DIVISION OF COMPUTER SCIENCE

Structural Invariance, Structural Definability and the Galois Theory of Elementarily Invariant Structures

J.D. Broido

Technical Report No. 272

January 1997

J.D. Broido (1979)

Structural Invariance, Structural Definability and the Galois Theory of Elementarily Invariant Structures.

Review of fundamental Results

Introduction. *Suppose A and B are two adequately described structures— can we decide whether and how A is interpretable in terms of B?*
The question is itself in need of interpretation, of course. In different contexts, the term *interpretation* admits of different readings, suggesting different kinds of operations between the alleged structures; and even the term *structure*, popular and precise as it may sound, is already used with somewhat divergent senses within the range of Mathematics itself—the very discipline that is supposed to focus on structure *per se*. The use of the term *interpretation* is certainly neither restricted to structures that are models of the same first-order theory, nor even to such as are merely "structures for" the very same minimal set of predicates. As we all know, it is possible to envisage reductive "interpretations"—and Science is full of such—whereby the fundamental individuals and predicates in one structure are *mapped* on totally different types of entities, logically—entities which may be much more complex and derivative within the "interpreting" structure. (*Statistical Thermodynamics*, for instance, can be considered as a prescription for interpreting classical thermodynamic "models" in terms of particles in a mechanical "model" and in terms of sums and averages of some of their mechanical functions).

Regarding interpretations as *mappings*, however, it is incontestable that one must satisfy at least two conditions: *First*, that the basic entities in the interpreted source structure must be mapped on entities which are in some sense *definable* in the interpreting target structure; and, *secondly*, that truths of the interpreted source must remain, under such interpretative mapping, *truths—basic or derivative—* of the interpreting structure. We explore some of the ramifications of these minimal constraints on interpretability for *first order strucures* , as understood by *Model Theory.*

This exploration sets the stage for a different approach to concepts of structure in general, which will nominalistically elucidate such concepts in terms of certain *equivalence relations* between *descriptions.* From the vantage point of interpretability, however, the significant thing about this approach is that the various inter-descriptive equivalence-relations that count for our purposes, can all be understood as different types of *bilateral interpretability.* The weaker our contraints on what constitutes an "interpretation", the more liberal and fuzzy will be our general concepts of structure!

Definability and Invariance in first order structures. Definability is normally understood with respect to theories. Yet since *first-order models* —exemplifying for us the simplest and strictest concept of structure[1]—are defined *for* a given first-order language, it also makes sense to talk of sets of various kinds as being definable or undefinable in a given first order structure. Suppose $\mathbf{L}$ is a first order language for which $\mathfrak{A}$ is a structure, in the sense used in Model Theory. A subset S of $|\mathfrak{A}|^n$ —where $|\mathfrak{A}|$ is *the universe of a first order structure* $\mathfrak{A}$—will be said then to be *definable in* $\mathfrak{A}$, iff when there is a formula $F(x_1,...,x_n)\in\mathbf{L}$ such that $F(a_1,...,a_n)$ is true in $\mathfrak{A}^{|\mathfrak{A}|}$ iff $\langle a_1,...,a_n\rangle \in S$ — where $\mathfrak{A}^{|\mathfrak{A}|}$ is $\mathfrak{A}$ expanded to contain a name a for each $a\in|\mathfrak{A}|$. ($\mathfrak{A}^{|\mathfrak{A}|}$ is sometime denoted by $(\mathfrak{A},x)_{x\in|\mathfrak{A}|}$)[2].

For some first order structures, including all finite first order structures, there is a perfect correspondence between definable sets and *invariant* (set-theoretical) entities.

A set $S \subseteq |\mathfrak{A}|^n$ will be said to be *invariant in* A iff for every *automorphism*, σ, of $\mathfrak{A}$, we have $\sigma S=S$ (assuming always that $\sigma S=\{\sigma x \mid x \in S\}$, for any set S). Now, it is easy to show that any finite structure, A, has the following property

β: *A subset of* $|\mathfrak{A}|^n$ *is definable in* $\mathfrak{A}$ *if and only if it is invariant in* $\mathfrak{A}$.

For *finite* structures β can be easily derived from Beth's Definability Theorem or by other means, more directly and constructively. Yet for structures with a denumerable infinity of elements, β constitutes an extremely powerful constraint. It does *not* hold for many of the best known infinite mathematical structures, such as the Standard Model of Number Theory, the rationals, or field of complex Algebraic Numbers. In the case of the Standard Model of number theory, for instance, every subset of n-tuples of natural numbers is invariant (there are no non-trivial automorphisms), but there are clearly more subsets ($2^{\aleph_0}$) than available definitions ($\aleph_0$ only). With respect to β, in fact, one can prove (see appendix I, §4., later), that

THEOREM A. *A countable structure,* $\mathfrak{A}$, *has the property* β *iff* Theory($\mathfrak{A}$) *is* $\aleph_0$*-categorical.*

The requirement that Invariance and Definability be coextensive therefore restricts us to countable models of *categorical* and properly $\aleph_0$*-categorical* theories, and it can be shown in either of these cases, that for each n there must be only finitely many invariant subsets of n-tuples.

The trouble with β is that it restricts the number of invariants only to what can be "explicated" by finite first order formulae. We can easily see that in $|\mathfrak{A}|$ there are bound to be 2^C unary invariants (including $|\mathfrak{A}|$ and the empty set) where C is the cardinality of the set of all *minimal non-empty invariant subsets of* $|\mathfrak{A}|$. If there are infinitely many such minimal invariants—as is the case in the standard model of number theory—there will be more invariants than available definitions.

This suggests that we should consider weaker constraints than β (but still sufficient for our purposes). Consider the following property, β_{fin}, restricting the equivalence of definability and invariance to finite sets:

β_{fin} : *For any n, a finite subset of* $|\mathfrak{A}|^n$ *is definable in* $\mathfrak{A}$ *iff it is invariant in* $\mathfrak{A}$.

This property is shared by many well-known countable structures, including some that were the main subject of traditional Mathematics—e.g., the Standard Model of The *Natural Numbers*, the *Rational field* and *the field of Algebraic Numbers*, and is exactly the kind of property we need in order to study humanly useful interpretability relations between first order structures. As it turns out (see §5 in appendix I), this property too is closely related to a pure Model Theoretic property of (first order) structures—a property we call *Elementary invariance* :

Elementary Invariance. A structure $\mathfrak{A}$ (for language $\mathbb{L}$) is said to be *elementarily invariant* if and only if its domain is an *invariant* in any *elementary extension* thereof.[3]

There are some recognisable features of first order models that guarantee their elementary invariance. The most useful feature of this kind (a necessary and sufficient criterion) has each individual in the model's domain belonging to some *finite* definable subset. This is tantamount to requiring that *the orbits of individuals be all finite and definable* (*the orbit of an entity*, here, it the set of its images under all of the structure's automorphisms). While trivially satisfied in the case of finite structures, this is not so for an infinite structure.

Galois Theory of Structures. Classical Galois Theory is sometimes upheld as a paradigm of transforming a seemingly intractable problem, in one mathematical framework, into a relatively simple problem in another. The solvability by radicals of Algebraic equations over a given field is transformed by Galois Theory into a decidable question about the structure of certain finite groups. The fundamental mapping behind this miraculous transformation is the one which maps an algebraic structure on the group of those of its automorphisms which leave unmoved the elements of a certain substructure. Although Galois Theory was generalised for other algebraic structures beyond the original fields, it was not usually presented as a paradigmatic solution to interpretability questions. In our work we show, however, that many of the classical percepts and theorems of Galois Theory are naturally applicable to all elementarily invariant structures—with a near perfect analogy in the case of those structures with finitely many symmetries. Thus, the generalised Galois Theory will apply in particular to *interpretability relations* between *any finite structures*, and provide for *decidability* in principle.

Such a Galois theory is fundamentally predicated on *relative* notions of definability and invariance (in the original theory the terms used were quite different!). Given a substructure $\mathfrak{A}_0$, of $\mathfrak{A}$, one may ask which entities in $\mathfrak{A}$ are definable by means of the individuals in $|\mathfrak{A}_0|$—using them in addition to the structural predicates and functions. In the same vein one may talk of *Invariance-relative-to-*$\mathfrak{A}_0$, by which is meant invariance under all those automorphisms which leave *every* individual in $\mathfrak{A}_0$ *unmoved* [such automorphisms constitute a subgroup $G(\mathfrak{A}/\mathfrak{A}_0)$ of the group $G(\mathfrak{A})$ of all automorphisms of $\mathfrak{A}$]. As an example of a close analogue of a classical Galois theorem consider the following

THEOREM (see appendix I, §6, theorems **D** and **E**): *Let* $\mathfrak{A}$ *be any Elementarily Invariant Structure and let* $\mathfrak{A}_0$ *be an invariant substructure thereof, with corresponding subgroup* $G(\mathfrak{A}/\mathfrak{A}_0)$ of finite order r. *Then* (1) $G(\mathfrak{A}/\mathfrak{A}_0)$ *is a normal subgroup of* $G(\mathfrak{A})$; (2) $\mathfrak{A}_0$ *will be functionally closed in* $\mathfrak{A}$ [i.e., $|\mathfrak{A}_0|$ includes any $\mathfrak{A}_0$-definable singleton in $\mathfrak{A}$] *if and only if* $|\mathfrak{A}_0|$ *is the set of all elements in* $\mathfrak{A}$ *unmoved by* $G(\mathfrak{A}/\mathfrak{A}_0)$ [in which case one can call $\mathfrak{A}_0$ a *Galois substructure* of $\mathfrak{A}$]; (3) *if* $G(\mathfrak{A}/\mathfrak{A}_0)$ *is finite then there is a finite subset* $S \subseteq |\mathfrak{A}|$, *with* K *elements, where* $0 \leq K \leq \log_2 r$, *and where* $\mathfrak{A}$ *is the functional closure of* $|\mathfrak{A}_0| \cup S$; *and* (4) $\mathfrak{A}$ *can be viewed as the "splitting" structure over* $\mathfrak{A}_0$ *for some monadic formula in* $S_1(\mathbb{L}(\mathfrak{A}))$ *with a finite number* N *of solutions* [i.e., $\mathfrak{A}$ is functionally generated by these solutions over $|\mathfrak{A}_0|$], *where* $N \leq r\log_2 r$. (r can be actually chosen as the maximal order of commutative subgroups of $G(\mathfrak{A}/\mathfrak{A}_0)$).

Interpretability. The last theorem only illustrates the degree to which a general Galois theory of Elementarily Invariant structures mimics the classical theory for Algebraic extensions, a significant portion of which it includes. It does not tell us how we are to use such tools to decide on the existence of interpretability-mappings between structures—especially when we allow such transformations to map basic individuals onto *complex* entities, constructed by means of the host-structural language and the normal set-theoretic aparatus.

Here again the direction is pointed out by the classical theory: Just as we can understand classical Galois Theory to be dealing with the existence of a monomorphic embedding from a given field into what is obtained by repeated radical-extensions, so can we reduce the problem of interpreting one structure in an extension of another to the existence of a suitable monomorphic embedding of one structure in some *set-theoretic extension* of another—for which we can generate *necessary and sufficient group theoretic criteria.* However, we know how to do this, in general, only for injections of *finite* structures in set-theoretic extensions of *elementarily invariant* host structures.

To have the flavour of such results, we introduce a few definitions and notations:
Let $\mathbf{C}_{set}(\mathfrak{A})$ denote the union of $|\mathfrak{A}|$ with the class of all sets *constructible* (by normal set-theoretic operations) from the structure $\mathfrak{A}$ [Set Theoretically this means starting with the sets $\{|\mathfrak{A}|,...,\mathfrak{R}^{n_i}_i,...\}$—where $\mathfrak{R}^{n_i}_i$ models in $\mathfrak{A}$ the n-ary predicate-symbol $\mathbf{R}_i$—and repeatedly applying the set-construction tools provided by standard ZF set theory]. We extend the original $\mathbf{L}$ to $\mathbf{L}_{set}$, to include the symbols of set membership ('$\in$'), and of set-formation ('{','}' and '|'). A *finite entity* in $\mathbf{C}_{set}(\mathfrak{A})$ is constructed, starting with the elements of $|\mathfrak{A}|$ at stage 0, by forming only finite sets of finite entities, at each set-theoretic stage, using only a finite number of stages, but never using $\emptyset$. Excluding $\emptyset$, the ST-type of such an entity will be defined here as the set of ST-types of its members, where the ST-type of individuals in $\mathfrak{A}$ is set to 0. The ST-type of any subset ($\neq\emptyset$) of $|\mathfrak{A}|$ is $\{0\}$, while a subset ($\neq\emptyset$) of $|\mathfrak{A}|\times|\mathfrak{A}|$ will be of ST-type $\{\{0,\{0\}\}\}=\{<0,0>\}$.

We expect of any interpretation $\psi\lceil\mathfrak{A}\rightarrow\mathfrak{B}$ ($\psi:\mathfrak{A}\rightarrow\mathbf{C}_{set}(\mathfrak{B})$) that the individuals of $\mathfrak{A}$ should be mapped on entities in which are all of the same (arbitrary) ST-type τ, and that any definable subset of the ST-type$\{<0^{\leftarrow},.^{n}.\ .^{\rightarrow},0>\}$ should be then mapped *onto* an entity in $\mathbf{C}_{set}(\mathfrak{B})$ of type $\{<\tau^{\leftarrow},.^{n}.\ .^{\rightarrow},\tau>\}$. The definitions of $\mathfrak{A}$-*Invariance* and $\mathfrak{A}$-*Definability* of entities in $\mathbf{C}_{set}(\mathfrak{A})$ are obvious generalisations of our previous definitions [the only difference being that we allow for formulae in $\mathbf{L}_{set}$ to serve in definitions]. It is easy to show that if β_{fin} is true of $\mathfrak{A}$ then every *finite* invariant entity (in $\mathfrak{A}$) is definable (in $\mathfrak{A}$) by a formula in $\mathbf{L}_{set}$. We now define a *strong interpretation* $\psi\lceil\mathfrak{A}\rightarrow\mathfrak{B}$ to be an interpretation $\psi:\mathfrak{A}\rightarrow\mathbf{C}_{set}(\mathfrak{B})$, which satisfies—in addition to preserving relative type differences—the following conditions:
(1) ψ *restricted to* $|\mathfrak{A}|$ *is an injection (monomorphism) into a set of definable entities of* $\mathbf{C}_{set}(\mathfrak{B})$, *all of same ST-type* $\{\tau\}$; (2) *If* $X\in\mathbf{C}_{set}(\mathfrak{A})-|\mathfrak{A}|$, *then* $\psi X=\{\psi w \mid w\in X\}$; *and*
(3) *If* R *is any predicate symbol in* $\mathbf{L}$ *then* $\psi\mathfrak{R}_{\mathfrak{A}}$ *is definable in* $\mathfrak{B}$.
(We may take $\psi\mathfrak{R}_{\mathfrak{A}}$ or its definition to be the "interpretation" of R in $\mathfrak{B}$).

A simple example of an interpretability result is the following

THEOREM (see §7, theorem 7.G). *When* $\mathfrak{B}$ *is elementarily invariant* and $\mathfrak{A}$ *is finite, A necessary and sufficient condition for an injection* $\psi:\mathfrak{A}\rightarrow\mathfrak{B}$ *to constitute a strong interpretation* (of $\mathfrak{A}$ in $\mathfrak{B}$) *is*

$$\psi^{-1} \otimes G(\mathfrak{B}|_{\psi|\mathfrak{A}|}) \otimes \psi \subseteq G(\mathfrak{A}) ,$$

('$\mathfrak{B}|_{\psi|A|}$' stands for the substructure of $\mathfrak{B}$ determined by $\psi|\mathfrak{A}|$, and '$\otimes$' signifies composition.)
An equivalent formulation of this condition is that $\psi \otimes G(\mathfrak{A}) \otimes \psi^{-1}$ *must contain a subgroup isomorphic to the quotient group* $G(\mathfrak{B})/\ G(\mathfrak{B}/\psi(|\mathfrak{A}|))$ [where, of course, $G(\mathfrak{B}/\psi(|\mathfrak{A}|))$ must be a *normal subgroup* of $G(\mathfrak{B})$].

This is directly proved on the basis of the following instructive
Lemma (see 7.1 in §7): *When* $\mathfrak{B}$ *is elementarily invariant and* $\mathfrak{A}$ *is finite, an injection* ψ *will constitute a strong interpretation* of $\mathfrak{A}$ *in* $\mathfrak{B}$ **iff**

for any $\vec{a} \in |\mathfrak{A}|^n$ $(n\geq 1)$, $\psi(\text{orbit}(\vec{a}))$ is an invariant of $G(\mathfrak{B})$.

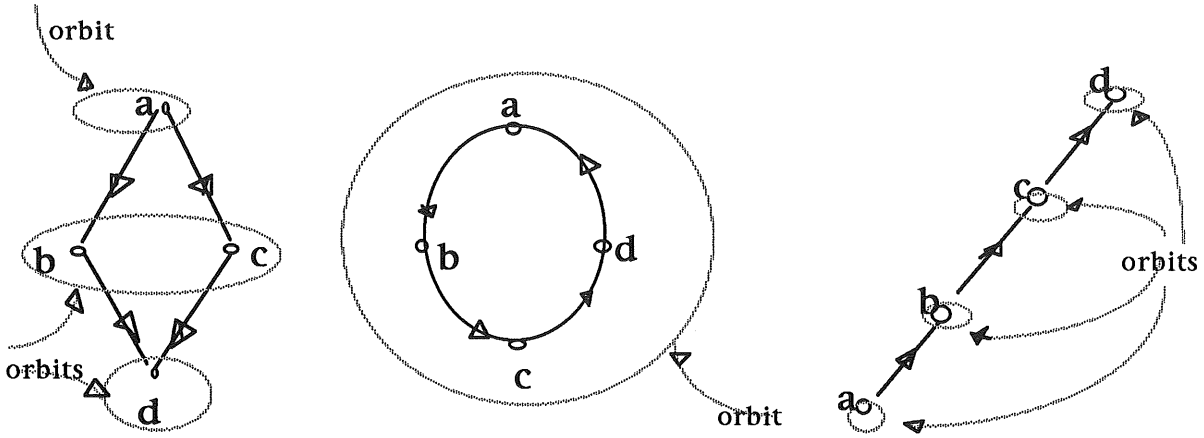
Although injections are very particular and rigid kinds of strong interpretations, they are useful in studying the more general type (this, in fact, is the gist of using Galois Theory as a paradigm for studying interpretations). Any strong interpretation can be conceived as an injection into a *derived structure* of the original host (interpreting) structure—where a derived structure of $\mathfrak{A}$ is defined as the structure we obtain by considering, for some ST-type τ, only those finitary entities that can be constructed out of type τ entities in $\mathbf{C}_{set}(\mathfrak{A})$.

Structural Information Theory. How much information does a structure $\mathfrak{A}$ provide about one of its individuals or, more generally, about any particular element, **e**, in $\mathbf{C}_{set}(\mathfrak{A})$?
Define the *minimal neighbourhood of* **e** *relative to* $\mathfrak{A}$, as the smallest invariant set in $\mathfrak{A}$ containing **e**, (or *the orbit of* **e**). It is obvious that this minimal neighbourhood, $S_{\mathfrak{A}}(\mathbf{e})$, contains only elements of the same type as **e**, and that in the case of a basic individual of the structure it is none other than its classical *orbit*. If **e** is of type τ and $\mathbf{m}$ is a measure on the subsets of $\mathfrak{A}^{\tau} = \{x \mid x \in \mathbf{C}_{set}(\mathfrak{A}) \ \&\ \text{type}(x)=\tau\}$, then the specific information provided by $\mathfrak{A}$ about **e**, $\text{Inf}_{\mathfrak{A}}(\mathbf{e})$, will be an appropriate function of $\mathbf{m}(S_{\mathfrak{A}}(\mathbf{e}))/\ \mathbf{m}(\mathfrak{A}^{\tau})$. If $\mathfrak{A}$ is finite we can take $\mathbf{m}$ to be the *cardinality-function* for any finite subset of $\mathfrak{A}^{\tau}$, and we can choose

$$\text{Inf}_{\mathfrak{A}}(\mathbf{e}) = -\log_N(\text{cardinality}(S_{\mathfrak{A}}(\mathbf{e}))/N), \text{ where } N=\text{cardinality of } \mathfrak{A}^{\tau}.$$

To be of general semiotic utility, such a concept needs to be elaborated further for the case of a complex structure providing more information than necessary for complete individuation of an entity within its type-set (category). Nonetheless, we can still deal with the information per entity, in the above sense, by dealing first with the information contributed by different "aspects" of the structure (per different fragments of the structural language)—inasmuch as these are separable. However, we will not dwell here on this feature of the general theory of structural interpretation, and restrict ourselves to illustrating the new concept of information in the simplest cases.

Thus, In the case of the following three structures



Δ Δ_1 Δ_2

where the arrows represent a binary relation, we have, in Δ, $Inf_{\Delta}(a)=1$,$Inf_{\Delta}(b)=0.5$, $Inf_{\Delta}(c)=0.5$, $Inf_{\Delta}(d)=1$, and an average information per individual (type 0), $I^0(\Delta)$, of 0.75. In Δ_1 on the other hand we have $Inf_{\Delta_1}(x)=0$ for any *individual* x (so $I^0(\Delta_1)=0$).
The picture is different for *orderd pairs*, however! In Δ_1 , for example, we have

$$Inf_{\Delta_1}(<x,y>)= -\log_{16}(4/16)=0.5 \quad (\text{or } I^{<0,0>}(\Delta_1)=0.5).$$

Finally, in the *linear* structure Δ_2 we have $Inf_{\Delta_2}(e)=1$, for e of any type !

Internal Informability vs. Metaphorical Suggestiveness. While such measures of the Semantic Information contained in a structural description give us a handle on the structure's capacity to encode specific information (about whatever is described when one uses it), they do not reflect the true relative value of various structures in their general use! We may have other reasons to use a specific structure, which far out-weigh its lesser *"Internal Informability"*. Culturally and Scientifically we gravitate towards structures that have for us a high *metaphorical suggestiveness*—the potential to serve as a metaphorical vehicle in describing and representing many different types of data and phenomena. While some of the reasons for such a metaphorical value are historical and cultural, others are certainly grounded in the nature of the structures themselves. The Intrinsic "Metaphorical" qualities of a structure have to do with its intrinsic *simplicity* and *symmetricity*, since it is a higher value of these, according to our Galois analysis, which will be positively correlated with a greater chance of successfully serving an *interpretative role* vis à vis new, empirically provided, structural descriptions.

It is easy to see that when "universes" of the same nominal size are organised by different structures , *Internal Informability* and *Metaphorical Power* are *inversely correlated*, and a decision may have to be made as to how much specific Information should be sacrificed for the sake of simplicity of description and of analogy to structured descriptions of other data. *This balancing act between Information and Metaphorical power is at the heart of both Science and Art.* The above tools allow us to develop precise measures of the intuitive *cost-effectiveness* of such multi-faceted activities, which integrate various *explanatory desiderata*, in Science, and which correspond to vital aspects of intuitive evaluation of metaphors in the Arts.

Appendix I: GALOIS THEORY OF ELEMENTARILY INVARIANT STRUCTURES.

1. **Definitions and Preliminaries.** In the foregoing we shall consider only first order languages *with equality*, with no more than $\aleph_0$ non-logical symbols (including individual names). Since we are interested here only in countable structures, it can be assumed, unless stated otherwise, that all structures to which we refer are such (finite or $\aleph_0$).

Let $\mathfrak{A}$ be a structure for language $\mathbf{L}$, and let D be a subset—possibly empty—of $|\mathfrak{A}|$, the universe of $\mathfrak{A}$. '$\mathbf{L}(D)$' denotes the language $\mathbf{L}$ extended to contain, for each $e \in D$, a name e. '$\mathfrak{A}^D$' will denote the structure $\mathfrak{A}$ considered as a structure for $\mathbf{L}(D)$. If 'R' is a non-logical symbol in $\mathbf{L}$, then '$R_{\mathfrak{A}}$' will denote its extension in $\mathfrak{A}$. An *automorphism* of $\mathfrak{A}$ is a bijective mapping, β, from $|\mathfrak{A}|$ to $|\mathfrak{A}|$ satisfying $\beta R_{\mathfrak{A}}=R_{\mathfrak{A}}$, for every non-logical symbol R in $\mathbf{L}$. The Group of all such automorphisms is denoted by '$\mathbf{G}(\mathfrak{A})$'. The subgroup of all automorphisms for which every member of a subset D, of $|\mathfrak{A}|$, is a fixed point (unmoved), is denoted by '$\mathbf{G}(\mathfrak{A}/D)$'. If $\mathfrak{B}$ is a substructure of $\mathfrak{A}$ then '$\mathbf{G}(\mathfrak{A}/\mathfrak{B})$' will mean the same as '$\mathbf{G}(\mathfrak{A}/|\mathfrak{B}|)$'. Note that $\mathbf{G}(\mathfrak{A}/\varnothing)=\mathbf{G}(\mathfrak{A})$. Let $\{z_i \mid i<\omega\}$ be a countable sequence of individual variables $\mathbf{L}$, and let $S_n(\mathbf{L}')$ be the set of all formulae in a language $\mathbf{L}' \supseteq \mathbf{L}$ in which any free variable belongs to the initial finite sequence $<z_1,...,z_n>$. A set $S \subseteq |\mathfrak{A}|^n$ is called D-*invariant in* or *invariant with respect to* D iff $\beta S=S$ for every β in $\mathbf{G}(\mathfrak{A}/D)$. A set $S \subseteq |\mathfrak{A}|^n$ is D-*definable in* $\mathfrak{A}$, or *definable with respect to* D *in* $\mathfrak{A}$ iff there if a formula $\Phi(z_1,...,z_n)$ in $S_n(\mathbf{L}(D))$, such that

$$\mathfrak{A}^D \models \Phi(a_1,...,a_n) \quad \text{iff} \quad <a_1,...,a_n> \in S$$

[We usually write loosely '$\mathfrak{A} \models \Phi(a_1,...,a_n)$' instead of the proper '$\mathfrak{A}^D \models \Phi(a_1,...,a_n)$'].

Let $\mathbf{G}^*$ be any subgroup of $\mathbf{G}(\mathfrak{A})$. Define $K_{\mathfrak{A}}^{(n)}\mathbf{G}^*$ as the set of all n-tuples of $|\mathfrak{A}|^n$, that are unmoved by any element of G'. (Note that $\sigma<a_1,...,a_n>=_{Def}<\sigma a_1,...,\sigma a_n>$). A subset of $|\mathfrak{A}|^n$ is called *invariant* in (or relative to) $\mathfrak{A}$ iff it is $\varnothing$-invariant in $\mathfrak{A}$. It is called *definable* in $\mathfrak{A}$ iff it is $\varnothing$-definable in $\mathfrak{A}$. We abbreviate ' $K_{\mathfrak{A}}^{(1)}\mathbf{G}^*$ as ' $K_{\mathfrak{A}}\mathbf{G}^*$. Note that $K_{\mathfrak{A}}^{(n)}\mathbf{G}^* = (K_{\mathfrak{A}}\mathbf{G}^*)^n$.

An individual $a \in |\mathfrak{A}|$ is *functionally definable in* $\mathfrak{A}$ with respect to D iff the singleton {a} is D-definable in $\mathfrak{A}$. The *functional closure of* D ($\subseteq |\mathfrak{A}|$) *in* $\mathfrak{A}$ is the the set of all elements in $|\mathfrak{A}|$ which are functionally definable in $\mathfrak{A}$ with respect to D. Denote this by '$Cf_{\mathfrak{A}}(D)$'. D is called functionally closed iff $D=Cf_{\mathfrak{A}}(D)$, and it is called a *Galois sub-domain* iff $D=K_{\mathfrak{A}}\mathbf{G}(\mathfrak{A}/D)$, i.e, iff every element of $|\mathfrak{A}|$-D is moved by some automorphism which keeps all elements of D unmoved. A substructure is *Galois* iff its domain (universe) is a Galois sub-domain. We shall say that $\mathfrak{B}$ *is a Galois extension of* $\mathfrak{A}$ iff $\mathfrak{A}$ is an invariant Galois substructure of $\mathfrak{B}$.

The following are elementary lemmas concerning the above concepts:

Lemma 1.1. $Cf_{\mathfrak{A}}(Cf_{\mathfrak{A}}(D))=Cf_{\mathfrak{A}}(D)$

Lemma 1.2. $Cf_{\mathfrak{A}}(D_1 \cup Cf_{\mathfrak{A}}(D_2))=Cf_{\mathfrak{A}}(D_1 \cup D_2)$.

Lemma 1.3. *A Galois sub-domain is functionally closed.*
(The converse for Elementarily Invariant structures—lemma 6.2—is proved later)

Lemma 1.4. *If* $D_0 \subseteq D \subseteq |\mathfrak{A}|$ *and* D *is* D_0*-invariant in* $\mathfrak{A}$*, then* $G(\mathfrak{A}/D)$ *is a normal subgroup of* $G(\mathfrak{A}/D_0)$.
corollary: $G(\mathfrak{A}/D)$ *is a normal subgroup of* $G(\mathfrak{A})$ *for an invariant* D.

Lemma 1.5. *If* D *is a Galois sub-domain of* $|\mathfrak{A}|$ *and* $G(\mathfrak{A}/D)$ *is a normal subgroup of* $G(\mathfrak{A})$*, then* D *is invariant.*

Notation: we use ' $G_1 <| G_2$ ' to say that G_1 is a normal subgroup of G_2 .

Proofs of Lemmas. 1.1 and 1.2 are left to the reader. For 1.3, it is enough to notice that if any element of $|\mathfrak{A}|$ is functionally definable with respect to D, then it will be unmoved by any automorphism of $G(\mathfrak{A}/D)$. Hence $D \subseteq Cf_{\mathfrak{A}}(D) \subseteq K_{\mathfrak{A}} G(\mathfrak{A}/D)$ and if D is a Galois subdomain we will have $K_{\mathfrak{A}}\ G(\mathfrak{A}/D)=D$, and therefore $Cf_{\mathfrak{A}}(D)=D$.
For Lemma 1.4, note that if $G(\mathfrak{A}/D)$ is not a normal subgroup of $G(\mathfrak{A}/D_0)$, then there must exist automorphisms $\sigma \in G(\mathfrak{A}/D_0)$ and $\mu \in G(\mathfrak{A}/D)$ such that $\sigma^{-1}\mu\sigma \notin G(\mathfrak{A}/D)$. Hence there would be $b \in D$ for which $\sigma^{-1}\mu\sigma(b) \neq b$, which implies $\mu\sigma(b) \neq \sigma b$, entailing that $\sigma b \notin D$ or, since $\sigma \in G(\mathfrak{A}/D_0)$, that D could not be a D_0-invariant.
For Lemma 1.5, suppose D were not an invariant. Then there must be a $\sigma \in G(\mathfrak{A})$, such that $\sigma D \neq D$. We can assume then that for some $b \in D$, $\sigma b \notin D$ (note that if $\sigma D \subset D$, we'll have $D \subset \sigma^{-1}D$ and we could choose σ^{-1} instead of σ). Since D is assumed to be a Galois sub-domain, σb must be movable by some $\mu \in G(\mathfrak{A}/D)$, i.e, $\mu\sigma(b) \neq \sigma b$ or $\sigma^{-1}\mu\sigma(b) \neq b$, for some $b \in D$, implying $\sigma^{-1}\mu\sigma \notin G(\mathfrak{A}/D)$ — contrary to the assumed normality of $G(\mathfrak{A}/D)$.

2. Beth's Theorem And Related Results. Let $\mathfrak{A}$ and $\mathfrak{B}$ be structures for L, and suppose ' R' is an n-place predicate symbol of L. An R-*isomorphism* from $\mathfrak{A}$ to $\mathfrak{B}$ is a bijective mapping $\beta: \mathfrak{A} \to \mathfrak{B}$, satisfying $\langle a_1,...,a_n\rangle \in R_{\mathfrak{A}}$ iff $\langle \beta a_1,...,\beta a_n\rangle \in R_{\mathfrak{B}}$ (for a function symbol 'f' the condition is $f(\beta a_1,...,\beta a_n)= \beta f(a_1,...,a_n)$, as usual). If Π is a set of non-logical predicate or function symbols of L, then a Π -isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$ is a bijective mapping $\beta: \mathfrak{A} \to \mathfrak{B}$, which is an R-isomorphism for every $R \in \Pi$.
One way to state Beth's Definability theorem is the following (see [Shoenfield, *Mathematical Logic*, p. 81]) :

BETH'S DEFINABILITY THEOREM. *Let* Π *be a set of non-logical predicate or function symbols of* L, *and let* P *be such a symbol which is not in* Π . *Then a necessary and sufficient condition for* P *to be definable in (or with respect to) a theory* T *in terms of* Π *alone*— i.e, for having $T\vdash P\leftrightarrow\phi$, where ϕ is a formula of L using only members of Π as non-logical symbols — *is that every* Π *-isomorphism between* T*-models is also a* P*-isomorphism..* [note: One can restrict the T-models considered here to countable ones].

There are several ways to prove Beth's theorem, one of which proceeds from Craig's famous *Interpolation Lemma* (see [Shoenfield, *Mathematical Logic,* pp. 79-80], or [Chang and Keisler, Model Theory, pp. 84-88]). Using the same Lemma and a few other basic results of Model Theory one can prove from Beth's Definability theorem above a similar result concerning the notion of *disjunctive definability*. If, as before, Π is a set of non-logical predicate or function symbols of L, and P is such a symbol which is not in Π, say that P is *disjuctively definable in (or with respect to)* T i*n terms of* Π iff there are finitely many formulae $\phi_1,...,\phi_n$, all of whose non-logical symbols belong to Π, such that $T\vdash (P\leftrightarrow\phi_1)^C \vee \ldots \vee (P\leftrightarrow\phi_n)^C$, where $'(f)^C'$ stands for the (universal) closure of f . One can then prove (see [Shoenfield, *Mathematical Logic,* p98, **14, a and b**] or cf. [Chang and Keissler, Model Theory, p.251]):

DISJUNCTIVE DEFINABILITY THEOREM (**Svenonius**). P *is disjunctively definable in* T *in terms of* Π *iff every* Π*–automorphism of any (countable) model of* T *is also a* P*- automorphism thereof.*
In the proof of this theorem, as well as in proofs to follow, the following Model Theoretic result is extremely useful:
Extending Automorphism Lemma. *Let* α *be a bijective mapping between two subsets* S_1 *and* S_2 *of* $|\mathfrak{A}|$, *which is a* Π*-isomorphism between them. Then there is an elementary extension* $\mathfrak{B}$ *of* $\mathfrak{A}$, *and a automorphism* β *of* $\mathfrak{B}$ *extending* α (i.e, $\alpha=\beta|_{S_1}$). —see [Shoenfield, *Mathematical Logic,* p.98, **13, d**]).

3. **Minimal Invariants and n-types.** If S is a subset of $|\mathfrak{A}|^n$ which is an invariant in $\mathfrak{A}$, We shall say that it is an *n-ary invariant*. A minimal n-ary invariant is one that does not contain any other non-empty n-ary invariant. For any $<a_1,...,a_n>\in|\mathfrak{A}|^n$ the set $\{<\sigma a_1,...,\sigma a_n> \mid \sigma\in G(\mathfrak{A})\}$ is obviously such a minimal invariant—also known as *the orbit of* $<a_1,...,a_n>$. Likewise, if S is a minimal (n-ary) invariant, $S=\text{orbit}(<a_1,...,a_n>)$, for any $<a_1,...,a_n>\in S$. Furthermore, we have
Lemma 3.1. *In a minimal invariant,* S, *any two members are related by automorphism*— i.e, for any $\vec{a}$ and $\vec{b}$ in S, $\sigma\vec{a}=\vec{b}$, for some $\sigma\in G(\mathfrak{A})$.
For otherwise the orbits of unrelated members would be smaller invariant subsets of S.

Definition. Given a structure $\mathfrak{A}$ for L, the *type* (in $\mathfrak{A}$) *of* $<a_1,...,a_n>\in|\mathfrak{A}|^n$ is the set of all formulae in $S_n(L)$ that are satisfied at $<a_1,...,a_n>$ for the interpretation (or substitution) $v(z_i)=a_i$. An n-type of $\mathfrak{A}$ is the type of some n-tuple in $|\mathfrak{A}|^n$, and an *n-type in (or of) a theory* T is an n-type in some model of T. An n-type, Γ, in T, is called *principal* if there is a formula in it that T-entails every formula therein.

The following are three trivial consequences concerning invariants and types:

Lemma 3.2. *Different minimal invariants are disjoint.*
[Notice that the elements of a minimal invariant must be all of the same set-theoretic type, even if we extend our approach to set-theoretic constructs based on $|\mathfrak{A}|$.]

Lemma 3.3. *Every n-ary invariant is a unique union of minimal invariants and every union-set of a set of minimal invariants is itself a unique invariant.*
[This, in fact, is true even of invariants of a mixed set-theoretic sort]

Lemma 3.4. *All the members of a minimal n-ary invariant share the same n-type.*
[This follows from lemma 3.1].

We can therefore talk without ambiguity of *the n-type of* S, when S is an n-ary minimal invariant. We now have

Lemma 3.5. *A minimal (n-ary) invariant in* $\mathfrak{A}$ (structure for $\mathbb{L}$) *is definable in* $\mathfrak{A}$ *only if its n-type is principal in* Th($\mathfrak{A}$)—the theory made of all formulae of $\mathbb{L}$ that are valid in $\mathfrak{A}$.
Proof. Let S be such a minimal invariant and let Φ be a defining formula (for S), so that $\mathfrak{A}^{\{a_1,...,a_n\}} \models \Phi(a_1,...,a_n)$ iff $<a_1,...,a_n> \in S$. Then clearly $\Phi \in$ n-type(S). Let Ψ be any other formula of n-type(S); then $\mathfrak{A} \models \Phi(x_1,...,x_n)$ implies that $<x_1,...,x_n> \in S$, which implies $\mathfrak{A} \models \Psi(x_1,...,x_n)$. Thus $\mathfrak{A} \models \Phi(x_1,...,x_n) \rightarrow \Psi(x_1,...,x_n)$ and Th($\mathfrak{A}$) $\vdash \Phi \rightarrow \Psi$.

The converse does not always hold, but it does for *homogeneous* structures.

Definition. A structure is *homogeneous* iff for any n, and any two n-tuples $<a_1,...,a_n>$ and $<b_1,...,b_n>$ the have the same n-type, there is an automorphism mapping $<a_1,...,a_n>$ on $<b_1,...,b_n>$.

Lemma 3.6. *An Elementarily Invariant structure is homogeneous.*
Proof: A bijective mapping γ between two subsets S_1 and S_2 of $\mathfrak{A}$ is called an *isomorphism of* S_1 *and* S_2 in $\mathfrak{A}$ iff for any formula Ψ of $\mathbb{L}(S_1)$, Ψ holds in $\mathfrak{A}$ ($\mathfrak{A}^{S_1}$) iff Ψ^γ holds in $\mathfrak{A}$ ($\mathfrak{A}^{S_2}$)— where Ψ^γ is obtained from Ψ by replacing a by the name of γ(a) for every $a \in S_1$ occuring in Ψ. We now use the extending automorphism lemma of §2 above, which implies that such isomorphism is extendible to an automorphism δ of an elementary extension, $\mathfrak{B}$, of $\mathfrak{A}$.
If $\mathfrak{A}$ is elementarily invariant, however, then $\delta|\mathfrak{A}| = |\mathfrak{A}|$, and $\delta|_{\mathfrak{A}}$ — δ restricted to $\mathfrak{A}$ — must be an automorphism of $\mathfrak{A}$ extending γ. If n-type($<a_1,...,a_n>$)=n-type($<b_1,...,b_n>$) then the mapping $\gamma: \{a_1,...,a_n\} \rightarrow \{b_1,...,b_n\}$ defined by $\gamma(a_i) = b_i$ ($i \leq n$) constitutes an isomorphism of $\{a_1,...,a_n\}$ and $\{b_1,...,b_n\}$ that can be extended to an automorphism of $\mathfrak{A}$. $\mathfrak{A}$ is therefore homogeneous.

We now prove the modified converse of 3.5.

Lemma 3.7. *If, in a homogeneous structure $\mathfrak{A}$, a minimal invariant S has a principal n-type in* Th($\mathfrak{A}$), *then* S *is definable in* $\mathfrak{A}$.

Proof: Let Γ=n-type(S), and suppose $\exists\Phi\in\Gamma$ such that Th($\mathfrak{A}$) $\vdash \Phi\rightarrow\Psi$ for all $\Psi\in\Gamma$. Clearly Φ is satisfied at any member of S. On the other hand, if any n-tuple $\langle x_1,...,x_n\rangle \in |\mathfrak{A}|^n$ satisfies Φ, it must have an n-type including all the Th($\mathfrak{A}$)-consequences of Φ, and therefore identical to Γ (no n-type can properly include another). Since $\mathfrak{A}$ is homogeneous, the identity of n-types implies that such $\langle x_1,...,x_n\rangle$ is related to any member of S by some global automorphism (of $\mathfrak{A}$). The invariance of S under any such automorphism, however, implies then that $\langle x_1,...,x_n\rangle$ must belongs to S (or we would have some automorphism moving an element of S outside S).

The last argument in the above proof shows in addition that we also have the *Corollary*. For a homogeneous structure, $\mathfrak{A}$, there is, for any n, a 1-1 correspondence between n-types and minimal n-ary invariants and, furthermore, minimal n-ary invariants are definable iff they have principal n-types in Th($\mathfrak{A}$).

4. **Structures that satisfy β** . We now deal with infinite countable structures in which every invariant set is definable and show that they are exactly the infinite countable structures whose complete theory is $\aleph_0$-categorical—i.e, those countable structures *to whom a countable structure can be elementarily equivalent only if it is isomorphic* .
All finite structures (whose complete theory, in a language with equality, is necessarily categorical) can be proved directly to satisfy β (see remarks at the beginning of §5 below). An $\aleph_0$-categorical theory, T (in a countable $\mathbb{L}$) that has only infinite models, is *complete* by the Łoś-Vaught theorem, if it is consistent; whereas by Ryll-Nardjewski's Theorem it can have only principal n-types, and only finitely many of them, for each n. Furthermore, by the same theorem, either of these last two properties guarantees $\aleph_0$-categoricity of a complete and consistent T with no finite models. (cf. [Shoenfield, *Mathematical Logic,* pp.89-91]). Concerning $\aleph_0$-categoricity, we shall use the following model theoretic results (where any theory is presumed an $\aleph_0$-theory) :

Lemma 4.1. *A countable model of an $\aleph_0$-categorical* T, *with no finite models, is saturated.*
Proof: Let $\mathbb{C}$ be a countable model of such a theory, T. To show that it is *saturated*, we have to show that for any n-type Γ in T which contains the type of $\langle a_1,...,a_{n-1}\rangle \in |\mathbb{C}|^{n-1}$, there is an a_n in $|\mathbb{C}|$ such that $\langle a_1,...,a_{n-1},a_n\rangle$ has Γ as an n-type in $\mathbb{C}$.
Since every type of a countable theory is realised in some countable model thereof (by the completeness theorem), they must be all realised in $\mathbb{C}$, because all other countable models are isomorphic to it ($\aleph_0$-categoricity). From the above comments we also know that T is complete and that every n-type in it is principal (i.e, generated by some formula in $S_n(\mathbb{L})$). In particular, it follows that the existential closure any formula of $\mathbb{L}$ that is satisfied in some countable model of T must be a theorem of T. Let $\gamma(z_1,...,z_n)$ and $\delta(z_1,...,z_{n-1})$ be the generating formulae, respectively, of Γ and of the (n-1)-type of $\langle a_1,...,a_{n-1}\rangle$. From the assumptions above we have that

$T \vdash \gamma(z_1,..,z_{n-1},z_n) \rightarrow \delta(z_1,...,z_{n-1})$, which implies by Logic that
$T \vdash \neg\delta(z_1,...,z_{n-1}) \rightarrow \neg(\exists x)\gamma(z_1,...,z_{n-1},x)$.
On the other hand, if we suppose that $(\exists x)\gamma(a_1,...,a_{n-1},x)$ is not satisfied in $\mathbb{C}$, then the formula $\neg(\exists x)\gamma(z_1,...,z_{n-1},x)$ belongs to the type of $<a_1,...,a_{n-1}>$ and is implied in T by its generator, $\delta(z_1,...,z_{n-1})$. Being T-entailed by both δ and $\neg\delta$, $\neg(\exists x)\gamma(z_1,...,z_{n-1},x)$ becomes a theorem of T, contradicting the fact that $\gamma(z_1,...,z_{n-1},z_n)$ belongs to an n-type Γ of T and must be satisfied at some n-tuple $<a'_1,...,a'_{n-1},a'_n>$ in $\mathbb{C}$ (and any other countable model)—which implies, by the completeness of T, that $T \vdash (\exists z_1)...(\exists z_{n-1})(\exists z_n)\ \gamma(z_1,...,z_{n-1},z_n)$.
We can thus conclude (by negation) that $(\exists x)\gamma(a_1,...,a_{n-1},x)$ is satisfied in $\mathbb{C}$, and we can select a_n as any value in $|\mathbb{C}|$ satisfying the existential quantifier. Since $\gamma(z_1,...,z_n)$ is the generating formula of Γ, Γ will be included in the n-type of $<a_1,...,a_{n-1},a_n>$ after such a selection and must therefore be identical to it .

Lemma 4.2. *Let $\mathfrak{A}$ and $\mathfrak{B}$ be two countable saturated models of complete theory* T *having only infinite models, and let* $<a_1,..,a_n> \in |\mathfrak{A}|^n$ *and* $<b_1,..,b_n> \in |\mathfrak{B}|^n$ *have the same type. Then there is an isomorphism* γ *from* $\mathfrak{A}$ *to* $\mathfrak{B}$ *which maps* $<a_1,..,a_n>$ *on* $<b_1,..,b_n>$. (i.e, for every i, $\gamma(a_i)= b_i$).
The proof of this lemma follows the same type of reasoning as employed in proving Ryll-Nardjewski's theorem, beginning with the "isomorphism" of $<a_1,..,a_n>$ and $<b_1,..,b_n>$, but using here the property of saturation at each stage to add a new $a \in |\mathfrak{A}|$ and a new $b \in |\mathfrak{B}|$ in order to extend the previously "constructed" partial isomorphism . One can define this process in such manner that every member of $|\mathfrak{A}|$ and $|\mathfrak{B}|$ will be selected (for details see [Shoenfield, *Mathematical Logic,* pp.91-92, 26,b, in pp. 102-103].

Lemma 4.3. *A countable model of an* $\aleph_0$*-categorical* T *having no finite model is homogeneous.*
This follows from the previous two lemmas. By Lemma 4.1 such a model ,$\mathfrak{A}$, must be saturated. Apply lemma 4.2 then to the reflexive case of $\mathfrak{A}$ and $\mathfrak{A}$ to obtain an automorphism of $\mathfrak{A}$ extending any initial correspondence between two n-tuples in $\mathfrak{A}$ that share the same type.

THEOREM A. *For an infinite countable structure $\mathfrak{A}$, invariance is equivalent to definability if and only if* Th($\mathfrak{A}$) *is* $\aleph_0$*-categorical .*

Proof: Assuming first that Th($\mathfrak{A}$) is $\aleph_0$-categorical , it follows from the last lemma that $\mathfrak{A}$ is homogeneous. This, together with the fact that any type in Th($\mathfrak{A}$) is principal, will imply by Lemma 3.7 that any minimal invariant in $\mathfrak{A}$ is definable. Since different minimal n-ary invariants have different n-types (corollary of 3.7), it will follow from Ryll Nardjewski's theorem that there are only a finite number of minimal n-ary invariants, for each n. Thus every n-ary invariant must be a finite union of minimal n-ary invariants, which are definable, and must therefore be itself definable by a disjunction of the defining formulae for its minimal constituents.
To prove *the converse,* assume *every* invariant in $\mathfrak{A}$ to be definable. This implies that

there are only *finitely many* minimal n-ary invariants for each n, or else we would obtain, by lemma 3.3 , $2^{\aleph_0}$ distinct n-ary invariants, in general, requiring $2^{\aleph_0}$ distinct definitions). Thus there are only finitely many n-ary invariants, in general, for each n (exactly $2^{C(n)}$ such, including $\varnothing$ and $|\mathfrak{A}|^n$, where C(n) is the number of minimal n-ary invariants).
Let $\mathfrak{B}$ be any model of Th($\mathfrak{A}$); we prove that any type in it is *principal*. Let Γ be an n-type in $\mathfrak{B}$, and let $\{\gamma_1,\gamma_2,\dots\}$ be any enumeration of its formulae. Define $\delta_1=\gamma_1$, ...,$\delta_{n+1}=\gamma_{n+1}\&\delta_n$,..., etc; clearly each δ_i belongs to Γ, and each δ_i implies all the previous ones. Since $(\exists z_1)...(\exists z_n)\ \delta_i(z_1,...,z_n)$ is valid in $\mathfrak{B}$ it must be in Th($\mathfrak{A}$) and must be valid in $\mathfrak{A}$. Let $S(\delta_i)$, for evey natural index i, be the subset of $|\mathfrak{A}|^n$ *defined* by $\delta_i(z_1,...,z_n)$. No such subset can be empty, and every such subset (since definable) is an n-ary invariant. Since there are only finitely many n-ary invariants in $\mathfrak{A}$, there must be some natural number, say k_0, such that $S(\delta_i)= S(\delta_{k_0})$, for infinitely many values of i. We claim that δ_{k_0} generates Γ in Th($\mathfrak{A}$), for if we take any γ_i in the the first enumeration of its formulae, there will always be some (in fact, infinitely many) $k\geq i$, such that $S(\delta_k)= S(\delta_{k_0})$. The last equality implies $\mathfrak{A} \models \delta_k\leftrightarrow\delta_{k_0}$, which implies Th($\mathfrak{A}$) $\vdash\!\!\!-$ $\delta_k\leftrightarrow\delta_{k_0}$. But, since $k\geq i$, we have both $\vdash\!\!\!-$ $\delta_k\rightarrow\delta_i$ and $\vdash\!\!\!-$ $\delta_i\rightarrow\gamma_i$, and therefore Th($\mathfrak{A}$) $\vdash\!\!\!-$ $\delta_{k_0}\rightarrow\gamma_i$.

It thus follows that every type in Th($\mathfrak{A}$) is principal (since we placed no restriction on $\mathfrak{B}$, save its being a model of Th($\mathfrak{A}$)), and therefore, by Ryll-Nardjewski's theorem, that Th($\mathfrak{A}$) is $\aleph_0$-categorical ■.

Corollary. T is $\aleph_0$-categorical iff T is complete and satisfies β in all its countable models .

Theorem A demonstrates the power of the unrestricted equivalence of structural invariance and structural definability, for (countable) theories that have infinite models.

5. **Elementarily Invariant Structures and the β_{fin} Property.** We shall now study the structures that satisfy β_{fin}—the equivalence of definability and invariance *for finite subsets only*. We shall first show that elementarily invariant structures ("EI structures", for short) satisfy this property. From this it will follow in particular that all finite structures must satisfy β.
We start with the intuitively obvious but important observations:

Lemma 5.1. *Definability and Invariance are preserved by isomorphism* .
For definability this means merely that when α is an isomorphism from $\mathfrak{A}$ onto $\mathfrak{B}$ (with respect to all the non-logical symbols that are interpreted by both $\mathfrak{A}$ and $\mathfrak{B}$ $(=\alpha\mathfrak{A})$), a subset, S, of $|\mathfrak{A}|^n$ is definable in $\mathfrak{A}$ iff αS is definable by the *same* formula in $\mathfrak{B}$.
This is provable by induction on the syntactic structure of formulae.

The preservation of invariance, although equally obvious, can be understood as a category-theory observation: Given an isomorphism (both mono- and epi-) $\alpha : \mathfrak{A} \to \mathfrak{B}$ and an automorphism $\phi : \mathfrak{A} \to \mathfrak{A}$, $\alpha^{-1}\phi\alpha$ must be an automorphism: $\mathfrak{B} \to \mathfrak{B}$, and every automorphism of $\mathfrak{B}$ can be obtained in this way—so that the *functor* F: $\phi \to \alpha^{-1}\phi\alpha$ is an isomorphism between $G(\mathfrak{A})$ and $G(\mathfrak{B})$ [1_A is mapped on 1_B, $F(\phi\psi)= \alpha^{-1}\phi\psi\alpha=(\alpha^{-1}\phi\alpha)(\alpha^{-1}\psi\alpha)=F(\phi)F(\psi)$, and, $F(\phi^{-1})= \alpha^{-1}\phi^{-1}\alpha = (\alpha^{-1}\phi\alpha)^{-1}=(F\phi)^{-1}$]
This treats the automorphisms of each structure as a separate category with a singleton set of one underlying structural "object".

Lemma 5.2. *Elementary Invariance is preserved by isomorphism* .
Take the isomorphic image, $\mathfrak{A}'$, by an isomorphism, α, of a structure, $\mathfrak{A}$ that has an elementary extension, $\mathfrak{B}$, and show (by "transplanting" $\mathfrak{A}'$ instead $\mathfrak{A}$ of in $\mathfrak{B}$) that it must have an elementary extension, $\mathfrak{B}'$, isomorphic to $\mathfrak{B}$, under an isomorphism extending α .
One uses then the previous lemma (to prove preservation of invariance in an elementary extension).

THEOREM B. *If $\mathfrak{A}$ is an* EI *structure for* $\mathbb{L}$, *then a finite subset of $|\mathfrak{A}|^n$ is invariant iff it is definable.*

Proof: Since any definable subset is invariant, we can assume that $S \subseteq |\mathfrak{A}|^n$ is a finite invariant, and proceed to prove its definability. Let $S=\{<b_{i1},...,b_{in}> \mid 1\le i\le K\}$, where $\{b_{ij}\}\subseteq|\mathfrak{A}|$. Let $\mathbb{L}+$ be the language obtained from $\mathbb{L}$ by adding a special n-ary predicate symbol R^S and special unary predicate symbols $\{A_a \mid a\in|\mathfrak{A}|\}$. Let $\mathfrak{A}+$ be the structure defined by

$|\mathfrak{A}+| = |\mathfrak{A}|$.
$R^S_{\mathfrak{A}+}=S$ and $A_{a\mathfrak{A}+}=\{a\}$ (for $a\in|\mathfrak{A}|$) and
$X_{\mathfrak{A}+}=X_{\mathfrak{A}}$ for any other non-logical symbol, X, of $\mathbb{L}+$.

Let $Th_{\mathbb{L}}(\mathfrak{A})$ and $Th_{\mathbb{L}+}(\mathfrak{A}+)$ be the complete theories of $\mathfrak{A}$ and $\mathfrak{A}+$ (relative to $\mathbb{L}$ and $\mathbb{L}+$) respectively.

Let T be $Th_{\mathbb{L}+}(\mathfrak{A}+)$. It must include the following sentences of $\mathbb{L}+$ that are true in $\mathfrak{A}+$.

(I) $\{(\exists!x)(A_{b_{ij}}x_i) \mid i\leq K, j\leq n\}$; and (II) $(\forall x_1)...(\forall x_n)(R^S x_1...x_n \equiv \bigvee_{i\leq K}\bigwedge_{j\leq n}A_{b_{ij}}x_j)$

[where '$(\exists!x)(\Phi x)$' stands as usual for '$(\exists x)(\Phi x)\ \&(\forall y)(\forall z)(\Phi y\&\Phi z\rightarrow y=z)$'].

Let $\mathfrak{B}+$ be *any* model of T, and let $\mathfrak{B}$ be the restriction of $\mathfrak{B}+$ to $\mathbf{L}$ (obviously $|\mathfrak{B}| = |\mathfrak{B}+|$). $\mathfrak{B}+$ must be an elementary extension of a model isomorphic to $\mathfrak{A}+$, and it is clear then that $\mathfrak{B}$ must be an elementary extension of some $\mathbf{L}$-structure isomorphic to $\mathfrak{A}$. From the above lemmas (as well as the preservation of elementary extensions and elementary submodels by isomorphism) it follows that there would be no loss of generality if we were to assume that $\mathfrak{B}+$ is an elementary extension of $\mathfrak{A}+$, and that $\mathfrak{B}$ is an elementary extension of $\mathfrak{A}$.

From T ((I) and (II)), and the assumption that $\mathfrak{A}+$ is an elementary submodel of $\mathfrak{B}+$, it follows that $\{A_{b_{ij}}\}$ and therefore R^S must have the same extensions $\{\{b_{ij}\} \mid \mid i\leq K, j\leq n\}$ and S in both $\mathfrak{A}+$ and $\mathfrak{B}+$. Let ψ be any $\mathbf{L}$-automorphism of $\mathfrak{B}+$ (and thus of $\mathfrak{B}$ as well). Since $\mathfrak{A}$ is EI, it follows that $\psi|\mathfrak{A}| = |\mathfrak{A}|$ and hence that $\psi \mid_{|\mathfrak{A}|}$ is an $\mathbf{L}$-automorphism of $\mathfrak{A}$. Thus $\psi R^S_{\mathfrak{B}+} = \psi S = \psi \mid_{|\mathfrak{A}|} S = S = R^S_{\mathfrak{B}+}$, and hence $\psi R^S_{\mathfrak{B}+} = R^S_{\mathfrak{B}+}$ and ψ is an R^S-automorphism. From the disjunctive definability (Svenonius) theorem (§2) it follows that for some finite k

$T\vdash (R^S \leftrightarrow \Phi_1)^C \vee ... \vee (R^S \leftrightarrow \Phi_k)^C$, where $\Phi_1, ..., \Phi_k$ are $\mathbf{L}$-formulae. Let $\Phi^*_1, ..., \Phi^*_k$ be the closure of $\Phi_1, ..., \Phi_k$ over all variables not used in R^S in the above disjunction. Then, by logic,

$T\vdash (\forall z_1)...(\forall z_n)(R^S[z_1...z_n] \leftrightarrow \Phi^*_1[z_1...z_n]) \vee ... \vee (\forall z_1)...(\forall z_n)(R^S[z_1...z_n] \leftrightarrow \Phi^*_k[z_1...z_n])$

In particular $\mathfrak{A}+ \models (\forall z_1)...(\forall z_n)\ (R^S[z_1...z_n] \leftrightarrow \Phi^*_{i^*}[z_1...z_n])$ for some $i^*\leq k$, or loosely $\mathfrak{A} \models \Phi^*_{i^*}[a_1...a_n]$ iff $\langle a_1,...,a_n\rangle \in R^S_{\mathfrak{A}+} = S$, for any $\langle a_1,...,a_n\rangle$ ■.

We now use the following:

Lemma 5.3. *If $S\subseteq|\mathfrak{A}|$ is finite and definable in $\mathfrak{A}$ by Φ then it is so in any elementary extension and, in addition, invariant in any elementary extension,*

Proof: For any $a\in|\mathfrak{A}|$, $\mathfrak{A} \models \Phi(a)$ implies $\mathfrak{B} \models \Phi(a)$ for any elementary extension $\mathfrak{B}$ of $\mathfrak{A}$

Likewise the fact that $\mathfrak{A}^S \models (\forall z)(\Phi(z) \leftrightarrow [(z=b_1) \vee ... \vee (z=b_k)]$, where $S=\{b_1,...,b_k\}$, implies $\mathfrak{B}^S \models (\forall z)(\Phi(z) \leftrightarrow [(z=b_1) \vee ... \vee (z=b_k)]$. Thus the set $\{z \mid \Phi(z)\}$ has the same extension in any elementary extension of $\mathfrak{A}$. Also, as definable in every such extension it is invariant therein.

Lemma 5.4. *If every element in $|\mathfrak{A}|$ belongs to a finite set definable in $\mathfrak{A}$, $\mathfrak{A}$ must be* EI.

Proof: $|\mathfrak{A}|$ would be then, by lemma 5.3, a union (finite or infinite) of sets $\{S_i\}$ that are invariant in any elementary extension of $\mathfrak{A}$. Since $f\bigcup_i S_i = \bigcup_i fS_i$ for any function f satisfying $fS=\{fx \mid x\in S\}$ (the same is not true for $\bigcap_i$) we get for any automorphism ψ of any elementary extension of $\mathfrak{A}$ that $|\mathfrak{A}| = \bigcup_i S_i = \bigcup_i \psi S_i = \psi \bigcup_i S_i = \psi|\mathfrak{A}|$.

Corollary I. Every finite structure is elementarily invariant.

Corollary II. A structure satisfying β_{fin} in which every minimal unary invariant is finite must be elementarily invariant.

(Notice that other minimal invariants must be then finite too, since

$$\text{orbit}_{\mathfrak{A}}\langle a_1,\ldots,a_n\rangle \subseteq \text{orbit}_{\mathfrak{A}}\langle a_1\rangle \times \cdots \times \text{orbit}_{\mathfrak{A}}\langle a_n\rangle)$$

corollary III. β holds for every finite structure.

corollary IV. Finite $G(\mathfrak{A}) \Rightarrow (\mathfrak{A}$ satisfies $\beta_{fin} \Leftrightarrow \mathfrak{A}$ is EI).

Lemma 5.5. *If a countable $\mathfrak{A}$ contains an infinite minimal invariant, then it can not be an Elementarily Invariant structure.*

Proof: By the remark following corollary II above, if there were such an invariant, there would be then an infinite minimal unary invariant subset S_ω of $|\mathfrak{A}|$. Furthermore, all the elements in S_ω would share the same 1-type, Σ, and given any $a \in S_\omega$, we must have $S_\omega = \text{orbit}(a)$.

Let $\mathbb{L}^*$ be the language $\mathbb{L}(|\mathfrak{A}| \cup \{a_{new}\})$, where $\mathbb{L}(|\mathfrak{A}|)$ is augmented to contain one additional constant symbol, a_{new}. Let T^* be the deductive closure of (1)+(2)+(3), where (1) is the complete theory of $\mathfrak{A}$ as a structure for $\mathbb{L}(|\mathfrak{A}|)$ (i.e, $\text{Th}(\mathfrak{A}^{|\mathfrak{A}|})$), which includes, for any constant, a, whose reference in $(\mathfrak{A}^{|\mathfrak{A}|})$ belongs to S_ω, the result of substituting a in all the formulae of Σ; where (2) = $\{\phi(a_{new}) \mid \phi \in \Sigma\}$; and where (3)= $\{a \neq a_{new} \mid a \in \mathbb{L}(|\mathfrak{A}|)\}$. Notice that a_{new} is bound to have the 1-type Σ, in *the restriction to* $\mathbb{L}$ of any T^*-model (since Σ is included in its 1-type), but this would be vacuously true if T^* were inconsistent.

It is easy to show that T^* is consistent (if $|\mathfrak{A}|$ were *finite*, it would not be so!), by using the compactness theorem and the infinitude of S_ω. For given any finite subset of sentences, in T^*, we can satisfy them as follows: If $\{a_{i_1},\ldots,a_{i_k}\}$ is the finite subset of all the constant symbols, in $\mathbb{L}(|\mathfrak{A}|)$, that are used in these sentences, define the model $\mathfrak{A}^+_{\{i_1,\ldots,i_k\}}$ to be the same as $\mathfrak{A}^{|\mathfrak{A}|}$, as far as its universe, its non-logical predicates and function symbols, and $\{a_{i_1},\ldots,a_{i_k}\}$ are concerned, but as one that picks the reference of a_{new} to be some (any) member of $S_\omega - \{a_{i_1},\ldots,a_{i_k}\}$. Given the above assumptions about $\mathfrak{A}$ and S_ω, it is clear that this model would satisfy any subset of T^* that utilises only the constant-symbols $a_{i_1},\ldots,a_{i_k}$ and a_{new}.

Let $\mathfrak{B}^*$ be a model of T^*, and let $\mathfrak{B}$ be its restriction to $\mathbb{L}$. $\mathfrak{B}$ is an elementary extension of a model isomorphic to $\mathfrak{A}$, which we can assume—without loss of generalisation—to be $\mathfrak{A}$ itself. Furthermore, picking any particular constant symbol, say a^*, whose reference in $\mathfrak{B}$ belongs to S_ω, a^* and a_{new} in $\mathfrak{B}$ must have the same ($\mathbb{L}$-) 1-type—i.e, Σ—a fact which constitutes an isomorphism, ζ, of $\{a^*\}$ and $\{a_{new}\}$ in $\mathfrak{B}$. By the *extending automorphism lemma*, then, ζ is extendible to an automorphism of an elementary extension, $\mathfrak{C}$, of $\mathfrak{B}$. We thus get an elementary extension of $\mathfrak{A}$, $\mathfrak{C}$, in which an automorphism fails to conserve either S_ω or $|\mathfrak{A}|$ (for in any case an invariant subset of an EI structure must be invariant in any elementary extension thereof) ■.

We can therefore characterise EI structures by the following

THEOREM 5.6. *A structure is Elementarily Invariant iff every minimal invariant (every orbit) is both finite and definable.*

This, of course, does not imply that elementarily invariance must entail a finite number of symmetries, but merely that each element can be acted upon only in finitely many ways. Examples of EI structures with infinitely many symmetries are
(1) *The infinite full binary tree*, in which each node has exactly two successors, and
(2) The *field of all algebraic numbers* over the rationals.

We can define, now, the property β_{min}, requiring every *minimal* invariant to be definable. By lemma 3.5 it would follow that in a structure satisfying β_{min} every minimal n-ary invariant must have a principal n-type. Now it is true, in general, that any n-type in Th($\mathfrak{A}$) must be realised in (all the members of) some n-ary minimal invariant of $\mathfrak{A}$ if it is realisable in $\mathfrak{A}$. Let S be the set of *all* n-tuples in $|\mathfrak{A}|$ that have this n-type. Clearly any automorphism will preserve the satisfaction of this n-type, and therefore any member of S can be moved by it only *into* S. If S is finite any automorphism moves it *onto* itself; while if S is infinite and is moved by an automorphism into a proper subset of S, T, the reverse automorphism would move members of S-T out of S, and would not preseve the n-type. Hence S must be an invariant and any minimal n-ary invariant contained in S must satisfy the given n-type. It thus follows that in any structure, $\mathfrak{A}$, satifying β_{min}, every *realisable* n-type is *principal* in Th($\mathfrak{A}$), and by a well known model theoretic result (see [Shoenfield, Mathematical Logic, pp.103- 104, 27,g.]), this is equivalent to $\mathfrak{A}$ being an *elementarily prime model* of Th($\mathfrak{A}$)—i.e., to the fact that every model which is elementarily equivalent to $\mathfrak{A}$ must be isomorphic to an elementary extension of $\mathfrak{A}$. We can therefore infer

Corollary V. A structure for $\mathbf{L}$ is Elementarily Invariant only if it is an Elementarily Prime Model of its own $\mathbf{L}$-theory.

The converse is not necessarily true. It is easy to produce an example of an elementarily prime model of a complete theory with an infinite minimal invariant, which would fail then to be elementarily invariant.
One example of such a model is any countable model of the theory of a *dense ordered set without first or last element* (in a language containing only '<' as a non-logical symbol!), e.g, $\mathbf{Q}^{<}$, the Rationals with respect to their order type.
Any two countable models of this theory are <-isomorphic (i.e. the theory is $\aleph_0$-categorical). The theory is complete (and there are no finite models) and any of its models is saturated. Thus any countable extension model of this theory—such as $\mathbf{Q}^{<}(\sqrt{2})$, or the real algebraic numbers, *with respect to order only*— would be an elementary extension. Such extensions of $\mathbf{Q}$ have infinitely many <-automorphisms (e.g, any linear transformation X—> aX+b with a>0 and b in the extension model) which do not map $\mathbf{Q}$ on $\mathbf{Q}$. (e.g, X—> X+$\sqrt{2}$ for $\mathbf{Q}(\sqrt{2})$). However, we notice that all invariants of these automorphisms are infinite!

Another example: Consider the theory T that has , as axioms, sentences in a language with a only one monadic predicate, P, asserting that for any set of n different individuals satisfying P, there is another individual satisfying P, as well as a sentence asserting that there is an individual satisfying P. Given any countable model satisfying this theory, the submodel ,$\mathfrak{A}'$, determined by all individuals satisfying P would itself be a countable elementarily prime model of T satisfying, in addition, $(\forall x)(Px)$. It is easily proven that any two countable models of T'= T+$(\forall x)(Px)$ are P-isomorphic. Therefore T' is $\aleph_0$-categorical and complete, so T' is deductively equivalent to Th($\mathfrak{A}'$). It is clear then that any model elementarily equivalent to $\mathfrak{A}'$ —which must satisfy T'—contains an elementary submodel isomorphic to $\mathfrak{A}$. On the other hand $\mathfrak{A}'$ is not elementarily invariant, because $|\mathfrak{A}'|$ is the only non trivial invariant in A', and is infinite. This can be seen directly by proving the existence of an elementary extension $\mathfrak{B}'$ of $\mathfrak{A}'$ containing one additional element (also satisfying P). That such an extension exists can be easily proved by applying the compactness theorem to prove the consistency of the union of the complete diagram of $\mathfrak{A}'$ with an infinite set of statements, each of which asserting that the only new individual is different from an individual of $\mathfrak{A}'$, but collectively referring to every element of $\mathfrak{A}'$. Any permutation of the elements of $\mathfrak{B}'$ defines an automorphism therein, but some such permutations fail to move $|\mathfrak{A}'|$ onto itself.

In the next section we will deal only with EI structures and their "Galois Theory".

6. Galois Theory of EI structures.

We start with a generalisation of Theorem B (§5):

THEOREM C. *In an* EI *structure* $\mathfrak{A}$, *a finite subset of* $|\mathfrak{A}|^n$ ($n<\omega$) *is* D-*definable—where* D *is countable subset of* $|\mathfrak{A}|$*—iff it is* D-*invariant*.

Proof. Let $L^U(D)$ be the language L augmented by a countable set of unary predicates $\{U_a \mid a\in D\}$, Let $\mathfrak{A}^{+D}$ be a structure for $L^U(D)$ identical to $\mathfrak{A}$ for L, but in which for any $a\in D$ the extension (interpretation) of each U_a is {a}. We first notice that if $\mathfrak{A}$ is EI so is $\mathfrak{A}^{+D}$. For, any automorphism of an elementary extension, $\mathfrak{B}^{+D}$, of $\mathfrak{A}^{+D}$, is by definition nothing but an automorphism β of $\mathfrak{B}=\mathfrak{B}^{+D}|_L$, for which every member of D is a fixed point! A-fortiori, $|\mathfrak{A}^{+D}|=|\mathfrak{A}|=\beta|\mathfrak{A}|=\beta|\mathfrak{A}^{+D}|$. Now, from theorem B above it follows that any finite subset of $|\mathfrak{A}|^n = |\mathfrak{A}^{+D}|^n$, which is an n-ary invariant in $\mathfrak{A}^{+D}$, is definable in $\mathfrak{A}^{+D}$. To be invariant in $\mathfrak{A}^{+D}$ means, by the above remarks, to be invariant under all those automorphisms of $\mathfrak{A}$ which leave every element of D unmoved, which constitute the subgroup $G(\mathfrak{A}/D)$. Invariance in $\mathfrak{A}^{+D}$ is therefore tantamount to what we defined as D-invariance in $\mathfrak{A}$ (or invariance in $\mathfrak{A}$ with respect to D). Similarly, for a set $S\in|\mathfrak{A}|^n =|\mathfrak{A}^{+D}|^n$ to be D-definable in $\mathfrak{A}$ means that there exists a formula $\Psi(z_1,...z_n, d_{i_1},...,d_{i_k})$ in $S_n(L(D))$—where $d_{i_1},...,d_{i_k}$ are all the names of elements of D (in $\mathfrak{A}^D$) that occur explicitly in the formula—such that $\mathfrak{A}^D \models \Psi(a_1,...,a_n, d_{i_1},...,d_{i_k})$ iff $\langle a_1,...,a_n\rangle \in S$.

For any such Ψ let $\Psi^*(z_1,...z_n)$ be the formula

$$(\exists x_{i_1})(\exists x_{i_2})...(\exists x_{i_k})[\, U_{d_{i_1}}(x_{i_1}) \,\&\, U_{d_{i_2}}(x_{i_2}) \,\&\, ... \,\&\, U_{d_{i_k}}(x_{i_k}) \,\&\, \Psi(z_1,...z_n, x_{i_1},...,x_{i_k})\,].$$

It is obvious that $\mathfrak{A}^D \models \Psi(z_1,...z_n, d_{i_1},...,d_{i_k})$ iff $\mathfrak{A}^{+D} \models \Psi^*(z_1,...z_n)$. Thus D-definability is tantamount to simple definability in $\mathfrak{A}^{+D}$ ■.

Suppose D is an invariant subset in $\mathfrak{A}$. Consider the substructure, $\mathfrak{A}|_D$, of $\mathfrak{A}$, defined by restricting the domain to D. We shall use 'G(D)' to loosely denote $G(\mathfrak{A}|_D)$. The relationship between this group and $G(\mathfrak{A})$ is provided by the following

Lemma 6.1. *If* D *is an invariant subset of* $|\mathfrak{A}|$ *in an* EI *structure* $\mathfrak{A}$, *then*

$G(D)=_{Df} G(\mathfrak{A}|_D)$ *is isomorphic to* $G(\mathfrak{A})/G(\mathfrak{A}/D)$.

Proof. From lemma 1.4 we know that $G(\mathfrak{A}/D) < | G(\mathfrak{A})$. Define the natural mapping $\eta: G(\mathfrak{A}) \longrightarrow G(D)$ by $\eta(\sigma)=\sigma|_D$=σ-restricted-to-D. This is a proper definition since $\sigma(D)=D$ implies $\sigma|_D \in G(\mathfrak{A}|_D)$. To show η is surjective, suppose $\mu\in G(\mathfrak{A}|_D)$; then by the extending automorphism lemma μ can be extended to an automorphism of an elementary extension of $\mathfrak{A}$, which, by the elementary invariance of $\mathfrak{A}$, becomes by restriction to $|\mathfrak{A}|$ an automorphism ψ of $\mathfrak{A}$ satisfying $\eta(\psi)=\mu$.

The kernel of η is $\{\sigma \mid \sigma\in G(\mathfrak{A}) \,\&\, \sigma|_D =$ identity on D$\}$ which is exactly $G(\mathfrak{A}/D)$. Thus $G(D)\cong G(\mathfrak{A})/G(\mathfrak{A}/D)$ and the isomorphism is defined by $\phi(\sigma G(\mathfrak{A}/D))=\sigma|_D$.

Lemma 6.2. *In an EI-structure a functionally closed subdomain is a Galois subdomain.* (This is the converse of lemma 1.3).

Proof. Let $D=Cf_{\mathfrak{A}}(D)$. This means that if $d\notin D$, $\{d\}$ is not D-definable, and, by theorem C, not D- invariant. d must be movable then by some $\mu\in G(\mathfrak{A}/D)$. Hence $D=K_{\mathfrak{A}}G(\mathfrak{A}/D)$.

We thus see that in an EI-structure the Galois subdomains are exactly the functionally closed subdomains. We are now in position to prove a near analogue to one of the main theorems of classical Galois Theory:

THEOREM D. *Let* $\mathfrak{A}$ *be an elementarily invariant structure and let* D *be a Galois subdomain. Suppose further that* $G(\mathfrak{A}/D)$ *is a finite normal subgroup of* $G(\mathfrak{A})$. *Then*

(i) D *is invariant in* $\mathfrak{A}$.

(ii) $|\mathfrak{A}|=Cf_{\mathfrak{A}}(D\cup S)$, *where* cardinality(S)<o($G(\mathfrak{A}/D)$), *and*

(iii) $|\mathfrak{A}|=Cf_{\mathfrak{A}}(D\cup\{x\mid\Phi(x)\})$, *where* $\Phi\in S_1(L(D))$, *and*

$$\text{cardinality}(\{x\mid\Phi(x)\})<o(G(\mathfrak{A}/D))\times(o(G(\mathfrak{A}/D))-1).$$

This shows, in effect, that when $G(\mathfrak{A}/D)$ is finite, $\mathfrak{A}$ is the *splitting* extension of $\mathfrak{A}|_D$—i.e, it can be generated from it by adding to D the finite number of $\mathfrak{A}$-solutions of a 1-free-place formula of L(D), having no solutions in D.

Proof. (i) follows from lemma 1.5. We shall define now a finite ascending chain of Galois subdomains of $\mathfrak{A}$, as follows:

(1) $D_0=D$; (2) if D_i is constructed, and it is a Galois subdomain, and $D_i\neq|\mathfrak{A}|$, choose $y_i\in|\mathfrak{A}|-D_i$, and let $\Sigma_i=\{\sigma_1^{(i)},\ldots,\sigma_{k_i}^{(i)}\}$ be the set of all elements of $G(\mathfrak{A}/D_i)$ which really move y_i. By definition (of a Galois subdomain) $k_i\geq1$. Define then $D_{i+1}=Cf_{\mathfrak{A}}(D_i\cup\{y_i\})$. Therefore D_{i+1} must be Galois by lemmas 6.2 and 1.1.

We can easily establish that $\sigma\in\Sigma_i\ \longrightarrow\ \sigma\notin\bigcup_{k<i}\Sigma_k$, since $\sigma\in\Sigma_i\ \longrightarrow\ \sigma\in G(\mathfrak{A}/D_i)$ implies that any $\sigma\in\Sigma_i$ leaves unmoved *any* element of D_i. Thus, if $\mu\in\Sigma_k$ and k<i, we have $y_k\in D_{k+1}\subseteq D_i$ and $\mu y_k\neq y_k$, whereas $\sigma y_k=y_k$ for any $\sigma\in\Sigma_i$.

The automorphisms of $\Sigma_0\cup\ldots\cup\Sigma_i$ are all different ones belonging to $G(\mathfrak{A}/D)-\{\iota\}$, (where ι is the identity of $G(\mathfrak{A})$) and no Σ_i is empty unless $D_i=|\mathfrak{A}|$. Thus, since $G(\mathfrak{A}/D)$ is finite, we must have $D_N=|\mathfrak{A}|$ for some $N\leq o(G(\mathfrak{A}/D))-1$.

Lemma1.2 entails now, by induction, that $D_N=|\mathfrak{A}|=Cf_{\mathfrak{A}}(D\cup\{y_0,\ldots,y_{N-1}\})$; so $|\mathfrak{A}|=Cf_{\mathfrak{A}}(D\cup S)$, where cardinality(S)<o($G(\mathfrak{A}/D)$).

Let $S^*=\{\sigma y_i\mid y_i\in S\ \&\ \sigma\in G(\mathfrak{A}/D)\}$. Then $|\mathfrak{A}|=Cf_{\mathfrak{A}}(D\cup S^*)$, where S^* is a D-invariant and cardinality(S^*)$\leq$ order($G(\mathfrak{A}/D)$)xcardinality(S) $\leq$ order($G(\mathfrak{A}/D)$)x(order($G(\mathfrak{A}/D)$) - 1).

By theorem C, S^* is the solution-set in for some 1-free-place formula Φ in $S_1(L(D))$ ■.

We note that the above proof is wasteful—since the arbitrary choice of $y_i\in|\mathfrak{A}|-D_i$, at the i-th stage, does not allow us to postulate more than one automorphism of $G(\mathfrak{A}/D_i)$ that really moves y_i. The freedom to choose any $y_i\in|\mathfrak{A}|-D_i$, at the i-th stage, means that we can use it to maximize k_i—the number of appropriate automorphisms moving it.

Furthermore, while the set S* above is obviously the smallest D-invariant containing S, one can still improve the estimates on the size of the solution-set required, in addition to the base domain D, in generating the full structure by functional closure.

Finally we note that one does not necessarily require an entire solution set of some formula Φ in order to define, on the basis of a smaller structure, a full splitting structure for F. Some of the solutions of a predicate may be definable in terms of others (and in any case any one of them is definable in terms of the others, in a language with equality).

Definition. Suppose $\mathfrak{A}_0$ is a functionally closed substructure of $\mathfrak{A}$. *The Functional Dimension of* $\mathfrak{A}$ *over* $\mathfrak{A}_0$ —to be denoted by ' $FD(\mathfrak{A}:\mathfrak{A}_0)$') will then be the minimal integer, M, for which there is a set S with M-1 members satisfying $|\mathfrak{A}| = Cf_{\mathfrak{A}}(|\mathfrak{A}_0| \cup S)$.

Theorem D above shows then that the functional dimension of an EI structure, $\mathfrak{A}$, over a Galois subsructure, $\mathfrak{A}_0$,with a finite normal subgroup $G(\mathfrak{A}/\mathfrak{A}_0)$, can not be greater than the size (order) of that group. The actual value of the functional dimension, however, is far smaller in most such cases, since we can easily prove

Lemma 6.3. *Under the above conditions on* $\mathfrak{A}$ *and* $\mathfrak{A}_0$, $FD(\mathfrak{A}:\mathfrak{A}_0) \leq 1+\log_2(o(G(\mathfrak{A}/\mathfrak{A}_0))$.

This will follow from

THEOREM E. *Let* $\mathfrak{A}$ *be an elementarily invariant structure and let* $\mathfrak{A}_0$ *be a Galois substructure. with a finite subgroup* $G(\mathfrak{A}/\mathfrak{A}_0)$. Let $M = FD(\mathfrak{A}:\mathfrak{A}_0)$, *and let* $\{b_1,...,b_{M-1}\}$ *be a minimal basis for generating* $\mathfrak{A}$ *out of* $\mathfrak{A}_0$ *by functional closure, i.e, one that satisfies*

$|\mathfrak{A}| = Cf_{\mathfrak{A}}(|\mathfrak{A}_0| \cup \{b_1,...,b_{M-1}\})$ — while no lesser set (in cardinality) does.

Then there exist in $G(\mathfrak{A}/\mathfrak{A}_0)$ M-1 *automorphisms,* $\sigma_1,...,\sigma_{M-1}$, *satisfying*

(i) $\sigma_i b_j \neq b_j$ iff $i=j$, and

(ii) The subgroup generated by $\sigma_1,...,\sigma_{M-1}$ is Abelian of order$\geq 2^{M-1}$.

Proof. Let $S=\{b_1,...,b_{M-1}\}$ and let $S_{-j}=S-\{b_j\}$. It is obvious that no b_j belongs to $Cf_{\mathfrak{A}}(|\mathfrak{A}_0| \cup S_{-j})$, or otherwise S_{-j} would provide a basis with a smaller number of elements. Furthermore, by lemma 6.2 any functionally closed subdomain such as $Cf_{\mathfrak{A}}(|\mathfrak{A}_0| \cup S_{-j})$ must be Galois.Therefore, for any j, $1 \leq j \leq M-1$, there must be an automorphism σ_j in $G(\mathfrak{A}/|\mathfrak{A}_0| \cup S_{-j})$ which moves b_j but leaves unmoved any other b_i , where $i \neq j$.

We now show that the automorphisms, $\sigma_1,...,\sigma_{M-1}$ commute with each other:
By assumption $|\mathfrak{A}| = Cf_{\mathfrak{A}}(|\mathfrak{A}_0| \cup \{b_1,...,b_{M-1}\})$; therefore , for any $a \in |\mathfrak{A}_0|$, there is a formula $F(z_1,...,z_{M-1},z_M)$ in $S_M(L(|\mathfrak{A}_0|))$, such that
$\mathfrak{A}^{|\mathfrak{A}_0|} = F(b_1,...,b_{M-1}, a) \;\&\; (\forall x)[\, F(b_1,...,b_{M-1}, x) \longrightarrow x=a \,]$.
This implies (applying σ_j) that

$\mathfrak{A}|\mathfrak{A}_0| = F(b_1,...,\sigma_j b_j,...,b_{M-1}, \sigma_j a) \;\&\; (\forall x)[\, F(b_1,...,\sigma_j b_j,...,b_{M-1}, x) \longrightarrow x=\sigma_j a]$,
which implies (applying σ_i, where, say, i<j) that
$\mathfrak{A}|\mathfrak{A}_0| = F(b_1,...,\sigma_i b_i,...,\sigma_j b_j,...,b_{M-1}, \sigma_i\sigma_j a) \;\&\; (\forall x)[F(b_1,...,\sigma_i b_i,...\sigma_j b_j,...,b_{M-1}, x) \longrightarrow x=\sigma_i\sigma_j a]$
If, instead, we were to apply σ_i first and then σ_j, to the "definability" of {a}, we would get
$\mathfrak{A}|\mathfrak{A}_0| = F(b_1,...,\sigma_i b_i,...,\sigma_j b_j,...,b_{M-1}, \sigma_j\sigma_i a) \;\&\; (\forall x)[F(b_1,...,\sigma_i b_i,...\sigma_j b_j,...,b_{M-1}, x) \longrightarrow x=\sigma_j\sigma_i a]$.
Thus, by (2nd order) logic, $(\forall a)[a\in|\mathfrak{A}_0| \longrightarrow \sigma_j\sigma_i a=\sigma_i\sigma_j a]$.
Now let r_i be the the least positive exponent for which $\sigma_i^{r_i} b_i = b_i$ (there must be such because every orbit is finite!). By the definition of σ_i above $r_i \geq 2$, and therefore the order of σ_i in $G(\mathfrak{A}/\mathfrak{A}_0)$ is $\geq r_i \geq 2$.
The Abelian group G_A generated by $\sigma_1,...,\sigma_{M-1}$, contains the set
$\{\, \sigma_1^{n_1}\sigma_2^{n_2}\cdots\sigma_{M-1}^{n_{M-1}} \mid 1\leq n_i\leq r_i \,\}$. Now, each $<n_1,...,n_{M-1}>$ defines a unique automorphism in this set, since $<n_1,...,n_{M-1}>\neq<n'_1,...,n'_{M-1}>$, where $1\leq n_i,n'_i\leq r_i$, implies $n_i\neq n'_i$ for some i<M, and then $\sigma_1^{n_1}\sigma_2^{n_2}\cdots\sigma_{M-1}^{n_{M-1}} b_i = \sigma_i^{n_i} b_i$, while $\sigma_1^{n'_1}\sigma_2^{n'_2}\cdots\sigma_{M-1}^{n'_{M-1}} b_i = \sigma_i^{n'_i} b_i$; but $\sigma_i^{n_i} b_i \neq \sigma_i^{n'_i} b_i$, since $0<|n_i-n'_i|<r_i$.
Thus the order of $G_A \geq r_1 x...x r_{M-1} \geq 2^{M-1}$ ■.

From this theorem it follows that $M-1\leq \log_2(o(G(\mathfrak{A}/\mathfrak{A}_0))$, which is lemma 6.3.
Furthermore, since we can always find in $\mathfrak{A}$ an $|\mathfrak{A}_0|$-invariant subset of size$\leq$(M-1) x order($G(\mathfrak{A}/\mathfrak{A}_0)$, containing a subset of size M-1, we have the following result:
THEOREM F. *If $\mathfrak{A}$ is an elementarily invariant structure and $\mathfrak{A}_0$ is a functionally closed substructure determining a finite subgroup $G(\mathfrak{A}/\mathfrak{A}_0)$, then $\mathfrak{A}$ is a splitting structure over $\mathfrak{A}_0$ for a 1-free-place formula $\Phi\in S_1(L(|\mathfrak{A}_0|))$, with a finite number of solutions N (in any elementary extension of $\mathfrak{A}$) where $N\leq R\log_2 R$ and R is the order of an Abelian subgroup contained in $G(\mathfrak{A}/\mathfrak{A}_0)$. In any case we have $N\leq o(G(\mathfrak{A}/\mathfrak{A}_0)x\log_2(o(G(\mathfrak{A}/\mathfrak{A}_0))$.* (see below for better result).

Emended Upper Bound for "Splitting Degree": From the proof of theorem E above we can easily see that for each minimal basis the elements of a certain Abelian subgroup of $G(\mathfrak{A}/\mathfrak{A}_0)$ (G_A in that proof) act on it in a special way, which might allow us to get a slightly better upper bound for N above. We thus look at the minimal invariant closure, S*, of a minimal basis,$\{b_1,...,b_{M-1}\}$, as a union
$\{\sigma b_i \mid \sigma\in G_A\} \cup \{\sigma b_i \mid \sigma\in G(\mathfrak{A}/D)\text{-}G_A\}$. Remembering that G_A is generated by $\sigma_1,...,\sigma_{M-1}$,
where each moves exactly one (corresponding) basis element , and letting r_i again be the minimal positive exponent satisfying $\sigma_i^{r_i} b_i = b_i$, we get
cardinality $\{\sigma b_i \mid \sigma\in G_A\} \leq \Sigma r_i \leq (M-1) \times \max\{r_i\}$
cardinality $\{\sigma b_i \mid \sigma\in G(\mathfrak{A}/D)\text{-}G_A\} \leq (M-1) x(o(G(\mathfrak{A}/\mathfrak{A}_0) - o(G_A))$, where $o(G_A)\geq \Pi r_i$.
Thus N=cardinality $S^* \leq (M-1)x\,[\, o(G(\mathfrak{A}/\mathfrak{A}_0) - (\Pi r_i - \max\{r_i\})\,]\leq$
$(M-1)x\,[\, o(G(\mathfrak{A}/\mathfrak{A}_0) - \max\{r_i\}(2^{M-2}-1)\,]$, therefore giving the improved upper bound

$$N\leq \log_2(o(G(\mathfrak{A}/\mathfrak{A}_0))x\,[\, o(G(\mathfrak{A}/\mathfrak{A}_0) - \max\{r_i\}(2^{M-2}-1)\,].$$

(Emended Upper Bound for "splitting degree " when M>2)

Irreducible Predicates, Minimal Invariants and proper Splitting Extensions—More about the Analogy with classical Galois Theory. Until now we have been rather cavalier in our use of the term *splitting extension*. We will now show how the analogy to the classical Galois theory, that is suggested by the use of this term, in the context of investigating EI structures, could be made almost perfect by obtaining for such structures the general analogues of the allied classical concepts, such as irrducible polynomials, and minimal normal extensions (the last corresponding, via the Galois functor, to single steps in a composition series of the symmetry-group of the larger structure). We start with a review of the classical theory in comparison to the results we have presented thus far. This can be skipped over without affecting the continuity of what is to follow.

In classical Galois theory the term *splitting extension* is used when one has a base field, F, and an extension field E, in which a polynomial p(x) over F is factorable into linear factors, but not in any intermediate field. E is then said to be a *splitting field* of p(x) , and is generated by a root or roots of p(x). The concept of a *splitting extension for* p(x) is well defined up to isomorphism. An extension field is classically called *normal*, when it is a Galois extension according to our terminology. One of the basic classical theorems states that E is a normal extension of F iff it is a splitting field of a polynomial over F. This corresponds to parts of our above theorem D and theorem F for EI structures which, in turn, fit in with the idea of an Algebraic extension (such an extension of an EI structure is EI itself, while a transcendental extension need not be so!). In the classical theory it is proved that an intermediate field, B, between a base field, F, and a splitting extension, E, is normal (that is, Galois in our sense) iff G(F/B) is a normal subgroup of G(E/F). This could be proved by our lemmata 1.4, and 1.5 provided, however, that we added the requirement that when any such B is the fixed field of G(E/B)—i.e, when it is Galois, according to our terminology—it must be an F-*invariant in* E, i.e, any automorphism of G(E/F) must move B onto itself! This fact (which is just as crucial in the classical case, where it is stated as "B is a normal extension of F if and only if each isomorphism of B into E is an automorphism of B"—see, for example, [Artin, E., Galois Theory, p. 48, bottom paragraph]), is classically proved by using first the concept of the *degree* of one field (as a *vector space*) over another, in order to show that if G is a group of automorphisms of E (a subgroup of G(E)) and B is the fixed field of G, then the degree of E over B is equal to the order of G) and by exploiting specific field properties (existence of inverses, the distributive law, etc.). In general, however, this invariance with respect to a core structure is not automatically guaranteed for an intermediate structure unless it is explicitly required (It is conceivable that a more suitable sense of *Galois substructure* would include this desideratum of invariance, but this would always make it relative to a third core structure, besides itself and the larger structure, and would not automatically conform to the standard use of *Galois* as a synonym for *normal* when applied to field extensions).

Classically a polynomial p(x) over F is irreducible iff it is not the product of two polynomials over F—whose degrees are both less than that of p, but higher than 0. Suppose p is separable, i.e, in its splitting field, E_p, no two linear factors are "numerically" proportional (with a ratio in F). Another way to state then the irreducibility of p over F is to use the following metamathematical formula:

$(\forall q)(q \text{ is a polynomial over } F \rightarrow E_p \models ([(\forall x)[qx=0 \rightarrow px=0] \rightarrow (\forall x)[px=0 \rightarrow qx=0])$ —

in other words, "any polynomial whose roots are all p-roots must share all the roots of p". One can generalise this idea, for all unary predicates, on the basis of the observation that, like polynomial-equations, any formula defining a minimal (unary) invariant in an EI structure, must be satisfied only by finitely many values (This observation means, in particular, that for finite structures we can regard all predicates as "polynomial-equation-like") . It is trivial to note that that finitely satisfiable predicates—just like polynomial equations over splitting fields—are equivalent to finite disjunctions of the simplest linear "equations", equating a variable to an element of the splitting field.

This analogy was explored already by [Morely 1965], where the idea of irreducible polynomial was taken up and generalised for structures of different infinite powers. It is much more obvious perhaps, in the context of our elementary investigations, that the irreducibe predicates should be correlated in EI structures with minimal (unary) invariants. If irreducibility is to be defined by the lights of the above metamathematical formula, then the following ought to be true: *In* EI *structures every irreducible (unary) predicate defines a minimal invariant and vice versa, every minimal invariant is definable only by irreducible predicates.*

In fact, this is true for all models in which every minimal invariant is definable—i.e, those satisfying β_{min} (see lemma 6.5 below). In EI structures, however, every irreducible predicate has only a finite number of "solutions". Thus, it is only in EI structures that predicates defining minimal invariants constitute perfect analogues of irreducible polynomial equations.

Definition. For a structure $\mathfrak{A}$ for $\mathbf{L}$ let a 1-place formula $\Phi(z)$ belong to $S_1(\mathbf{L}(D))$. Then, we shall say that it is *(semantically)* D-*irreducible in* $\mathfrak{A}$ iff

$(\forall\Psi)\ [\ \Psi\in S_1(\mathbf{L}(D))\ \&\ \mathfrak{A}^D|=(\exists z)\Psi z \rightarrow (\ \mathfrak{A}^D|=(\forall z)(\Psi z\rightarrow\Phi z)\ \rightarrow \mathfrak{A}^D|=(\forall z)(\Phi z\rightarrow\Psi z)\ )\ ].$

We say that such a $\Phi\in S_1(\mathbf{L})$ is *irreducible in* $\mathfrak{A}$ iff it is $\varnothing$-irreducible there.

We can use the notation '$\mathfrak{A}(\Psi)$' to signify, for $\Psi\in S_1(\mathbf{L})$, the subset $\{x \mid \mathfrak{A}|=\Psi x\}$ of $|\mathfrak{A}|$.
The irreducibility in $\mathfrak{A}$ of $\Phi\in S_1(\mathbf{L})$ can alternatively be spelled out then as

$(\forall\Psi)\ [\ \Psi\in S_1(\mathbf{L})\ \&\ \mathfrak{A}(\Psi)\neq\varnothing \rightarrow (\ (\mathfrak{A}(\Psi)\subseteq\mathfrak{A}(\Phi)\ ) \rightarrow (\mathfrak{A}(\Psi)\supseteq\mathfrak{A}(\Phi)\ )\ )]\qquad(\nabla)$

Φ is *properly irreducible.*, when it is irreducible and satisfied by some individual($\mathfrak{A}(\Phi)\neq\varnothing$).

Let $\Phi\in S_1(\mathbf{L})$ & $\mathfrak{A}(\Phi)\neq\varnothing$ and let $\mathfrak{F}_{\Phi:\mathfrak{A}}$ be defined by $\mathfrak{F}_{\Phi:\mathfrak{A}}=\{\mathfrak{A}(\Psi) \mid \Psi\in S_1(\mathbf{L})\ \&\mathfrak{A}(\Psi)\supseteq\mathfrak{A}(\Phi)\}$.
$\mathfrak{F}_{\Phi:\mathfrak{A}}$ is a proper principal filter. Furthermore , we have (omitting the simple proof).

Lemma 6.4. If Φ is *properly irreducible in* $\mathfrak{A}$, *then for every* $\Psi\in S_1(\mathbf{L})$ *either* $\mathfrak{A}(\Psi)$*or* $|\mathfrak{A}|$-$\mathfrak{A}(\Psi)$ belongs to $\mathfrak{F}_{\Phi:\mathfrak{A}}$ *but not both.*

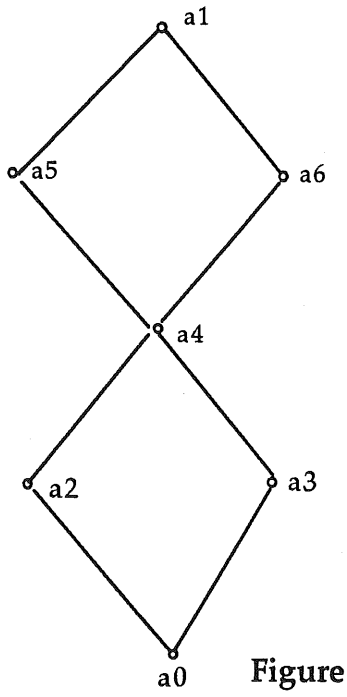
We now establish the correlation between proper irreducibility and minimal invariance.

Lemma 6.5. *In a model satisfying* β_{min} *(minimal invariants are definable) every properly irreducible (1-place) predicate defines a non-empty minimal (unary) invariant, and every such invariant is definable by some (and only by) properly irreducible predicate.*

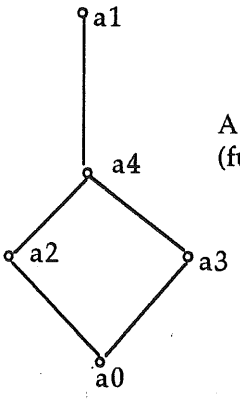
Proof. Let Φ be properly irreducible in $\mathfrak{A}$. $\mathfrak{A}(\Phi)$ is clearly invariant and not empty. It contains a non-empty minimal unary invariant (an orbit of any of its members), that must be definable by a formula Ψ of $S_1(\mathbf{L})$. We thus get $\mathfrak{A}(\Psi)\neq\varnothing$ & $(\mathfrak{A}(\Psi)\subseteq\mathfrak{A}(\Phi))$, which, by the irreducubility of Φ, imply that $\mathfrak{A}(\Psi)=\mathfrak{A}(\Phi)$, and therefore that $\mathfrak{A}(\Phi)$ is a minimal invariant.
Conversely, if S is a minimal unary invariant it is definable by some formula Φ, and if for some other formula Ψ of $S_1(\mathbf{L})$, we have $\mathfrak{A}(\Psi)\neq\varnothing$ & $\mathfrak{A}(\Psi)\subseteq\mathfrak{A}(\Phi)$, then we have a non-empty invariant $\mathfrak{A}(\Psi)$—any definable set is invariant— contained in $\mathfrak{A}(\Phi)$, and by the minimality of the latter, must be equal to it.

EXAMPLES: We want now to discuss a few simple examples which would show that the upper bounds— provided by Theorem E and the last remark following theorem F— on the relative functional dimension, and on the size of the smallest invariant containing a minimal functional definiton basis (defined by the "splitting formula"), can not be improved-upon in general.

Example1. Let L1 be the finite lattice, with the Hasse diagram depicted in figure 1.



Let L0 be the substructure defined by the closure of {a2,a3}. L0 can be depicted then by the diagram below. G(L1/L0) is the group of permutations on {a5,a6}, i.e, S_2



A Galois sub-Lattice (functionally closed)

Figure 1. A seven element Lattice

The size of a minimal set we must add to L0 in order to functionally define L1 is $1 \le \log_2 2 = 1$, while the smallest invariant we must consider is of size $\le 1 \times 2 = 2$. In this case we see that the upper bounds of theorem F—for the sizes of minimal basis and minimal invariant containing it— are both reached(and the possibe improvement indicated by the remark following theorem F does not materialise—since $\log_2(o(G(\mathfrak{A}/\mathfrak{A}_0)) \times [\, o(G(\mathfrak{A}/\mathfrak{A}_0) - \max\{r_i\}(2^{M-2} - 1)] = 1 \times [2 - 2(2^0 - 1)] = 2$).

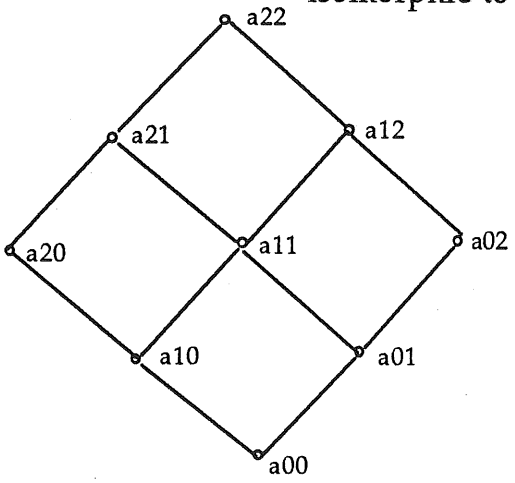
If Rxy is modelled by the partial order relation in the lattice ("x is connectedly lower than y"), then the 1-free-place formula, $Fz = Ra_4z \,\&\, Rza_1$, over L0 defines the invariant {a5,a6}. Both $\{a_1\}$ and $\{a_4\}$ are definable, respectively, in both L1 and L0 by

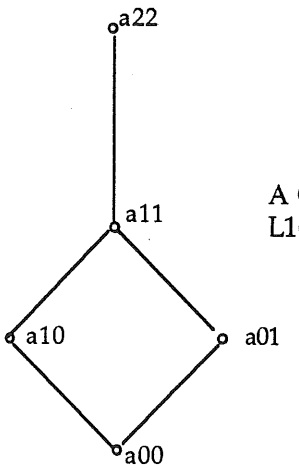
$\Psi_1(x) = (\forall u)\,(x = u \vee Rux)$ and

$\Psi_4(x) = (\exists w)(\exists u)(\exists v)(\forall y)\,(\forall z)[(y = w \vee Rwy) \,\&\, (z = u \vee z = v \vee z = w \vee (Ruz \,\&\, Rvz)) \,\&\, Rux \,\&\, Rvx \,\&\, (\neg Rux \vee \neg Rvx \vee Rxz)]$.

Example2. Let L2 be the finite lattice, with the Hasse diagram depicted in figure 2.

Let L0 be the substructure defined by the closure of {a10,a01}. L0 can be depicted then by the diagram below. G(L2/L0) is isomorphic to S2xS2. The full group G(L2) is isomorphic to the Abelian S2xS2xS2.





A Galois sub-Lattice L1(functionally closed)

An intermediate Galois substructure, L1, is isomorphic to the seven element lattice of the previous example. $|L1| = (L2-\{a20,a02\})$.

Figure 2. A Nine Element Lattice

The size, M-1, of a minimal set (for example, {a20,a21} we must add to L0 in order to functionally define L2 is $2 \leq \log_2(o(G(L2/L0)) = 2$, while the smallest invariant we must consider is of size 4, where by the emended formula of theorem F
$4 \leq \log_2(o(G(L2/L0)) \times [o(G(L2/L0) - \max\{r_i\}(2^{M-2} - 1)] = 2 \times [4 - 2(2^1 - 1)] = 4$,
since the automorphisms which move each element of the basis but not the other, are each of order 2. Notice that the upper bound provided by theorem F for this *size* of the smallest invariant we need (comparable to the degree of the polynomial for which a larger field is a "splitting field" of a given Galois subfield) is $\log_2(o(G(L2/L0)) \times o(G(L2/L0) = 8$, which is double the actual size! This invariant (comparable to the set of all solutions in the larger field of a certain polynomial over the smallest Galois subfield) is the set $S_m = \{a20,a02,a12, a21\}$.
If Rxy is modelled by the partial order relation in the lattice ("y is connectedly above x", in the diagram), then the 1-free-place formula over L0, $Fz = F_1z \vee F_2z$ defines S_m, where $F_1z = (Ra_{11}z \,\&\, Rza_{22})$, and $F_2z = \neg Ra11z \,\&\, \neg Rza11$. The fact that the defining formula of S_m, Fz, is a disjunction of two formulae F_1z and F_2z, each of which defines a certain minimal invariant, is completely analogous to the way a field constructed out of the roots of a polynomial over a base field can be constructed via an intermediate field, using at each stage a factor-polynomial. If f(x)=g(x)h(x), in a field, $f(x)=0 \iff (g(x)=0) \vee (h(x)=0)$.

Example 3. In the two previous examples the groups considered were all Abelian. We now consider a trivial case of non-commutative groups.

Let $\mathfrak{U}=<U, UxU>$ be a finite model, with n individuals, of the single statement $(\forall x)(\forall y)Rxy$.

Since every permutation is an automorphism, here, there are no invariants save $\emptyset$ and U^k, $k\geq 1$. Every domain of less than $n-1$ elements is a proper Galois subdomain (since for any such domain any two external elements can be interchanged by a 2-cycle, that keeps unmoved all the internal elements), but none of them, save $\emptyset$, is an invariant.

The subgroup $G(\mathfrak{U}/\{m_1,...,m_k\})$—where $\{m_1,...,m_k\}$ is any subset of $k< n$ different elements of U— is clearly isomorphic to S_{n-k} .

Thus, by lemmata 1.4 and 1.5, S_{n-k} will be a normal subgroup of S_n —for $1\leq k< n-1$—if and only if $\{1,...,k\}$ is an invariant, but since none of these subsets are invariant, we will have obtained the well known Group Theoretic fact that for $n\geq 3$, the sub-groups of S_n isomorphic to $S_2,...,S_{n-1}$, are not normal subgroups!

The functional degree of $\mathfrak{U}$ over the empty structure is n (since a minimal basis requires $n-1$ elements). The group of $\mathfrak{U}$ over $\emptyset$ is isomorphic to S_n and is of order $n!$, and we have, of course,

$\log_2 G(\mathfrak{U}/\emptyset)= \log_2 n! =\sum_{1\leq i\leq n}\log_2 i \geq (n-1)$ (with equality only when $n=1$ or2).

but according to the emendment on F we should have, for $n\geq 3$,

$n\leq \log_2 n!\ x\ [n!- 2(2^{n-2}- 1)]$, since n is the size of the minimal *invariant* needed to functionally generate U out of $\emptyset$ is n (size of U itself), but this is even more trivial than the previous inequality.

We note that according to Theorem E, some Abelian subgroup of S_n must have an order $\geq 2^{n-1}$. A direct proof of the existence of such a subgroup is slightly more tedious. It is possible to get much more interesting results of this sort by considering less trivial structures.

Consider the structure $\mathfrak{E}=<\{1,2,3,...,n\},\{1,2,...,m\}>$, where $m<n$, for a language with one extralogical monadic predicate symbol. The functional degree of $\mathfrak{E}$ over the empty structure is $n-1$ (since a minimal basis requires $n-2$ elements). The group of $\mathfrak{E}$ over $\emptyset$ is isomorphic to $S_m x S_{n-m}$ and is of order $m!x(n-m)!$, and we have

$\log_2 G(\mathfrak{E}/\emptyset)= \log_2 m! +\log_2(n-m)! =\sum_{1\leq i\leq m}\log_2 i + \sum_{1\leq i\leq n-m}\log_2 i$.

The minimum of the last sum is obtained when $m = n-m$. So we should have $2\log_2(n/2)! \geq n-2$, which is equivalent to $\log_2(n/2)! \geq n/2-1$ —the same weak inequality obtained before.

Example 4. The Symmetries of Trees.

A Tree $\mathcal{T}$ is a structure <A,R>, R⊆AxA, satisfying

(i) $(\exists!x)(\forall y)(x\neq y\rightarrow Rxy)$;

(ii) $(\forall x)(\forall y)(Rxy \rightarrow \neg Ryx)$;

(iii) $(\forall x)(\forall y)(\forall z)(Rxy\&Ryz \rightarrow Rxz)$; and

(iv) $(\forall x)(\forall y)(\forall w)(x\neq y\&Rxw\&Ryw \rightarrow Rxy \vee Ryx)$.

The individuals (members of A) are usually referred to as *nodes*.

'Rxy' is often read as "x is the*ancestor* of y".

Axioms (i)+(ii) guarantee that any tree will have a unique "base" node, without ancestors, which is an ancestor of every other node. There can be no "cycle" in a tree. (iv) guarantees that branches will never merge after separation.

In "discrete" trees (including all finite trees) there is a functional relationship of *immediate ancestry* (x *is a parent of* y: Pxy) applying to all nodes but the base node, and a relationship of *immediate descent* (x is *a child of* y: Cxy), applying to all except those without any descendents (*terminal* nodes). Thus $Pxy \Leftrightarrow_{Df} Rxy\&(\forall z)(Rzy\&x\neq z\rightarrow Rzx)$ and $Cxy \Leftrightarrow_{Df} Pyx$.

The mapping α: x—> {y | Ryx} is an isomorphism from <A,R> into a substructure of $<\wp(A),\subseteq>$, in which the base node is mapped on $\varnothing$. For each node **a** the set $\Phi(\mathbf{a})$= {x | x=**a** **v** Rax } is a subtree with **a** as a base node. Any subtree that can be defined so will be called *hereditarily complete*. The *family* of x, Fam(x), will be defined as $\alpha(x)\cup\Phi(x)$—i.e, the subtree obtained by grafting the subtree defined by x (as a base) on top of the gnealogical past line of x. Notice that while every family is a subtree the only hereditarily complete family is the entire original tree.

We will consider trees in which for every node the set of ancestors is well ordered by R. Call such trees *well-grown*. All finite trees are well-grown, of course.

For well-grown trees the *height* of a node is a mapping of the nodes into the ordinals, inductively defined by : h(x)=0 if x is the base node, h(x) = n+1 if $(\exists y)(h(y)=n \,\&\, Pyx)$, and h(x)=limsup{h(y) | Ryx}, otherwise. It is easily proved that this is a proper definition for well grown trees.

The *branching factor* of a node, x, is cardinality{y| Pxy}, i.e, the number of its "children".

A *laterally uniform* tree is a well grown one in which any two elements of the same height have the same branching factor.

It is fairly obvious that height and branching factor are preserved by any isomorphism.

One can prove the following properties of well grown trees:

(i). *A hereditarily complete subtree is an invariant iff there is no other such subtree isomorphic to it at the same height (of its base node).*

(ii). *The (unary) minimal invariants are exactly the sets of all nodes of equal height that belong to invariant, laterally uniform, subtrees.*

(iii). *A subtree is a Galois substree iff it is an invariant family of some node.*

Example 5. Standard and non-standard Models of Arithmetic.
We know that the standard model is Elementarily Invariant (since every singleton is definable), with a trivial Galois group. What about non-standard models? Is any of them Elementarily Invariant? The answer is negative.
Lemma: *A non-standard model of Arithmetic is not elementarily invariant.*
Proof. If any such model were EI, then every minimal invariant would be finite and definable. Let h be any infinite number and let f(x) be the arithmetical formula defining the minimal invariant containing it. Since f(h)& h>n, for any finite numeral n , then $(\exists x)(f(x)\ \&\ x>n)$ is satisfiable in the standard model for any finite numeral n, i.e, $(\forall n)(\exists x)(f(x)\ \&\ x>n)$ is true in the standard model. It follows that the minimal invariant containing h must already contain infinitely many standard "natural" numbers. Contradiction.

Corollary I. *Any non-standard countable model of arithmetic has an elementary extension in which it is moved by some automorphism onto another non-standard submodel of arithmetic.*

Corollary II. *In a non-standard model of arithmetic any finite definable subset is standard.*

The last corollary, reformulating the argument above, actually "demonstrates" the non-algebraic nature of any non-standard model—as an extension of the standard. For, inasmuch as any non-standard number can be dinstinguished from others by some arithmetical property, there must be infinitely many other (natural) numbers satisfying it. There are no irreducible predicates and no splitting structures (for finitary formulae).

A non-standard model of arithmetic must be of the order type $\omega+(\omega+\omega^{-})\lambda$, where λ is an order type of a dense linear set without first or last element. We can thus describe such a model as consisting of the natural integers followed by a dense ordered set of "blocks"—each of which is of the order type of the whole numbers—without a first or last block. It is clear that any automorphism α preserves the naturals, and that if it moves any infinite integer, it must move with it the whole block containing it. Suppose an infinite x is moved to $\alpha(x)$, then it is easy to prove that any finite number divides $\alpha(x) - x$, since $x \equiv n \pmod{m}$ implies $\alpha(x) \equiv n \pmod{m}$, when m is finite.