theta h \theta^{-1}(\theta b_\lambda) = \theta h(b_\lambda) = \theta b_\lambda = c_\lambda$, that is, c_λ is invariant under any member of $D\|V$, and $c_\lambda \in V$. So, V is a normal extension of W.

Now, we prove that if V is a normal extension of W, then $D\|V$ is a normal subgroup of $D\|W$.

Let us suppose that $\theta \in D\|W$ and $h \in D\|V$. Then, any solution of ρ has its range contained in V. So, θ transforms a basis $a_\iota \oplus a'_\lambda$, of B/W, where a_ι is a basis of V/W and a'_λ is a basis of D/V, in a basis of $b_\iota \oplus b'_\lambda$; analogously h transforms b'_λ in c_λ. Then, θ^{-1} transforms $b_\iota \oplus c_\lambda$ in $a_\iota \oplus d_\lambda$, and there is $g \in D\|V$ such that g transforms a'_λ in d_λ. This means that for all $\theta \in D\|W$ and $h \in V\|W$, there is $g \in D\|V$ verifying the condition $\theta^{-1} h \theta = g$.

Similarly, for all $\theta \in D\|W$ and $g \in V\|W$, there is $h \in D\|V$ such that $\theta^{-1} h \theta = g$. ∎

THEOREM 8.6. *If $W \subset V \subset D$ and V is a normal extension of W, then $V\|W$ is isomorphic to the quotient group of $D\|W$ by $D\|V$.*

PROOF. (in outline) According to the previous theorem, $D\|V$ is a normal subgroup of $D\|W$. Then, let a_ι be a basis of D/V and b_λ a basis of V/W; this way, in $D\|W$, $D\|V$ and $V\|W$ there are transformations that operate changes of bases, respectively, as follows: $a_\iota \oplus b_\lambda$ in $a'_\iota \oplus b'_\lambda$, a_ι in a'_ι, and b_λ in b'_λ.

Therefore, the equivalence classes of the quotient group of $D\|W$ by $D\|V$ are composed by transformations that send $a_\iota \oplus b_\lambda$ in $a'_\iota \oplus b'_\lambda$, where a_ι and a'_ι remain fixed in each equivalence class; this fact implies that the quotient group is isomorphic to $V\|W$. ∎

Numerous other propositions could also be proved and various notions generalized. For instance, it is possible to introduce the Galois group of a relation, which possesses interesting properties and to formulate extensions of the theorem of symmetric functions, as well as Lagrange's theorem that, as shown by Silva, can be taken as the foundation of classical Galois theory.

Two remarks have still to be made:

1. by the restriction of the primitive relations of structures to operations, employing a restricted notion of definability and applying standard results of the theory of fields (separability, the primitive element theorem, the theory of polynomial eliminability, Techirnhaus transformation, etc.) we are able to obtain Galois classical theory of algebraic separable extensions of fields;

2. most of the content of this paper can be adapted to cover the case of homomorphisms and endomorphisms.

9. Axiomatic systems

An axiomatic system (mathematical system or, to simplify, system) S is constituted by two parts:

1. a description of a class $\overline{S}$ of structures of the same signature in the language of set theory plus certain extra constants or parameters, the so-called primitive terms of S. If the signature is t_ι, $\iota \in \lambda$, where λ is a fixed ordinal, one of the system's characteristics, the structures belonging to $\overline{S}$ are all of the form $e = \langle D, r_\iota \rangle$, and D and r_ι, $\iota \in \lambda$, are the above mentioned primitive terms of S;
2. a finite or infinite set of sentences of the language $L^{\omega}_{\omega\omega}(\{D\} \cup \widehat{r}_\iota)$, called the axioms of S.

The structures in S are supposed to satisfy the axioms; in other words, the structures are models of the collection of axioms. Normally, λ and the number of axioms are finite.

In order to formulate the axioms, we may employ instead of $L^{\omega}_{\omega\omega}(\{D\} \cup \widehat{r}_\iota)$ the language of set theory with certain parameters, corresponding to the primitive elements, but in this case the axioms have to be invariant under isomorphism, that is, transportable according to the terminology of Bourbaki (see [1]). These two formulations, through higher-order logic and through set theory, are in effect equivalent (cf. [3] and [9]).

The analogy between systems and Bourbaki's species of structures (cf. [1]) is evident, and Bourbaki's treatment of species of structures can be adapted to encompass our systems and conversely. Mathematical systems and species of structures are practically the same thing.

The concept of a mathematical system originates various relevant problems and results. Among the results, we present here only two, stated without proof.

In what follows, we include among the structures any set-theoretic construct composed by two sets, a first set D, and a second set Δ of elements of $\varepsilon(D)$, called primitive elements, even when Δ does not belong to $\varepsilon(D)$. The entire, previous exposition can be adapted to the new version of the notion of structure; in particular, the automorphisms of a structure $u = \langle D, \Delta \rangle$ have to leave invariant Δ, but not necessarily every element of Δ.

In the structure $u = \langle D, \Delta \rangle$, the Galois group of Δ (with reference to u) is the group G of permutations of the primitive elements of u, satisfying

the following condition: if $g \in G$ and s is a sentence of $L^{\omega}_{\omega\omega}(\{D\} \cup \Delta)$, then $g(s)$ is true in u iff s is true in u, where $g(s)$ is obtained from s through the application of g to the primitive constants occurring in s.

We have:

THEOREM 9.1. *Let G and H be the Galois groups of $e = \langle D, range(r_\iota)\rangle$ and of $e' = \langle D, r_\iota\rangle$, respectively. Then H is an invariant subgroup of G and $K \approx G/H$, where K is the Galois group of $range(r_\iota)$ with reference to e.*

The group of a system is the group of permutations of its primitive terms which transform its axioms into new ones, in the sense that the collection of the original axioms is semantically equivalent to the collection of the new ones.

THEOREM 9.2. *Let G be the group of the system S, whose sequence of primitive terms is r_ι, and let $e = \langle D, r_\iota\rangle$ be a model of S; K and H denote the groups of automorphisms of e and of $e' = \langle D, range(r_\iota)\rangle$, respectively, and $G' = H/K$. Under these conditions, $G' \leq G$ and, if S is categorical, i.e., any two models of S are isomorphic, then $G' \approx G$.*

In three-dimensional strict Euclidean geometry, $G' = G$ and $K = H$ is the group of isometries. In real projective three-dimensional space, H is the group of all projectivities and K is the group of homographies; the group $G' = H/K$ is of order two, corresponding to the law of duality.

10. Final Remark

The referee called our attention to the fact that some results of the present paper invoke the question of the relations that seem to exist between Silva's ideas and the current notions of stability theory (see the works of Bouscaren, Marker, Hrushovski and Pillay, listed in the References). The study of such relations might be an interesting venue to pursue, even from the historical point of view.

References

[1] BOURBAKI, N., *Theory of Sets*, London-Ontario: Hermann, Addison Wesley, 1968.

[2] BOUSCAREN, E. (ed.), *Model Theory and Algebraic Geometry: An Introduction to E. Hrushovski's Proof of the Geometric Mordell-Lang Conjecture*, New York, Springer-Verlag, 1998.

[3] DA COSTA, N. C. A. and CHUAQUI, R., 'On Suppes set-theoretical predicates', *Erkenntnis,* 29:95–112, 1988.

[4] Hodges, W., *A Shorter Model Theory*, Cambridge: Cambridge University Press, 1997.
[5] Hrushovski, E., 'The Mordell-Lang conjecture for function fields', *Journal Am. Math. Soc.*, 9:667–690, 1996.
[6] Krasner, M., 'Une généralisation de la notion de corps', *Journal de Math. Pures et Appl.,* 17:367–385, 1938.
[7] Krasner, M., 'Endothéorie de Galois abstraite', *Séminaire Dubreil-Pisot, Alg. et Théorie des Nombres 22*, 6, 1968-69.
[8] Marker, D., *Model Theory: An Introduction*, New York, Springer-Verlag, 2002.
[9] Marshall, M. V. and Chuaqui, R., 'Sentences of type theory: the only sentences preserved under isomorphisms', *Journal of Symb. Logic*, 56:932–948, 1991.
[10] Pillay, A., *An Introduction to Stability Theory*, Oxford, Oxford Sci. Pu., 1983.
[11] Pillay, A., *Geometric Stability Theory*, Oxford, Oxford Sci. Pu., 1996.
[12] Sebastião e Silva, J., 'Para Uma Teoria Geral Dos Homomorfismos (Thesis)', in J. C. Ferreira, J. S. Guerreiro and J. S. Oliveira (eds.), *Obras de José Sebastião e Silva, Volume 1*, Lisbon: Instituto Nacional de Investigação Científica, 1985, pp. 135–339.
[13] Sebastião e Silva, J., 'Sugli automorfismi di un sistema matematico qualunque', *Comm. Pontif. Acad. Sci.*, 9:327–357, 1945.
[14] Sebastião e Silva, J., 'On automorphisms of arbitrary mathematical systems', *History and Philosophy of Logic*, 6:91–116, 1985.
[15] Tarski, A., *Logic, Semantics, Metamathematics*, Indianapolis: Hackett, 1983.
[16] Tarski, A., 'What are logical notions?', *History and Philosophy of Logic*, 7:143–154, 1986.

N. C. A. da Costa
Department of Philosophy
Federal University of Santa Catarina
Florianópolis, SC, Brazil
ncacosta@usp.br

A. A. M. Rodrigues
Institute of Mathematics
University of São Paulo
São Paulo, SP, Brazil
aamrod@terra.com.br