ON ALGEBRAS AND THEIR SPECTRA. THE CASE OF RINGS OF INTEGERS.

L. SHAHEEN AND B.ZILBER

Abstract. The paper is a part of the project which aims to construct a functor from a broadest possible category of algebras, seen as "coordinate algebras" to a category of "geometric structures", where the latter should be defined and analysed in terms of geometric stability theory. The introduction contains a brief survey of some completed steps of the project. Then we concentrate on the case of the rings of integers of number fields. According to Grothendieck one should think of $\mathbb{Z}$ as a coordinate algebras of $\mathrm{Spec}(\mathbb{Z})$, the spectrum. However, it is still not clear what geometry this object carries. A.Connes and C.Consani published recently an important paper which introduces a much more complex structure called *the arithmetic site* which includes $\mathrm{Spec}(\mathbb{Z})$.

Our approach produces a structure with distinctive geometric features which, in the big picture, is not inconsistent with Connes-Consani's.

The current version is quite basic. We describe a category of certain objects representing integral extensions of $\mathbb{Z}$ and establish its tight connection with the space of elementary theories of pseudo-finite fields. From model-theoretic point of view this category is a multisorted structure which we prove to be superstable with pregeometry of trivial type. It comes as some surprise that a structure like this can code a rich mathematics of pseudo-finite fields.

1. Introduction and the general framework

1.1. **Introduction.** The idea that the integers $\mathbb{Z}$, as an object of number-theoretic studies, could be better understood by associating a geometric object to it is an accepted point of view. Following A.Grothendieck one views $\mathbb{Z}$ as a potential "coordinate algebra" of a geometric object which one can refer to as $\mathrm{Spec}(\mathbb{Z})$. Conventionally, one thinks of $\mathrm{Spec}(\mathbb{Z})$ as a set of prime ideals of ring $\mathbb{Z}$ but it is not clear what *structure*, that is what relations and operations this set naturally acquires. In [10] Yu.Manin sets a sort of test question on what $\mathrm{Spec}(\mathbb{Z}) \times \mathrm{Spec}(\mathbb{Z})$ is. Manin also speculates in [10] on what $\dim \mathrm{Spec}(\mathbb{Z})$ could be (pointing to three possible answers arising in discussions, $1, 3$ and ∞).

A.Connes and C.Consani in a series of papers that go back to the 1990's developed a rich and interesting theory around this problem and more recently (see [1]) introduced and studied a relevant structure which they called *the arithmetic site*. Their construction builds the arithmetic site, following Grothendieck's prescriptions, as a topos in which "points" correspond to representations of the monoid $\mathbb{N}^{\times}$ of positive integers. The conventional $\mathrm{Spec}(\mathbb{Z})$ can be seen embedded in the arithmetic site.

Our work does not aim to counterpose the existing approaches but rather is a test for a quite general proposal for establishing duality between the broad category of "co-ordinate algebras", *Algebras*, and a category of "spectra", *Spectra*; the first one containing among others the rings of integers O_K. The object of the second category is

Date: 04 April 2018.

Key words and phrases. Spectrum of a ring, Zariski Geometry, Elimination of Quantifiers.

not easy to define in such a general context but model theory can suggest an answer. The answer is based on the notion of a Zariski geometry (Zariski structure) and has been first tested and studied in [13] by the second author for the category of *quantum algebras at roots of unity* which includes many non-commutative algebras as well as all commutative affine algebras (without nilpotent elements).

1.2. **Syntax and semantics.** The ideology of our approach is that objects R of the category *Algebras* encode a *syntactic* information and the respective object $\mathbf{M}_{\mathrm{R}} \in$ *Spectra* is an adequate *semantic, geometric* realisation of this information. To give a meaning to what *geometric* means in this context we suggest to use model-theoretic notion of Zariski structure, [15], and it generalisations. One might note here that the role that we assign to the notion of Zariski structures is in many ways equivalent (but possibly more narrow) to the role played by the Grothendieck topos.

A **Noetherian topological structure** in a language L is a (possibly multisorted) L-structure $\mathbf{M}$ with topologies τ_n on sorts of M^n, all n. The closed subsets of τ_n are subsets definable by quantifier-free positive L-formulas in n variables.

The topologies are assumed to be Noetherian.

Boolean combinations of closed sets are called constructible. The topologies τ_n for different n are linked by the condition: the projection of a closed subset of M^{n+1} into M^n is constructible.

A **Noetherian Zariski structure M** in a language L is a topological structure in a language L such that the expansion of $\mathbf{M}$ to the language $L(M)$ (adding a name to every point $p \in M$) is a Noetherian topological structure and:

To any constructible $L(M)$-subset S is assigned $\dim S$, a non-negative integer number, the dimension of S.

Dimension satisfies the following axioms. For $L(M)$- definable closed subsets S_1, S_2, S and point $p \in M$:

1. $\dim\{p\} = 0$, $\dim(S_1 \cup S_2) = \max\{\dim S_1, \dim S_2\}$.
2. If $S_1 \subsetneq S$ and $\dim S_1 = \dim S$ then there is $S_2 \subsetneq S$ such that $S = S_1 \cup S_2$.
3. Assuming $S \subseteq M^{n+1}$ is irreducible, $\mathrm{pr} : M^{n+1} \to M^n$, a projection,

$$\dim S = \dim \mathrm{pr} S + \min\{\dim \mathrm{pr}^{-1}(p) \cap S : p \in \mathrm{pr} S\}$$

and there is a relatively open subset $U \subseteq \mathrm{pr} S$ such that

$$u \in U \Rightarrow \dim \mathrm{pr}^{-1}(u) \cap S = \min\{\dim \mathrm{pr}^{-1}(p) \cap S : p \in \mathrm{pr} S\}.$$

We further define $\mathbf{M}$ to be a **Zariski geometry** if there is a 1-dimensional sort A in $\mathbf{M}$ which

(i) co-ordinatises any other sort X in $\mathbf{M}$, that is there are relatively open subsets $X^0 \subseteq X$, $Y \subseteq A^{\dim X}$ and finite-to-finite correspondence $R \subset X^0 \times Y$ given by positive formula;

(ii) A satisfies the *presmoothnes* condition: for every n, any closed irreducible $S_1, S_2 \subset A^n$ and an irreducible component $S_{1,2}$ of the intersection $S_1 \cap S_2$,

$$\dim S_{1,2} \geq \dim S_1 + \dim S_2 - n.$$

1.3. **The functor.** The functor $\mathrm{R} \mapsto \mathbf{M}_R$, when R is e.g. a semisimple finitely generated k-algebra finite over its centre, is defined as follows. We introduce a language L_{R} for 3 -sorted structures with sorts F, E and M. Elements of R become names of operator acting on E. The sort F has a field structure on it which we set to be isomorphic to $\bar{k}$, the algebraic closure of k. The language also has the name pr for a surjective map $E \to M$ such that the fibres $\mathrm{pr}^{-1}(q)$ of the map have structure of vector spaces with respect to a "+" in L_{R} and the multiplication $\cdot$ by elements of F. Moreover the fibres are invariant under the operators $a \in \mathrm{R}$ so that $\mathrm{pr}^{-1}(q)$ are R-modules. We then require that

(1) for each $q \in M$ the R-module $\mathrm{pr}^{-1}(q)$ is irreducible;
(2) $q_1 = q_2$ if and only if $\mathrm{pr}^{-1}(q_1) \cong \mathrm{pr}^{-1}(q_2)$ as R-modules;
(3) any isomorphism type of irreducible R-modules is represented by some $q \in M$.

It is proven in [13] that so defined $\mathbf{M}_{\mathrm{R}}$ is a Noetherian Zariski geometry. More precisely, [13] discussed only the case $k = \bar{k}$ but the argument goes through for the general case.

Note that the functor $\mathrm{R} \mapsto \mathbf{M}_{\mathrm{R}}$ is invertible since we can get back $\mathbf{M}_{\mathrm{R}} \to \mathrm{R}$ by reconstructing R as the algebra of Zariski-continuous (so, definable) operators on the vector bundle.

1.4. **The spectrum.** As suggested above (and in [13]) one should take the spectrum of R, Spec(R), to be the multisorted structure $\mathbf{M}$. Of course, then the answer to the question "what is Spec(R) $\times$ Spec(R)?" is: "the multisorted Zariski structure $\mathbf{M}_{\mathrm{R}} \times \mathbf{M}_{\mathrm{R}}$".

One can note that when R is an affine k-algebra, the vector fibration is equivalent to a trivial line bundle over the algebraic variety M defined over k with the coordinate algebra $k[M] = \mathrm{R}$. In this case $\mathbf{M}_{\mathrm{R}}$ is nicely bi-interpretable with the one-sorted structure induced on the sort M, which is just an algebraic variety over k and the conventional spectrum of R. The closed points of the affine k-scheme R are exactly the L_{R}-definable points of $\mathbf{M}_{\mathrm{R}}$.

This above construction works only for semisimple case. The more general case considered in [13] required a more general condition (1) in the construction of $\mathbf{M}_{\mathrm{R}}$:

(1') for each $q \in M$ the R-module $\mathrm{pr}^{-1}(q)$ is maximal indecomposable (into direct sum).

With this generalisation the construction covers the general case of quantum algebras at roots of unity (see the definition in [13]).

However, the class of quantum algebras at roots of unity does not include some important classes, e.g. affine (commutative) schemes of finite type with nilpotent elements (non-reduced schemes). This, key to algebraic geometry case has been studied by Alfonso Guido Ruiz in [6]. It turns out, as expected, that the construction similar to the one indicated in (1') gives a correct functor, an extension of the previous functor to the larger categories. Again, so defined $\mathbf{M}_{\mathrm{R}}$ is a Noetherian Zariski geometry.

1.5. **Towards the general case.** The same approach is expected to work in principle when R is an algebra in a very general case, e.g. a C^*-algebra or $*$-algebra (without assumption of it being a Banach algebra) or, on the opposite, R being just a ring or monoid. Of course, generalising in any of the directions one needs to generalise respectively the notion of Zariski structure, with a reasonable level of model-theoretic stability.

The case corresponding to the $*$-algebra R generated by operators P and Q satisfying the *canonical commutation relation*

$$QP - PQ = i\hbar$$

is treated in [4], [14] and in an ongoing work. The construction of $\mathbf{M}_{\mathrm{R}}$ for this case extends the method described above, in particular, replacing R by a category of non-commutative quantum algebras at roots of unity approximating R in a certain sense. Correspondingly, $\mathbf{M}_{\mathrm{R}}$ becomes a category of Noetherian Zariski structures with distinguished "real parts", equivalently a multisorted (with infinitely many sorts) Zariski structure. The crucial part of this construction, an additional sort, *the space of states* $\mathbb{S}$ with a homomorphism (called "limit")

$$\lim : \mathbf{M}_R \to \mathbb{S}$$

which projects the structure on $\mathbf{M}_{\mathrm{R}}$ onto $\mathbb{S}$. The induced structure on $\mathbb{S}$ is shown to be the well-known symplectic phase space of quantum mechanics with the action of time evolution operators for quadratic Hamiltonians.

It should be noted that this particular "geometric structure" $\mathbf{M}_R$ is complex enough to encode non-trivial number-theoretic relations, in the form of special Gauss quadratic sums. And in the limit form (on the sort $\mathbb{S}$) the sums are represented by oscillating Gaussian (quadratic) integrals. A work in progress develops calculations around higher order Gauss sums and oscillating integrals.

1.6. **On rings of integers.** The constructions and results presented in the short survey above provides us with a suggestion for the treatment of the spectrum of $\mathbb{Z}$ and, more generally, spectra of rings of integers O_K, or more precisely the multiplicative structure on O_K.

There are several serious reasons for avoiding the full ring structure in this context. First, the representation theory of rings naturally reduces to the representations on k-vector spaces and there is no natural good choice for the field k under the circumstances (a popular suggestion is to take k to be a "field of characteristic 1" which essentially amounts to the same suggestion of working with the monoid structure of O_K).

Another reason is that as long as we are interested in distribution of prime numbers and other aspects of multiplicative number theory, the additive structure on O_K may be irrelevant.

Finally, since we make use of the whole category of "algebras" O_K (similar to 1.5 above) morphisms between objects for different K should be definable in our structure in some geometric way. This, we believe, would not be compatible with preserving the additive structure of the K.

1.7. **Our structure.** We construct a multi-sorted structure $\mathfrak{M}$ which as a whole is to be seen as a geometric structure corresponding to the category of rings of integers O_K, for number fields K. This type of "geometric" structure is closest to $\mathbf{M}_{\mathrm{R}}$ reviewed in subsection 1.5. However, the current version is minimalist; the potential of richer versions is discussed in the final "Concluding remarks and further direction" section of the paper.

For each K is given a 2-sorted substructure (A_K, Sp_K) with surjection $\mathrm{pr} : A_K \to \mathrm{Sp}_K$ which can be read as a set of "points" Sp_K with a structure over each point $\mathfrak{p}$ given on the fibre $\mathrm{pr}^{-1}(\mathfrak{p})$. (Note that we deliberately have chosen the notation Sp_K to distinguish from the more common $\mathrm{Spec}(O_K)$. In fact, the latter will be determined, in accordance with 1.4, as Sp_K along with the fibration given by pr.)

Each element $m \in O_K$ defines an action on the fibre. We define a certain "Zariski" topology on the sorts of the structure and their cartesian products. We then can identify the set of all the $m \in O_K$ with the set of operators

$$m : A_K \to A_K, \quad \mathrm{pr}^{-1}(p) \to \mathrm{pr}^{-1}(p).$$

The structure on fibres of the projection, $\mathrm{pr}^{-1}(\mathfrak{p})$ can be obtained as the reducts of structure of a one-dimensional vector space over $\mathbb{F}_{\mathfrak{p}} = O_K/\mathfrak{p}$, which ignores the additive structure of the vector space and is essentially a representations of the monoid O_K.

Objects (A_K, Sp_K), which we call *arithmetic planes* over respective number fields, are linked together into a category by morphisms

$$\pi_{K,L} : A_K \to A_L \text{ for } K \supseteq L,$$

which on each fibre $\mathrm{pr}^{-1}(\mathfrak{p})$ shadows the norm map $\mathbb{F}_{\mathfrak{p}} \to \mathbb{F}_{\mathfrak{q}}$, for $\mathfrak{p} \supseteq \mathfrak{q}$, prime ideals of respective rings.

This defines the multisorted structure, the object of our model-theoretic analysis. Before stating results of this analysis we must note that it is not difficult to see that this structure is definable in the ring of finite adeles, well undersood object of model theory, in particular studied recently in much detail by J.Derakhshan and A.Macintyre, see [5] and their forthcoming papers. These studies of the rings of adeles shed some light at our structure but do not explain the limits of expressive power of our language.

Our main theorem states that the theory of the structure is superstable and allows elimination of quantifiers to certain family of core formulas of geometric flavour. This is not very surprising given that the structure is defined in terms of very simple relations, and indeed the only definable subsets on each spectral sort Sp_K are certain unary predicates. However, the language of the structure has quite a considerable expressive power: we prove that to any point $v \in \mathrm{Sp}_K$ in a model of the theory one can associate a pseudo-finite field $\mathbb{F}_v$ so that

$$\mathrm{tp}(v) = \mathrm{tp}(w) \text{ if and only if } \mathbb{F}_v \equiv \mathbb{F}_w, \quad v, w \in \mathrm{Sp}_K$$

where the elementary equivalence is in the language of fields extended by the names of its algebraic elements.

The quantifier-elimination theorem allows to define a natural topology on the multi-sorted structure and determine the dimensions (which we take to be just the U-ranks) of closed, and more generally definable, subsets. In particular,

$$\mathrm{U}(\mathrm{Sp}_K) = 1, \quad \mathrm{U}(A_K) = 2, \ \mathrm{U}(\mathrm{pr}^{-1}(p)) = 1$$

for any number field K and any $p \in \mathrm{Sp}_K$. If we take the dimension to be the Morley rank then the first two values are equal to ∞ and $\mathrm{MR}(\mathrm{pr}^{-1}(p))$ is finite (so our analysis explains two of the three versions of dimension of $\mathrm{Spec}(\mathbb{Z})$ suggested by Yu.Manin in [10]).

Another interesting result is that a large subalgebra of the boolean algebra of definable subsets on a sort Sp_K can be given a probabilistic measure, which is just the *natural* or *analytic density* in the sense of number theory. We don't know if this measure is well-defined on all definable subsets.

We note that the topology is not Noetherian and that in the standard model the arithmetic planes A_K and the spectral line Sp_K are not compact. However, we find that there are compact models and determine the minimal compact model. This model has finitely many non-standard (infinite) primes in each Sp_K, more precisely, the number is equal to $\deg K/\mathbb{Q}$, and these primes w are characterised by the property that any polynomial over $\mathbb{Z}$ splits into linear factors in $\mathbb{F}_w$.

Acknowledgement. We would like to express our gratitude to the referee whose thorough analysis accompanied by constructive criticism made us to essentially revise the first version of the paper.

We are also grateful to J.A. Cruz Morales who read the paper and made many useful comments.

2. A bundle over the spectrum of O_K

All fields K below are number fields and rings are O_K, the integers of the fields. We generally assume that the fields belong to a collection $\mathcal{R}$ closed under intersections such that for any $K, L \in \mathcal{R}$ an embedding $L \subset K$ is Galois. By default we assume that the minimal object in $\mathcal{R}$ is $\mathbb{Q}$ but in general it could be any number field.

The spectrum of a ring O_K, $\mathrm{Spec}(O_K)$, is the collection of all prime ideals of O_K. Equivalently, for Dedekind rings, the collection of maximal ideals $\mathrm{maxSpec}(O_K)$, together with the zero ideal. We denote for brevity

$$\mathrm{Sp}_K := \mathrm{maxSpec}(O_K),$$

equivalently, the collections of irreducible representations of O_K. This will be our main universe, a geometric space (of closed points), which agrees with the notion of universe for a Zariski geometry, see [15]. Note that when we introduce a "Zariski" topology on Sp_K this universe as a whole is assumed to be closed, which in scheme-theoretic terms amounts to take the zero ideal into account.

The maximal (that is non-zero prime) ideals we call points of Sp_K and often just say points of the spectrum.

However, we want to consider the O_K as monoids and to every point p of Sp_K we put in correspondence an irreducible O_K-module $\lceil \mathrm{F}_p \rceil$ which we consider as a monoid-module, that is we ignore the additive structure on $\lceil \mathrm{F}_p \rceil$ but do distinguish the zero element $0 \in \lceil \mathrm{F}_p \rceil$.

Since K acts on $\lceil \mathrm{F}_p \rceil$ as O_K/p and p is maximal, $O_K/p \cong \mathbb{F}_q$, a finite Galois field, $q = q(p) = \ell^n$ for some prime ℓ which depend on K and p. So, choosing a non-zero $a_p \in \lceil \mathrm{F}_p \rceil$ we can identify $\lceil \mathrm{F}_p \rceil$ with $\mathbb{F}_q.a_p$, where the action of $\mathbb{F}_q^*$ on $\lceil \mathrm{F}_p^* \rceil = \lceil \mathrm{F}_p \rceil \setminus \{0\}$ is free.

The characteristic property of $\lceil \mathrm{F}_p \rceil$ is that

$$\mathrm{Ann}(\lceil \mathrm{F}_p \rceil) = p,$$

the annihilator of $\lceil \mathrm{F}_p \rceil$ (in fact, of any non-zero point in $\lceil \mathrm{F}_p \rceil$) is equal to the ideal in O_K generated by p.

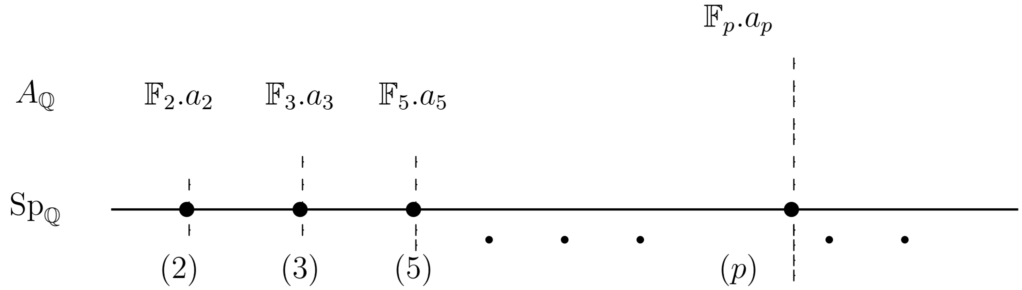
2.1. **The arithmetic plane over K.** We define the 2-sorted (standard) universe (A_K, Sp_K) with the projection

$$\mathrm{pr} : A_K \setminus \{0\} \to \mathrm{Sp}_K$$

where

$$A_K := \bigcup_p \lceil \mathrm{F}_p \rceil \text{ and } \mathrm{pr}(x) = p \leftrightarrow x \in \lceil \mathrm{F}_p \rceil.$$

see the picture for $K = \mathbb{Q}$, $O_K = \mathbb{Z}$ below.



We think about A_K as an **arithmetic plane over** K and Sp_K the horizontal axis of the plane.

Thus, the $\lceil \mathrm{F}_p^* \rceil$ are fibres of the projection. Note that for each standard fibre $O_K \cdot a_p = \lceil \mathrm{F}_p \rceil$, but this is not first-order expressible uniformly in p.

We call the structure described above $\mathrm{Rep}(O_K)$, the representations of the monoid O_K.

We summarise: the language L_K of $\mathrm{Rep}(O_K)$ has two sorts, A_K and Sp_K, names for unary operations $m : x \mapsto mx$ for elements $m \in K$, and the map $\mathrm{pr} : A_K \to \mathrm{Sp}_K$.

Remark. We can equivalently represent $\mathrm{Rep}(O_K)$ in a one-sorted way, with just a sort A_K with equivalence relation E instead of pr, such that the equivalence classes are exactly the $\lceil \mathrm{F}_p \rceil$.

2.2. **Topology.** To every ideal $m \subset O_K$ we associate the $\emptyset$-definable subset $\mathcal{S}_m = \{x \in A_K : \mathrm{An}(x) \supseteq m\}$, equal to $\bigcup_{p|m} \lceil \mathrm{F}_p \rceil$. Since every m is finitely generated, the latter is a union of finitely many orbits.

We call such sets and finite union of those **closed in** A_K.

Along with this topology on A_K we define a topology on Sp_K with the basis of closed sets of the form $\mathrm{pr}(\mathcal{S}_m)$.

We will refer to as the *conventional* Zariski topology on A_K and Sp_K.

It is not hard to prove the following statement which will be superseded by Theorem 4.14.

Proposition. *The complete first-order theory of* $\mathrm{Rep}(O_K)$ *has an explicit axiomatisation* $T(K)$. *The theory admits elimination of quantifiers. This theory is* ω*-stable of finite Morley rank. The sort* Sp_K *is strongly minimal and of trivial type. The sort* A_K *is of Morley rank* 2 *and the fibres of* pr *are either finite or strongly minimal.*

3. The Multi-Sorted Structure of Representations

3.1. **The language.** In this section we present a construction of a multi-sorted structure with sorts of the form A_K, Sp_K where K runs through a family $\mathcal{R}$ of (by default all) number fields.

The language $L_{\mathcal{R}}$ of the **multisorted representation structure** $\mathrm{Rep}(\mathcal{R})$ will be the union of the languages L_K, $K \in \mathcal{R}$, extended by maps $\pi_{K,L} : A_K \to A_L$, for $K, L \in \mathcal{R}$, $\mathrm{O}_L \subseteq \mathrm{O}_K$.

3.2. **Notation.** Let $\mathfrak{q}, \mathfrak{p} \subset O_K$ and $q, p \subset O_L$ are prime ideals of the corresponding rings $O_L \subseteq O_K$ such that $\mathfrak{q} \supset q$ and $\mathfrak{p} \supset p$. Throughout this paper we use notations for $\mathfrak{q}, \mathfrak{p} \subset O_K$ and $q, p \subset O_L$ such that

$$\mathfrak{q} \supseteq q, \mathfrak{p} \supset p \tag{1}$$

that is always "$\mathfrak{q}$ lies over q and $\mathfrak{p}$ lies over p in O_K".

We will also use notation for definable maps

$$\pi^{\mathrm{Sp}}_{K,L} : \mathrm{Sp}_K \to \mathrm{Sp}_L$$

defined by

$$\pi^{\mathrm{Sp}}_{K,L}(\mathfrak{q}) = q \Leftrightarrow \lceil \mathrm{F}_{\mathfrak{q}} \rceil \subseteq \pi^{-1}_{K,L}(\lceil \mathrm{F}_q \rceil).$$

Recall that the ring homomorphism

$$\mathrm{res}_{\mathfrak{q}} : \mathrm{O}_K \to \mathrm{O}_K/\mathfrak{q} =: \mathbb{F}_{\mathfrak{q}}$$

can be seen as a residue map (or place) for a valuation of K with the value ring equal to O_K and the valuation ideal equal to $\mathfrak{q}$. Here $\mathbb{F}_{\mathfrak{q}} \cong \mathbb{F}_{q^m}$ for some positive integer m, which depends on K. We define

$$|\mathfrak{q}| := q^m.$$

Note that if $K : L$ is Galois, acting by a Galois automorphism on K we move $\mathfrak{q}$ to some $\mathfrak{q}^{'} \subset \mathrm{O}_K$. In this sense $\mathfrak{q}'$ runs through all prime ideals of O_K which are Galois-conjugated to $\mathfrak{q}$, while $\mathbb{F}_{\mathfrak{q}'} \cong \mathbb{F}_{q^m}$ with the same m.

We will often refer to $\mathrm{res}_{\mathfrak{q}}$ as a **naming homomorphism** as it associates elements $\gamma \in \mathrm{O}_K$ (which we see as "names") with elements in $\lceil \mathbb{F}_{\mathfrak{q}} \rceil$.

3.3. **Orbits.** For each prime ideal $\mathfrak{q}$ we associate a unique orbit $\lceil \mathrm{F}_{\mathfrak{q}} \rceil$ on which O_K acts, for each $\gamma \in O_K \setminus \mathfrak{q}$ and $x \in \lceil \mathrm{F}_{\mathfrak{q}} \rceil$

$$x \mapsto \gamma \cdot x \in \lceil \mathrm{F}_{\mathfrak{q}} \rceil$$

and $\gamma \cdot x = 0$ (a common zero) iff $\gamma \in \mathfrak{q}$. By definition we assume

$$\gamma_1 \cdot x = \gamma_2 \cdot x \text{ iff } \gamma_1 - \gamma_2 \in \mathfrak{q}$$

and we assume that the action is transitive. Thus, by definition, for any $\gamma \in O_K$ and $a \in \lceil \mathrm{F}_{\mathfrak{q}} \rceil$,

$$\gamma \cdot a = \bar{\gamma}_{\mathfrak{q}} \cdot a \tag{2}$$

where $\bar{\gamma}_{\mathfrak{q}} \in \mathbb{F}_{\mathfrak{q}}$, the element with the name γ.

3.4. **Corollary.** For $\mathfrak{q}, \mathfrak{q}' \in \mathrm{Sp}_K$

$\mathfrak{q} = \mathfrak{q}'$ **iff** for any $\gamma_1, \gamma_2 \in O_K \, \forall x \in \lceil \mathrm{F}_{\mathfrak{q}} \rceil \, \forall x' \in \lceil \mathrm{F}_{\mathfrak{q}'} \rceil \; \gamma_1 \cdot x = \gamma_2 \cdot x \leftrightarrow \gamma_1 \cdot x' = \gamma_2 \cdot x'$.

Note also that, given $\mathfrak{q}'' \in Sp_K$, $a \in \lceil \mathrm{F}_{\mathfrak{q}''} \rceil$ we can represent any element $b \in \lceil \mathrm{F}_{\mathfrak{q}''} \rceil$ as

$$b = \bar{\gamma}_{\mathfrak{q}''} \cdot a, \text{ for some } \bar{\gamma}_{\mathfrak{q}''} \in \mathbb{F}_{\mathfrak{q}''}.$$

We will also write accordingly

$$\lceil \mathrm{F}_{\mathfrak{q}''} \rceil = \mathbb{F}_{\mathfrak{q}''} \cdot a_{\mathfrak{q}}$$

where $\mathfrak{q}'' \mapsto a_{\mathfrak{q}''}$ is a cross-section $\mathrm{Sp}_K \to A_K$.

3.5. **Morphisms between sorts.** Let $\mathrm{Norm}_{K,L} : \mathbb{F}_{\mathfrak{q}} \to \mathbb{F}_q$ be the norm map. Define, the morphisms

$$\pi_{K,L} : A_K \to A_L$$

by its action on each orbit

$$\pi_{K,L} : \lceil \mathrm{F}_{\mathfrak{q}} \rceil \to \lceil \mathrm{F}_q \rceil,$$

for each prime $\mathfrak{q}$ over q, which is defined once the sections $a_{\mathfrak{q}} \in \lceil \mathrm{F}_{\mathfrak{q}} \rceil$ and $a_q \in \lceil \mathrm{F}_q \rceil$ are given: for $\eta \in \mathbb{F}_{\mathfrak{q}}$

$$\pi_{K,L}(\eta \cdot a_{\mathfrak{q}}) := \mathrm{Norm}_{K,L}(\eta) \cdot a_q.$$

Note that this definition applies to all primes $\mathfrak{q}'$ in O_K over q and morphisms

$$\pi_{K,L} : \lceil \mathrm{F}_{\mathfrak{q}'} \rceil \to \lceil \mathrm{F}_q \rceil.$$

3.6. **Remark.** It is crucial for the definition of morphisms $\pi_{K,L}$ that we treat the O_K as monoids (not rings), that is there is no additive structure on the fibres $\lceil \mathrm{F}_{\mathfrak{q}} \rceil$.

<u>**Naming homomorphisms**</u>:

$$\begin{tikzcd}
 & & \mathrm{O}_K \arrow[dll, "\mathrm{res}_{\mathfrak{q}}"'] \arrow[d, "\mathrm{res}_{\mathfrak{q}'}"] \arrow[drr, "\mathrm{res}_{\mathfrak{q}''}"] & & \\
\mathbb{F}_{\mathfrak{q}} \arrow[drr, "\mathrm{Norm}_{K,L}"'] & \cdots\cdots & \mathbb{F}_{\mathfrak{q}'} \arrow[d, "\mathrm{Norm}_{K,L}"'] & \cdots & \mathbb{F}_{\mathfrak{q}''} \arrow[dll, "\mathrm{Norm}_{K,L}"] \\
 & & \mathbb{F}_q & &
\end{tikzcd}$$

3.7. **Lemma.** *The action of* O_K *on* $\lceil \mathrm{F}_{\mathfrak{q}} \rceil$ *induces via* $\pi_{K,L}$ *an action of* O_K *on* $\lceil \mathrm{F}_q \rceil$.

This action extends the action of O_L *on* $\lceil \mathrm{F}_q \rceil$.

This action does not depend on the sections $a_{\mathfrak{q}}$ *and* a_q.

Proof. Given $\gamma \in \mathrm{O}_K$ and $b \in \lceil \mathrm{F}_q \rceil$ define

$$\gamma \cdot_{\mathfrak{q}} b := \mathrm{Norm}_{K,L}(\bar{\gamma}_{\mathfrak{q}}) \cdot b. \tag{3}$$

This is clearly an action since norm is multiplicative. We will write it without the subscript $\mathfrak{q}$ when the latter is clear from the context.

For $\gamma \in \mathrm{O}_L$ we have $\bar{\gamma}_{\mathfrak{q}} \in \mathbb{F}_q$ and $\bar{\gamma}_{\mathfrak{q}} = \bar{\gamma}_q$ since $\mathfrak{q} \cap \mathrm{O}_L = q$. Hence $\mathrm{Norm}_{K,L}(\bar{\gamma}_{\mathfrak{q}}) = \bar{\gamma}_q$ for such γ and so this is its usual action. Clearly, it does not depend on the choice of sections.

Now we show that the $\pi_{K,L}$ preserve the action by O_K, that is

$$\pi_{K,L}(\gamma \cdot a_{\mathfrak{q}}) = \gamma \cdot \pi_{K,L}(a_{\mathfrak{q}}) = \gamma \cdot a_q. \tag{4}$$

Indeed, by definition $\gamma \cdot a_q = \mathrm{Norm}_{K,L}(\bar{\gamma}_{\mathfrak{q}}) \cdot a_q$, $\pi_{K,L}(\bar{\gamma}_{\mathfrak{q}} \cdot a_{\mathfrak{q}}) = \mathrm{Norm}_{K,L}(\bar{\gamma}_{\mathfrak{q}}) \cdot a_q$ and $\gamma \cdot a_{\mathfrak{q}} = \bar{\gamma}_{\mathfrak{q}} \cdot a_{\mathfrak{q}}$. The equality follows. $\square$

3.8. **Remark.** The definition of the action can equivalently be written as

$$\gamma \cdot_{\mathfrak{q}} b := \mathrm{Norm}_{K,L}(\mathrm{res}_{\mathfrak{q}}(\gamma)) \cdot b.$$

3.9. **Corollary.** *The actions $\cdot_{\mathfrak{q}}$ and $\cdot_{\mathfrak{q}'}$ on $\lceil \mathrm{F}_q \rceil$ by O_K coincide if and only if $\mathfrak{q}' = \mathfrak{q}$.*

Indeed, to see that the actions differ when $\mathfrak{q}' \neq \mathfrak{q}$ consider a $\gamma \in \mathfrak{q}' \setminus \mathfrak{q}$. Then by definition for any $b \in \lceil \mathrm{F}_q \rceil$, $\gamma \cdot_{\mathfrak{q}'} b = 0$ and $\gamma \cdot_{\mathfrak{q}} b \neq 0$.

3.10. **Remark.** Note also that $\mathrm{Norm}_{K,L}$ can be alternatively defined as the map

$$\mathrm{Norm}_{K,L}(x) = x^{\frac{|\mathfrak{q}|-1}{|q|-1}}.$$

It follows that for a non-zero $y \in \lceil \mathrm{F}_q \rceil$

$$|\pi_{K,L}^{-1}(y) \cap \lceil \mathrm{F}_{\mathfrak{q}} \rceil| = \frac{|\mathfrak{q}|-1}{|q|-1}. \tag{5}$$

Now note that one can determine, for $y \in A_L$, the number $|\pi_{K,L}^{-1}(y)|$ once one knows that $y \in \lceil \mathrm{F}_q \rceil$ and one knows all the $\mathfrak{q}'$ which lie over q in O_K.

3.11. **Special predicates on** Sp_L**.** We consider the $\pi_{K,L}$-**multiplicities** of primes $\mathfrak{p} \in \mathrm{Sp}_L$.

Define for positive integers N the binary relation $P_{K,L}^N \subset \mathrm{O}_K \times \mathrm{O}_L$ by the first order formula:

$$P_{K,L}^N(\mathfrak{q}, q) \equiv \exists y \in \lceil \mathrm{F}_q \rceil \ |\pi_{K,L}^{-1}(y) \cap \lceil \mathrm{F}_q \rceil| \leq N.$$

Note that by the definition of $\pi_{K,L}$ it follows that $P_{K,L}^N(\mathfrak{q}, q)$ implies $q \subseteq \mathfrak{q}$.

3.12. **Lemma.** *Let $L \subseteq K$, $q \in \mathrm{Sp}_L$, $\mathfrak{q} \in \mathrm{Sp}_K$, and assume that $P_{K,L}^N(\mathfrak{q}, q)$ holds. Then*

(i) $N \geq \frac{|q|^{|\mathbb{F}_{\mathfrak{q}}:\mathbb{F}_q|}-1}{|q|-1}$.

(ii) *In particular, there exists N such that $P_{K,L}^N(\mathfrak{q}, q)$ holds for infinitely many $q \in \mathrm{Sp}_L$ with some extension $q \subseteq \mathfrak{q} \in \mathrm{Sp}_K$ if and only if $|\mathbb{F}_{\mathfrak{q}} : \mathbb{F}_q| = 1$ for all but finitely many of pairs $\mathfrak{q}, q$.*

(iii) *If there exists N such that $P_{K,L}^N(\mathfrak{q}, q)$ holds for infinitely many $q \in \mathrm{Sp}_L$ with some extension $q \subseteq \mathfrak{q} \in \mathrm{Sp}_K$ then $P_{K,L}^1(\mathfrak{q}, q)$ holds for all but finitely many pairs $\mathfrak{q}, q$ satisfying $P_{K,L}^N(\mathfrak{q}, q)$.*

Proof. (i) This quantative estimate is a direct consequence of (5).

(ii) $|q|$ is unbounded when q runs in an infinite subset of Sp_L.

(iii) $|\mathbb{F}_{\mathfrak{q}} : \mathbb{F}_q| = 1$ is equivalent to the statement that $\pi_{K,L}$ induces a bijection $\lceil \mathrm{F}_{\mathfrak{q}} \rceil \to \lceil \mathrm{F}_q \rceil$. $\square$

3.13. **Remark.** The case $|\mathbb{F}_{\mathfrak{q}} : \mathbb{F}_q| = 1$ corresponds to the fact that $\mathbb{F}_{\mathfrak{q}} \cong \mathbb{F}_q$ for the prime $\mathfrak{q} \in \mathrm{Sp}_K$ over the prime $q \in \mathrm{Sp}_L$. In case when K is Galois over L this means that the minimal polynomial of α over L splits into linear factors modulo q. Then, except for finitely many such q (over which $\mathfrak{q}$ ramifies) there are exactly $|K : L|$ distinct prime ideals $\mathfrak{q}$ over q.

3.14. Define

$$\Pi_{K,L} := \{q \in \mathrm{Sp}_L :\ \exists \mathfrak{q} \in \mathrm{Sp}_K\ q \subseteq \mathfrak{q}\ \&\ \mathbb{F}_\mathfrak{q} \cong \mathbb{F}_q\}$$

$$\Psi_{K,L} := \{q \in \mathrm{Sp}_L :\ \forall \mathfrak{q} \in \mathrm{Sp}_K\ q \subseteq \mathfrak{q}\ \rightarrow\ \mathbb{F}_\mathfrak{q} \cong \mathbb{F}_q\}$$

By 3.12 both are first order definable (using $P^1_{K,L}(\mathfrak{q}, q)$).

Note that $q \in \Psi_{K,L}$ if and only if every extension $\mathfrak{q}$ of q to O_K splits completely.

We will show later (see 4.10 and 4.12) that $\Psi_{K,L}$ can be expressed essentially in terms of $\Pi_{K,L}$.

3.15. Lemma. *Suppose K and K' are Galois conjugated extensions of L. Then*

$$\Pi_{K,L} = \Pi_{K',L}.$$

Proof. Let $g : K \to K'$ be an isomorphism over L. Suppose $q \in \Pi_{K,L}$ and so for some $\mathfrak{q} \in \mathrm{Sp}_K$ over q, $\mathrm{O}_K/\mathfrak{q} \cong \mathrm{O}_L/q$. Then $\mathrm{O}_{K'}/\mathfrak{q}' = g(\mathrm{O}_K)/g(\mathfrak{q}) \cong \mathrm{O}_L/q$ Hence $q \in \Pi_{K',L}$. □

3.16. Galois action on the spectra. Let $\alpha_1, \ldots, \alpha_k$ be the generators of the ring O_K over O_L and $\sigma \in \mathrm{Gal}(K : L)$. Let $\alpha_1^\sigma, \ldots, \alpha_k^\sigma$ be the result of application of σ to the generators.

Consider the formula with free variables $\mathfrak{q}, \mathfrak{q}'$ in sort Sp_K :

(6)

$$\exists x, x' \in A_K :\ \mathrm{pr}(x) = \mathfrak{q}\ \&\ \mathrm{pr}(x') = \mathfrak{q}'\ \&\ \pi_{K,L}(x) = \pi_{K,L}(x')\ \&\ \bigwedge_{l=1}^{k} \pi_{K,L}(\alpha_l x) = \pi_{K,L}(\alpha_l^\sigma x')$$

Lemma.[1] *Given $\mathfrak{q} \in \mathrm{Sp}_K$ such that $\pi^{\mathrm{Sp}}_{K,L}(\mathfrak{q}) \in \Psi_{K,L}$ the formula (6) holds for $\mathfrak{q}' \in \mathrm{Sp}_K$ if and only if $\mathfrak{q}' = \mathfrak{q}^\sigma$.*

Proof. Suppose (6) does hold. Then $q := \pi^{\mathrm{Sp}}_{K,L}(\mathfrak{q}) = \pi^{\mathrm{Sp}}_{K,L}(\mathfrak{q}')$.[2]

Under our assumptions $\mathrm{Norm}_{\mathbb{F}_\mathfrak{q},\mathbb{F}_q} : \mathbb{F}_\mathfrak{q} \to \mathbb{F}_q$ is an isomorphism and definition (3) implies that for any $\alpha \in O_K$,

$$\pi_{K,L}(\alpha \cdot x) = \bar{\alpha}_q \cdot y, \quad \text{for } y := \pi_{K,L}(x),$$

where $\bar{\alpha}_\mathfrak{q} = \mathrm{res}_\mathfrak{q}(\alpha) \in \mathbb{F}_q$.

Since $\pi_{K,L}(\alpha x) = \pi_{K,L}(\alpha^\sigma x')$, we get that

$$\bar{\alpha}_\mathfrak{q} = \bar{\alpha^\sigma}_{\mathfrak{q}'}$$

for all $\alpha \in O_K$. In particular,

$$\alpha \in \ker(\mathrm{res}_\mathfrak{q}) \Leftrightarrow \alpha^\sigma \in \ker(\mathrm{res}_{\mathfrak{q}'}).$$

But $\ker(\mathrm{res}_\mathfrak{q}) = \mathfrak{q}$ and $\ker(\mathrm{res}_{\mathfrak{q}'}) = \mathfrak{q}'$, that is $\mathfrak{q}' = \mathfrak{q}^\sigma$. □

[1]We should be able to write down a formula which defines an action of σ on A_K (not just Sp_K) without the restriction to $\psi_{K,L}$.

[2]In particular, we can write the formula (6) so that all the variables are relativised to $\mathrm{cl}(p)$.

4. The quantifier elimination theorem

In this section we discuss the relationship between the spectra of rings of integers on the one hand side, and the space of (elementary) theories of pseudo finite fields. The latter is of course well understood due to the work of J. Ax and was studied in other contexts by [8] and [7]. The main distinction in our study is that we work in a different language.

4.1. The space of finite fields. The multisorted structure $\mathcal{PF}$, *a space of finite fields,* consists of sorts $\mathcal{PF}_K$, $\mathcal{AF}_K$ for number fields K, with a surjective map

$$\mathrm{pr} : \mathcal{AF}_K \to \mathcal{PF}_K.$$

As was noted in subsection 3.2 a unital homomorphism $\mathrm{res} : \mathrm{O}_K \to \mathbb{F}_{\mathfrak{q}}$ can be seen as assigning names in O_K to elements in $\mathbb{F}_{\mathfrak{q}}$. We will consider elements of O_K as extra constant symbols and $\mathbb{F}_{\mathfrak{q}}$ a structure in the **language of rings with names in** O_K. We denote the language $L_{\text{rings}}(K)$.

The fibre $\mathrm{pr}^{-1}(\mathfrak{q})$ over a point $\mathfrak{q} \in \mathcal{PF}_K$, has a structure given by the language $L_{\text{rings}}(K)$ that can be identified with a finite field $\mathbb{F}_{\mathfrak{q}}$ (later, in 4.4, a pseudofinite field) with names in O_K.

We assume that for finite $\mathbb{F}_{\mathfrak{q}}$,

$$\mathbb{F}_{\mathfrak{q}} \cong \mathbb{F}_{\mathfrak{q}'} \Leftrightarrow \mathfrak{q} = \mathfrak{q}' \tag{7}$$

We also assume that,

$$\text{for every prime } \mathfrak{q} \subset \mathrm{O}_K \text{ there is } \mathcal{Q} \in \mathcal{PF}_K \text{ such that } \mathbb{F}_{\mathfrak{q}} = \mathbb{F}_{\mathcal{Q}} := \mathrm{O}_K/\mathfrak{q}. \tag{8}$$

There are maps

$$\mathrm{Nm}_{K/L} : \mathcal{AF}_K \to \mathcal{AF}_L, \quad j_{K/L} : \mathcal{AF}_L \to \mathcal{AF}_K \text{ for } \mathrm{O}_K \supseteq \mathrm{O}_L$$

between sorts, defined fibrewise as

$$\mathrm{Norm}_{K/L} : \mathbb{F}_{\mathfrak{q}} \to \mathbb{F}_q, \quad j_{K/L} : \mathbb{F}_q \to \mathbb{F}_{\mathfrak{q}} \text{ for } \mathbb{F}_{\mathfrak{q}} \supseteq \mathbb{F}_q. \tag{9}$$

where $j_{K/L}$ is the canonical embedding.

Note that

$$\mathrm{Nm}_{K/L} \text{ is surjective} \tag{10}$$

since every prime $q \subset \mathrm{O}_L$ can be lifted to a prime $\mathfrak{q} \subset \mathrm{O}_K$.

We also assume that

$$\mathbb{F}_{\mathfrak{q}} = \mathbb{F}_q(\bar{\alpha}), \text{ for } \alpha \text{ such that } K = L(\alpha) \tag{11}$$

where $\bar{\alpha} = \mathrm{res}_{\mathfrak{q}}(\alpha)$.

4.2. Remarks. (i) Note that $\mathbb{F}_{\mathfrak{q}}$ is determined by (11) uniquely, up to the naming, and we have one-to-one correspondence between extensions of $\mathbb{F}_q$ in the language $L_{\text{rings}}(K)$ and the residue maps $\mathrm{res}_{\mathfrak{q}}$.

(ii) The assumptions (7)–(11) are first-order axiom schemes of spaces of pseudofinite fields. The axioms (7) and (8) are written for each finite $\mathfrak{q}$ separately.

4.3. Lemma. *There exists a bijection*

$$\mathbf{i}: \ A_K \to \mathcal{AF}_K, \quad \mathrm{Sp}_K \to \mathcal{PF}_K, \quad \textit{for all } K$$

between the (standard) multisorted representation structure (A_K, Sp_K) *(section 3) and the space of finite pseudofinite fields* $(\mathcal{AF}_K, \mathcal{PF}_K)$ *such that*

$$\mathbf{i} \circ \mathrm{pr} = \mathrm{pr} \circ \mathbf{i}, \quad \mathrm{Nm}_{K/L} \circ \mathbf{i} = \mathbf{i} \circ \pi_{K,L} \tag{12}$$

and for any $\gamma \in O_K, \ x \in A_K$

$$\mathbf{i}(\gamma \cdot x) = \mathrm{res}_{\mathrm{pr}(x)}(\gamma) \cdot \mathbf{i}(x). \tag{13}$$

Proof. For each $L \subset K$ choose the sections $Sp_L \to A_L$, $q \mapsto a_q$. Then

$$x = \bar{\gamma} \cdot a_q \Rightarrow \mathbf{i}(x) := \bar{\gamma}, \quad \text{for } x \in A_L, \ \gamma \in O_K, \bar{\gamma} := \mathrm{res}_q(\gamma) \in \mathbb{F}_q$$

determines the map with required properties. □

4.4. Corollary (The space of pseudofinite fields). *Given an ultrapower* $({}^*A_K, {}^*\mathrm{Sp}_K)$ *(over an ultrafilter* $\mathcal{D}$*) of the standard* (A_K, Sp_K) *there exists a space of pseudofinite fields* $({}^*\mathcal{AF}_K, {}^*\mathcal{PF}_K)$ *and a bijection*

$$\mathbf{i}: \ {}^*A_K \to {}^*\mathcal{AF}_K, \quad {}^*\mathrm{Sp}_K \to {}^*\mathcal{PF}_K, \quad \textit{all } K$$

with the same properties (12) and (13) as above. More precisely, $({}^*\mathcal{AF}_K, {}^*\mathcal{PF}_K)$ *can be constructed as the ultrapower of* $(\mathcal{AF}_K, \mathcal{PF}_K)$ *over the same ultrafilter.*

4.5. Algebraic closure. We call a substructure M of the multisorted structure $(\mathcal{AF}'_K, \mathcal{PF}'_K)$ **algebraically closed** if

(i) all the finite primes and the fibres over them belong to M;
(ii) for any $q \in \mathrm{Sp}_L \cap M$ we have $\mathrm{pr}^{-1}(q) \subset M$,
(iii) and for any $K \supseteq L$ every $\mathfrak{q} \in \mathrm{Sp}_K$ such that $q \subseteq \mathfrak{q}$ belongs to M.

The same definition works for a substructure of the multisorted structure $({}^*A_K, {}^*\mathrm{Sp}_K)$.

Given arbitrary X in a multisorted structure, we will write $\mathrm{cl}(X)$ for the minimal algebraically closed substructure containing X.

Example. The algebraic closure of a point $x \in A_K$ is equal to the closure of the prime $\mathfrak{q} \in \mathrm{Sp}_K$, such that $\mathfrak{q} = \mathrm{pr}(x)$. In its turn $\mathrm{cl}(\mathfrak{q})$ contains, for every $L \subseteq K$, the point $q = \pi^{\mathrm{Sp}}_{K,L}(\mathfrak{q})$. But, at the same time, by definition $\mathfrak{q} \in \mathrm{cl}(q)$. Summarising, one gets $\mathrm{cl}(x) = \mathrm{cl}(\mathfrak{q})$ by starting from $q_{\mathbb{Q}} \in \mathrm{Sp}_{\mathbb{Q}}$, the unique prime in $\mathbb{Z}$ under $\mathfrak{q}$, and then adjoining all primes q over $q_{\mathbb{Q}}$, for all L, along with $\mathrm{pr}^{-1}(q)$.

Remark. Suppose $\mathrm{cl}(X) \cap \mathrm{cl}(Y) = \emptyset$, for $X, Y \subset ({}^*\mathcal{AF}_K, {}^*\mathcal{PF}_K)$. Since the language does not contain predicates and functions linking $\mathrm{cl}(X)$ and $\mathrm{cl}(Y)$, for any disjoint embeddings e_X and e_Y, $({}^*\mathcal{AF}_K, {}^*\mathcal{PF}_K) \to (\mathcal{AF}'_K, \mathcal{PF}'_K)$, of $\mathrm{cl}(X)$ and $\mathrm{cl}(Y)$, the union $e_X \cup e_Y$ is an embedding.

4.6. Lemma. *In $({}^*A_K, {}^*\mathrm{Sp}_K)$, for any point a, the substructure on the set $\mathrm{cl}(a)$ is ω-stable of finite Morley rank on each sort.*

Moreover, any formula $\varphi(v_1, \dots, v_n)$ relativised to $\mathrm{cl}(a)$ is equivalent to an $\exists$-formula.

Proof. As described in the Example in 4.5, the infinite definable subsets consist of O_K-monoid-modules (orbits) $\mathrm{F}_{\mathfrak{q}}$ with monoid homomorphism $\pi_{K,L} : \lceil \mathrm{F}_{\mathfrak{q}} \rceil \to \lceil \mathrm{F}_q \rceil$ between those. This is ω-stable of finite Morley rank.

The second statement is equivalent to the fact that the theory of $\mathrm{cl}(a)$ is model-complete. To prove the latter consider the structures in two embedded models, $\mathrm{cl}(a) \subseteq \mathrm{cl}(a)'$. It is clear from the description in 4.5 that $\mathrm{cl}(a)$ and $\mathrm{cl}(a)'$ have the same primes $\mathfrak{q}$ in all sorts. Hence the embedding reduces to the family of embeddings $\lceil \mathrm{F}_{\mathfrak{q}} \rceil \subseteq \lceil \mathrm{F}'_{\mathfrak{q}} \rceil$. The Tarski-Vaught test verifies that this is an elementary embedding, $\mathrm{cl}(a) \preceq \mathrm{cl}(a)'$. $\square$

4.7. Lemma. *In $({}^*\mathcal{AF}_K, {}^*\mathcal{PF}_K)$, for any point a, the substructure on the set $\mathrm{cl}(a)$ is supersimple of finite rank on each sort.*

Proof. As described in the Example in 4.5, the infinite definable subsets consist of fields $\mathbb{F}_{\mathfrak{q}}$ and its definable subfields $\mathbb{F}_q$. Each of these is a finite extension of $\mathbb{F}_{q\mathbb{Q}}$, the minimal field in $\mathrm{cl}(a)$, and so interpretable in $\mathbb{F}_{q\mathbb{Q}}$. The latter is supersimple of finite rank. $\square$

4.8. Lemma. *Assume the continuum hypothesis, let $\mathcal{D}$ of 4.4 be a non-principal good ultrafilter on a countable set of indices and let $(\mathcal{AF'}_K, \mathcal{PF'}_K)$ be any saturated space of pseudofinite fields of cardinality $\aleph_1$. Then for any algebraically closed $M \subset ({}^*\mathcal{AF}_K, {}^*\mathcal{PF}_K)$ and algebraically closed $M' \subset (\mathcal{AF'}_K, \mathcal{PF'}_K)$ such that $\mathrm{Sp}_L \cap M$ is countable for any L, and $M \cong_{\mathbf{e}} M'$ there is an extension of the isomorphism $\mathbf{e}$ to an isomorphism*

$$({}^*\mathcal{AF}_K, {}^*\mathcal{PF}_K) \cong (\mathcal{AF'}_K, \mathcal{PF'}_K).$$

Proof. Note that by our assumptions $({}^*\mathcal{AF}_K, {}^*\mathcal{PF}_K)$ is also a saturated space of pseudofinite fields of cardinality $\aleph_1$. So we need to construct an isomorphism between any two of those.

It is enough to show that for every $a \in {}^*\mathcal{AF}_K \setminus M$ there is an $a' \in \mathcal{AF'}_K \setminus M'$ such that $\mathbf{e}$ can be extended to an isomorphism $M \cup \mathrm{cl}(a) \to M' \cup \mathrm{cl}(a')$.

By assumptions $a \in \mathbb{F}_{\mathfrak{q}}$ for some pseudofinite field $\mathbb{F}_{\mathfrak{q}}$, for $\mathfrak{q} = \mathfrak{q}(a) \in \mathrm{Sp}_K$, some number field K. The type $\mathrm{tp}(a, \mathbb{F}_{\mathfrak{q}})$ of $\mathbb{F}_{\mathfrak{q}}$ and x in the language $L_{\mathrm{rings}}(K)$ determines, by axioms (7)–(9) and 4.5 the type $\mathrm{tp}(a, \mathrm{cl}(a))$.

On the other hand, since $\mathbb{F}_{\mathfrak{q}}$ and all the other fields in $\mathrm{cl}(a)$ are pseudofinite, each formula in $\mathrm{tp}(a, \mathbb{F}_{\mathfrak{q}})$ is realised by some pair with a finite field $\mathbb{F}_{q^n}$ in place of $\mathbb{F}_{\mathfrak{q}}$. It implies that the same collection of formulas is a type in $(\mathcal{AF'}_K, \mathcal{PF'}_K)$, and so has a realisation $a', \mathbb{F}_{\mathfrak{q}'}$. Hence, also

$$\mathrm{tp}(a, \mathrm{cl}(a)) = \mathrm{tp}(a', \mathrm{cl}(a')).$$

Since both $\mathrm{cl}(x)$ and $\mathrm{cl}(x')$ can be seen as sort-by-sort definable substructures of saturated structures, we have an isomorphism $\mathrm{cl}(a) \to \mathrm{cl}(a')$, $a \mapsto a'$. By the Remark in 4.5 we obtain an isomorphism $M \cup \mathrm{cl}(a) \to M' \cup \mathrm{cl}(a')$ extending $\mathbf{e}$. $\square$

4.9. Corollary. *Any two spaces of pseudofinite fields are elementarily equivalent. The type of the "flag" $\langle a, \mathfrak{q} \rangle$, $a \in \mathbb{F}_{\mathfrak{q}}$, over an algebraically closed M, $\mathfrak{q} \notin M$, is determined by the elementary theory of the pair in the language $L_{\mathrm{rings}}(K)$. The complete invariant* *of the theory of* $\mathbb{F}_{\mathfrak{q}}$ *is the size of* $\mathbb{F}_{\mathfrak{q}}$, *if* $\mathbb{F}_{\mathfrak{q}}$ *is finite, or, otherwise, the subfield* $\mathbb{F}_{\mathfrak{q}} \cap \tilde{\mathbb{Q}}$, *with names from* O_K.

For the last part of the statement see [2].

4.10. Lemma. *In the structure* $({}^*A_K, {}^*\mathrm{Sp}_K)$ *let* $\mathfrak{q}$ *be an infinite prime and* $\mathbb{F}_{\mathfrak{q}}$ *a pseudo-finite field containing* K *as the named subfield. Let* $M \supset K$, *then the following are equivalent.*

(i) $\mathbb{F}_{\mathfrak{q}}$ *contains some Galois conjugate* $M' \supseteq K$ *of* M *as a named field;*

(ii) for some Galois conjugate $M' \supseteq K$ *of* M *and prime* $\mathfrak{m}'$ *of* $\mathrm{O}_{M'}$ *lying above* $\mathfrak{q}$, $\mathbb{F}_{\mathfrak{q}} \cong \mathbb{F}_{\mathfrak{m}'}$.

Proof. Write ${}^*\mathrm{O}_{M'}$ for the ultrapower of $\mathrm{O}_{M'}$. This will by definition contain $\mathfrak{m}'$ as an ultraproduct of prime ideals.

(ii) $\Rightarrow$ *(i)*, since $\mathrm{res}_{\mathfrak{m}'}({}^*\mathrm{O}_{M'}) = {}^*\mathrm{O}_{M'}/\mathfrak{m}' = \mathbb{F}_{\mathfrak{m}'} \cong \mathbb{F}_{\mathfrak{q}}$ and $\mathrm{res}_{\mathfrak{m}'}$ is injective on M'.

(i) $\Rightarrow$ *(ii)* Suppose $\mathrm{O}_{M'}$ has a basis $b_1, \cdots b_n$ as an O_K-module. Then $b_1, \cdots, b_n$ is also a basis for ${}^*\mathrm{O}_{M'}$ over ${}^*\mathrm{O}_K$.

Now if (i) holds, let $\mathfrak{m}'$ be a prime of ${}^*\mathrm{O}_M$ lying above $\mathfrak{q}$, the residue fields ${}^*\mathrm{O}_M/\mathfrak{m}' = \mathbb{F}_{\mathfrak{m}'}$ would be a finite extension of ${}^*\mathrm{O}_K/\mathfrak{q} = \mathbb{F}_{\mathfrak{q}}$ generated by the named elements $\mathrm{res}_{\mathfrak{m}'}(b_1), \cdots, \mathrm{res}_{\mathfrak{m}'}(b_n)$ which are in $\mathbb{F}_{\mathfrak{q}}$ by assumption. Then $\mathbb{F}_{\mathfrak{m}'} = {}^*\mathrm{O}_M/\mathfrak{m}' = {}^*\mathrm{O}_K/\mathfrak{q} = \mathbb{F}_{\mathfrak{q}}$.

□

4.11. Corollary. *Let* N *be an algebraically closed substructure of the multisorted representations structure* $({}^*A_K, {}^*\mathrm{Sp}_K)$, *and* $\mathfrak{q}, \mathfrak{q}' \in \mathrm{Sp}_K$. *Then*

$$\mathrm{tp}(\mathfrak{q}/N) = \mathrm{tp}(\mathfrak{q}'/N) \Leftrightarrow \mathbb{F}_{\mathfrak{q}} \equiv_{L_{\mathrm{rings}}(K)} \mathbb{F}_{\mathfrak{q}'} \tag{14}$$

and, for $\mathfrak{q}$ *infinite,*

$$\mathrm{tp}(\mathfrak{q}/N) = \mathrm{tp}(\mathfrak{q}'/N) \Leftrightarrow \text{ for all } M \supset K: \ \mathfrak{q} \in \Pi_{M,K} \leftrightarrow \mathfrak{q}' \in \Pi_{M,K} \tag{15}$$

Proof. (14) follows from 4.4, 4.8 and 4.9.

In order to prove (15) invoke Kiefe's criterium (see [2], 4.7): $\mathbb{F}_{\mathfrak{q}} \equiv \mathbb{F}_{\mathfrak{q}'}$ in the language $L_{\mathrm{rings}}(K)$ if and only if for every irreducible polynomial $f(x)$ over K,

$$\mathbb{F}_{\mathfrak{q}} \vDash \exists x\, f(x) = 0 \Leftrightarrow \mathbb{F}_{\mathfrak{q}'} \vDash \exists x\, f(x) = 0,$$

where coefficients of $f(x)$ are interpreted in $\mathbb{F}_{\mathfrak{q}}$ and $\mathbb{F}_{\mathfrak{q}'}$ as names of elements in the pseudofinite fields.

Note that the assumption that $\mathfrak{q} \in \mathrm{Sp}_K$ is infinite (i.e. non-standard) implies that $\mathrm{char}\, \mathbb{F}_{\mathfrak{q}} = 0$ and the naming homomorphism $K \to \mathbb{F}_{\mathfrak{q}}$ is an embedding. It follows that $f(x)$ remains irreducible as a polynomial over $K_{\mathfrak{q}} = K$, the image of K in $\mathbb{F}_{\mathfrak{q}}$.

Let $M \supset K$ be a field generated by a root of $f(x)$ over K. Now

$$\mathbb{F}_{\mathfrak{q}} \vDash \exists x\, f(x) = 0 \Leftrightarrow \bigvee_{M' \cong_K M} \mathbb{F}_{\mathfrak{q}} \supseteq M'$$

where on the right we consider images of conjugates of M in $\mathbb{F}_{\mathfrak{q}}$. But this condition by 4.10 and 3.15 is equivalent to $\mathfrak{q} \in \Pi_{M,K}$. □

4.12. Remark. (i) *Suppose M/K is Galois. Then for all but finitely many $\mathfrak{q} \in \mathrm{Sp}_K$,*

$$\mathfrak{q} \in \Psi_{M,K} \Leftrightarrow \mathfrak{q} \in \Pi_{M,K}.$$

Indeed, let as above M be generated by a root of an irreducible $f(x)$ of order n over K. Then M contains all the roots of f and so for an infinite prime $\mathfrak{q}$

$$\mathbb{F}_{\mathfrak{q}} \vDash \exists x\, f(x) = 0 \Leftrightarrow \mathbb{F}_{\mathfrak{q}} \supseteq M \Leftrightarrow \mathbb{F}_{\mathfrak{q}} \vDash \exists x_1, \ldots, x_n \left(\bigwedge_{i=1}^{n} f(x_i) = 0 \;\&\; \bigwedge_{i \neq j} x_i \neq x_j \right).$$

The condition on the right means that $f(x)$ splits completely over $\mathfrak{q}$, that is $\mathfrak{q} \in \Psi_{M,K}$. The condition on the left means that $\mathfrak{q} \in \Pi_{M,K}$. This holds for all nonstandard primes $\mathfrak{q}$, hence does hold for all but finitely many standard primes.

(ii) *The condition that M/K is Galois is not essential. Let $\hat{M}$ be the minimal Galois extension of K containing M. Then for all but finitely many $\mathfrak{q} \in \mathrm{Sp}_K$,*

$$\mathfrak{q} \in \Psi_{M,K} \Leftrightarrow \mathfrak{q} \in \Psi_{\hat{M},K} \Leftrightarrow \mathfrak{q} \in \Pi_{\hat{M},K}.$$

Indeed, under the assumtion we have an infinite $\mathfrak{q} \in \mathrm{Sp}_K$ such that $\mathfrak{q} \in \Psi_{M,K}$. But then by definition of $\Psi_{M,K}$ we will have that the minimal polynomial $f(x)$ for M splits completely (see 3.14). Then $\mathbb{F}_{\mathfrak{q}}$ contains all roots of $f(x)$, so all conjugates of M so $\hat{M}$. Thus $\mathfrak{q} \in \Psi_{\hat{M},K}$. Conversely, if $\mathfrak{q} \in \Psi_{\hat{M},K}$ then $\mathbb{F}_{\mathfrak{q}}$ contains $\hat{M}$, so contains all conjugates of M and so $f(x)$ splits completely in $\mathbb{F}_{\mathfrak{q}}$, $\mathfrak{q} \in \Psi_{M,K}$.

4.13. Corollary (to 4.11). *The theory of the multisorted representations structure is superstable. The U-rank of a non-principal 1-type of sort Sp_K is 1, the U-rank of a 1-type of A_K containing the formula $\mathrm{pr}(v) = \mathfrak{q}$ over $\mathfrak{q} \in \mathrm{Sp}_K$ is 0 or 1 depending on whether $\mathfrak{q}$ is finite or infinite prime. If the type contains no such formula, it is generic and its U-rank is 2.*

Indeed, by (15) for any N the set of 1-types over N of sorts Sp_K is at most of cardinality continuum. Moreover, each 0-definable non-principal type has a unique non-algebraic extension over N.

A type of sort A_K by 4.8 is determined by a type of sort Sp_K and the type relative to the ω-stable substructure $\mathrm{cl}(a)$. If a 1-type contains a formula $\mathrm{pr}(v) = \mathfrak{q}$ for a parameter $\mathfrak{q}$, then it is a type of an element of the fibre $\lceil \mathrm{F}_{\mathfrak{q}} \rceil$, which is either finite, if $\mathfrak{q}$ is finite, or strongly minimal, so of U-rank 1. The unique complete 1-type which negates all formulas $\mathrm{pr}(v) = \mathfrak{q}$ is of U-rank 2. $\square$

4.14. Theorem. *The theory of the multisorted representations structure has QE in the language extended by boolean combination of the unary predicates:*

- $v \in \mathrm{Sp}_K$,
- $v = \mathfrak{q}$, *for* $\mathfrak{q} \in \mathrm{Sp}_K$, *finite,*
- $v \in \Pi_{K,L}$

and

- *existential formulas $\varphi(v_1, w_1, \ldots, v_n, w_n, q_{\mathbb{Q}})$ where the v_i are of sorts A_{L_i} and w_i of Sp_{L_i} and $v_1, w_1 \ldots, v_n, w_n$ are relativised to $\mathrm{cl}(q_{\mathbb{Q}})$, $q_{\mathbb{Q}} \in \mathrm{Sp}_{\mathbb{Q}}$, $L_1, \ldots, L_n \in \mathcal{R}$.*

Proof. By 4.6 and 4.11(15) a complete n-type in the theory is determined by formulas listed in the formulation of the theorem. By the compactness theorem any formula is equivalent to a boolean combination of those. $\square$

5. The topology and compactification

We extend the conventional topology of 2.2 on Sp_L by declaring **closed in** Sp_L subsets of the form $\Pi_{K,L}$, singletons and their finite unions, for all extension K of L.

We accordingly extend the topology on A_L by declaring **closed in** A

- the graph of pr restricted to $A_L \times \mathrm{Sp}_L$, $L \in \mathcal{R}$;
- the graph of $\pi_{K,L}$, for $K, L \in \mathcal{R}$;
- subsets of Sp_L of the form $\Pi_{K,L}$, $L \in \mathcal{R}$;
- subsets of $A_{L_1} \times \mathrm{Sp}_{L_1} \ldots \times A_{L_n} \times \mathrm{Sp}_{L_n}$ defined by positive existential formulas $\varphi(v_1, w_1, \ldots, v_n, w_n, q_{\mathbb{Q}})$ relativised to $\mathrm{cl}(q_{\mathbb{Q}})$, $q_{\mathbb{Q}} \in \mathrm{Sp}_{\mathbb{Q}}$, $L_1, \ldots, L_n \in \mathcal{R}$.

along with cartesian products, finite intersections and unions of those.

5.1. Lemma. *In the multisorted structure the maps* pr *and* $\pi_{K,L}$ *are continuous.*

Proof. The continuity of pr is just by definition.

In order to prove the continuity of $\pi_{K,L}$ we need to prove that $\pi^{-1}_{K,L}(S)$ is closed for every closed $S \subset A_L$. Since this is obvious for finite S, we need to consider only the closed subsets S of the form $\Pi_{M,L}$.

Claim.

$$\pi^{-1}_{K,L}(\Pi_{M,L}) = \Pi_{KM,K}$$

where KM is the composite of fields.

Proof. Let $q \in \Pi_{M,L}$, $M = L[\alpha]$. Then we have $KM = K[\alpha]$ and for some $a \in L$,

$$\alpha - a \in q. \tag{16}$$

Then

$$\alpha - a \in \mathfrak{q} \text{ for every prime } O_K \supset \mathfrak{q} \supseteq q \tag{17}$$

which implies $\mathfrak{q} \in \Pi_{KM,K}$. This proves

$$q \in \Pi_{M,L} \Rightarrow \mathfrak{q} \in \Pi_{KM,K} \text{ for every prime } O_K \supset \mathfrak{q} \supseteq q.$$

Now we prove the converse. Suppose

$$\mathfrak{q} \in \Pi_{KM,K} \text{ for every prime } \mathfrak{q} \supseteq q.$$

This is equivalent to say that $\mathbb{F}_{\mathfrak{q}'} = \mathbb{F}_{\mathfrak{q}}$ for $\mathfrak{q}' \in KM$ and $\mathfrak{q}'$ lie above $\mathfrak{q}$ and so to (17). But

$$\bigcap_{\mathfrak{q} \supseteq q} \mathfrak{q} = q$$

and hence we proved (16) and $q \in \Pi_{M,L}$. This finishes the proof of the claim and of the lemma. □

5.2. The Chebotarev density theorem and its corollaries. Recall that the **density** of a subset $S \subset \mathrm{Sp}_L$ is defined as

$$\mathrm{dn}\, S = \lim_{n \to \infty} \frac{\#\{q \in S : |q| \le n\}}{\#\{q \in \mathrm{Sp}_L : |q| \le n\}}.$$

The Chebotarev density theorem ([11], 4.4.3) states that a subset $S \subset \mathrm{Sp}_L$ defined by the pattern of splitting of f_K, the minimal polynomial for K over L, modulo q has a density. Moreover, it determines the density in terms of the structure of $G = \mathrm{Gal}(\hat{K} : L)$, where $\hat{K}$ is the minimal Galois extension of L containing K. More precisely, let $\sigma \in G$ and $C = \sigma^G$ a conjugacy class.

Then Chebotarev Density Theorem states that

$$\mathrm{dn}\{q \in \mathrm{Sp}_L : \ \sigma_q \in C\} = \frac{|C|}{|G|},$$

where σ_q are the Frobenius elements defined up to conjugacy.

5.3. Proposition. *Let $L \subset K \subset M$ and M/L minimal Galois extension containg K. Then* $\mathrm{dn}(\Pi_{M,L})$ *is well-defined and*

$$\mathrm{dn}(\Pi_{K,L}) \geq \frac{1}{|M : L|}.$$

Proof. Let $q \in Sp_L$, $\mathfrak{m} \in Sp_M$ such that $\mathfrak{m} \supset q$. Consider the Frobenius element $\mathrm{Frob}_q \in G = \mathrm{Gal}(M : L)$, that is such that its action on $\mathbb{F}_\mathfrak{m} = \mathrm{res}_q(M)$ fixes exactly $\mathbb{F}_q$ inside $\mathbb{F}_\mathfrak{m}$. Now $\mathrm{res}_\mathfrak{m}(K) = \mathbb{F}_r$, the image of K in $\mathbb{F}_\mathfrak{m}$, is fixed by the action of Frob_q^ℓ, where $\ell = |\mathbb{F}_r : \mathbb{F}_q|$.

Set $C \subseteq G$ to be the conjugacy class which contains Frob_q^ℓ. Clearly $|C| \geq 1$ and q is such that the Chebotarev formula above now counts the density of those $q \in \mathrm{Sp}_L$ for which there is (every) $\mathfrak{m} \in \mathrm{Sp}_M$, $\mathfrak{m} \supset q$, $\mathrm{Frob}_q^\ell = \mathrm{Frob}_q$. That is $\mathbb{F}_r = \mathbb{F}_q$, equivalently $\mathbb{F}_q \cong \mathbb{F}_\mathfrak{q}$. These are exactly the $\mathfrak{q}$ in $\Pi_{K,L}$. □

An immediate corollary to 5.3 is that $\Pi_{K,L}$ and $\Psi_{K,L}$ are infinite. Also $\Psi_{K,L}$ has well-defined density,

$$\mathrm{dn}(\Psi_{K,L}) = \frac{1}{|\hat{K} : L|},$$

where $\hat{K}$ is the minimal Galois extension of L containing K. See 4.12.

5.4. Lemma. *For any two Galois extensions K_1 and K_2 of L and any infinite prime* $q \in \mathrm{Sp}_L$,

$$q \in \Psi_{K_1,L} \cap \Psi_{K_2,L} \Leftrightarrow q \in \Psi_{K,L}$$

for $K = K_1K_2$, the composite of the two fields and so any intersection of the $\Psi_{K_i,L}$ has a well-defined positive density.

Proof. Indeed, K_1 and K_2 are subfields of $\mathbb{F}_q$ if and only if K is. □

5.5. Proposition. An intersection of finite family of special subsets $\Pi_{K,L}$ (arbitrary $K : L$) of Sp_L is nonempty:

$$\bigcap_{i \in I} \Pi_{K_i,L} \neq \emptyset.$$

Proof. First note that by definition

$$\bigcap_{i \in I} \Pi_{K_i,L} \supseteq \bigcap_{i \in I} \Psi_{K_i,L}.$$

By 5.4 and 4.12, for infinite $q \in \mathrm{Sp}_L$

$$q \in \bigcap_{i \in I} \Psi_{\hat{K}_i,L} \Leftrightarrow q \in \Psi_{K,L} \Leftrightarrow q \in \Pi_{K,L},$$

for K the composite of all the $\hat{K}_i$. Hence $\bigcap_{i \in I} \Psi_{\hat{K}_i,L}$ is infinite and non-empty. □

We note also the following.

5.6. Theorem. *For any extensions K_i of L, $i = 1, \dots, k$, any boolean combination of subsets $\Psi_{K_i,L}$ of Sp_L has a well-defined density.*

Proof. First we note that by 4.12(ii) we may assume that K_i/L are Galois.

Secondly, note that it is enough to prove the theorem for the intersection

$$\bigcap_{i\in\{i_1,\dots i_m\}} \Psi_{K_i,L} \cap \bigcap_{j\in\{i_{m+1},\dots i_k\}} \neg\Psi_{K_j,L}$$

for any permutation $\{i_1, \dots, i_k\}$ of $\{1, \dots, k\}$.

Also, as shown in 5.4 $\bigcap_{i\in\{i_1,\dots i_m\}} \Psi_{K_i,L}$ can be replaced by some $\Psi_{K,L}$.

Now we prove,

Claim. The density of the set of the form

$$\bigcup_{l\in\{1,\dots m\}} \Psi_{K_l,L}$$

is well-defined.

We prove this by induction on m. Assuming it is true for m note that by definition

$$\mathrm{dn}\left(\bigcup_{l\in\{1,\dots m+1\}} \Psi_{K_l,L}\right) = \mathrm{dn}\left(\bigcup_{l\in\{1,\dots m\}} \Psi_{K_l,L}\right) + \mathrm{dn}\,\Psi_{K_{m+1},L} - \mathrm{dn}\left(\left(\bigcup_{l\in\{1,\dots m\}} \Psi_{K_l,L}\right) \cap \Psi_{K_{m+1},L}\right)$$

provided the three summands on the right are well-defined. The first two are well-defined by the induction hypothesis. The same is true for the last one since

$$\left(\bigcup_{l\in\{1,\dots m\}} \Psi_{K_l,L}\right) \cap \Psi_{K_{m+1},L} = \bigcup_{l\in\{1,\dots m\}} \left(\Psi_{K_l,L} \cap \Psi_{K_{m+1},L}\right).$$

This proves the claim.

Now it remains to see that

$$\mathrm{dn}\left(\Psi_{K,L} \cap \bigcap_{j\in\{1,\dots m\}} \neg\Psi_{K_j,L}\right) = \mathrm{dn}\Psi_{K,L} \;-\; \mathrm{dn} \bigcup_{j\in\{1,\dots m\}} \Psi_{K,L} \cap \Psi_{K_j,L}.$$

The last term is well-defined by the claim. This finishes the proof of the theorem. ☐

Remark. The density is a measure on the boolean algebra generated by all the $\Psi_{K,L}$ for a given L.

Question. Is density well-defined on the boolean algebra generated by all the $\Pi_{K,L}$, for a given L?

5.7. Compact models. Note that the sorts Sp_L and A_L are not compact since the intersection $\bigcap_{i\in I} \Pi_{K_i,L}$, for an infinite I and distinct K_i, $i \in I$, is empty (no prime ideal in O_L belongs to such an intersection) but the intersection of any finite subfamily of the sets is non-empty by 5.5.

However, there are plenty of models which are compact in the special topology; all we need to do is to realise the maximal positive types

$$\bigcap_{K\supset L} \Pi_{K,L} \tag{18}$$

in each sort Sp_L (these are types by 5.5).

These contain positive types of the form

$$\bigcap_{K\supset L} \Psi_{K,L} \tag{19}$$

Any realisation of such type will be called a **splitting infinite prime** (or just a splitting prime) in Sp_L.

We call a multisorted structure $\mathfrak{M}$ of representations **a minimal compact model** if

(i) $\mathfrak{M}$ is an elementary extension of the standard multisorted structure of representations;
(ii) any sort $\mathrm{Sp}_L(\mathfrak{M})$ in the structure is compact;
(iii) for any other $\mathfrak{M}'$ satisfying (i) and (ii), for each sort A_L there is an embedding

$$A_L(\mathfrak{M}) \subset A_L(\mathfrak{M}').$$

5.8. Theorem. *A minimal compact model $\mathfrak{M}$ exists and is unique.*

(a) For each Galois extension L of $\mathbb{Q}$ a minimal $\mathfrak{M}$ contains exactly $\deg L$ infinite primes in Sp_L.

(b) All the infinite primes in $\mathrm{Sp}_K(\mathfrak{M})$ are splitting primes and all the infinite primes containing $q \in \mathrm{Sp}_L(\mathfrak{M})$ for $K : L$ Galois are conjugated by the definable action of the Galois group $\mathrm{Gal}(K : L)$ defined by formula (6).

(c) The residue field $\mathbb{F}_q$ over such an infinite prime q is characterised as a pseudo-finite field containing $\mathbb{Q}^{alg}$ with a naming homomorphism

$$\mathrm{res}_q : \mathrm{O}_L \to \mathbb{Q}^{alg} \subset \mathbb{F}_q$$

The first order theory of such $\mathbb{F}_q$ is determined uniquely by the latter inclusion.

(d) The fibres over infinite q have the form

$$\lceil \mathrm{F}_q \rceil(\mathfrak{M}) = \mathbb{Q}^{alg} \cdot a_q$$

for a non-zero element a_q of the fibre.

Proof. We use the analysis in 3.13 for finite primes in $\Pi_{K,L}$ and extend the conclusions to infinite primes satisfying the same first-order condition. The Tarski-Vaught test along with the statement of theorem 4.14 allows to conclude that the structure with properties (a)-(c) is an elementary submodel of a saturated model $({}^*A_K, {}^*\mathrm{Sp}_K)$, $K \in \mathcal{R}$, described in section 4.

It remains to establish properties (a)-(d).

(a)-(b). In our case the splitting occurs that is $\mathbb{F}_{\mathfrak{q}} = \mathbb{F}_q$ and $\mathrm{Norm}_{K,L}$ is the identity map. The $|K : L|$ distinct prime ideals $\mathfrak{q}^i \in \mathrm{Sp}_K$, $(i = 1, \ldots, |K : L|)$ lying over q give rise to $|K : L|$ naming homomorphisms

$$\mathrm{res}_{\mathfrak{q}^i} : \mathrm{O}_K \to \mathbb{F}_q, \quad \ker(\mathrm{res}_{\mathfrak{q}^i}) = \mathfrak{q}^i$$

which are pairwise non-isomorphic over $\mathrm{res}_q : \mathrm{O}_L \to \mathbb{F}_q$.

Hence we have $|K : L|$ different ways of naming elements of $\mathbb{F}_q$ when we pass from level L to level K. This proves that over infinite splitting $p_{\mathbb{Q}} \in \mathrm{Sp}_{\mathbb{Q}}$ there are exactly $\deg L$ splitting q in Sp_L.

The distinct prime ideals $\mathfrak{q}^i$ extending $q \in Sp_L$ in O_K are conjugated under the action of $\mathrm{Gal}(K : L)$, which is first-order definable by (6), so extends to the infinite splitting primes, and this proves the second statement.

(c) follows from (14) and the characterisation of the elementary types of pseudo-finite fields $\mathbb{F}$ of characteristic 0 by their subfield of algebraic numbers (see [2]).

(d) The only condition on the infinite fibres in A_K is that the action by K is defined and is free. This is satisfied if we set the fibre of the form (d). □

5.9. The minimal complete model. We call $\mathfrak{N}$ a minimal complete model if:

(i) $\mathfrak{N}$ is an elementary extension of the standard multisorted structure of representations;
(ii) any sort $\mathrm{Sp}_L(\mathfrak{N})$ in the structure realises all the 1-types over 0;
(iii) for any other $\mathfrak{N}'$ satisfying (i) and (ii), for each sort A_L there is an embedding

$$A_L(\mathfrak{N}) \subset A_L(\mathfrak{N}').$$

5.10. Theorem. *A minimal complete model exists and is unique.*

(a) For each Galois extension L of $\mathbb{Q}$ a minimal $\mathfrak{M}$ contains at most $\deg L$ *infinite primes in* Sp_L. *The primes $\mathfrak{q}$ over q, for K/L Galois, are conjugated under the action of Galois group* $\mathrm{Gal}(K:L)$.

(b) An infinite prime $q \in \mathrm{Sp}_L(\mathfrak{N})$ is uniquely characterised by the field

$$E_q = \mathbb{Q}^{alg} \cap \mathbb{F}_q$$

and the naming homomorphism

$$\mathrm{res}_q : O_L \to E_q.$$

(c) The fibres over infinite q have the form

$$\lceil \mathrm{F}_q \rceil(\mathfrak{N}) = E_q \cdot a_q$$

for a non-zero element a_q of the fibre.

Proof. Same arguments as in 5.8.□

5.11. Formal geometry. We leave out the problem of identifying a model which can be seen as a generalised Zariski geometry. It is clear that neither of the models we discussed above is an analytic (or Noetherian) Zariski geometry in the sense of [15].

6. The universal cover

6.1. The coarse cover. Let $\mathrm{O}_{\mathcal{R}} = \bigcup\{\mathrm{O}_K : \mathrm{O}_K \in \mathcal{R}\}$. Most of the time we will deal with the case of $\mathcal{R}$ containing all integral extensions of O_M, some number field M.

The systems of morphisms $\pi_{K,L}$ and $\pi^{\mathrm{Sp}}_{K,L}$, $K \supset L$, determine a projective system.

Define $A_{\mathcal{R}}$ and $\mathrm{Sp}_{\mathcal{R}}$ as the projective limits of A_K and Sp_K respectively, $\mathrm{O}_K \in \mathcal{R}$.

By definition we will have maps

$$\pi_{\mathcal{R},K} : A_{\mathcal{R}} \to A_K, \quad \text{and} \quad \pi^{\mathrm{Sp}}_{\mathcal{R},K} : \mathrm{Sp}_{\mathcal{R}} \to \mathrm{Sp}_K$$

satisfying

$$\pi_{\mathcal{R},K} \circ \pi_{K,L} = \pi_{\mathcal{R},L}, \quad \text{and} \quad \pi^{\mathrm{Sp}}_{\mathcal{R},K} \circ \pi^{\mathrm{Sp}}_{K,L} = \pi^{\mathrm{Sp}}_{\mathcal{R},L}.$$

Also the following (non-first-order) condition is satisfied:

$$\forall x_1, x_2 \in A_{\mathcal{R}}\ x_1 = x_2 \leftrightarrow \bigwedge_K \pi_{\mathcal{R},K}(x_1) = \pi_{\mathcal{R},K}(x_2) \tag{20}$$

The definition assigns to each point $\tilde{q} \in \mathrm{Sp}_{\mathcal{R}}$ an orbit $\lceil \mathrm{F}_{\tilde{q}} \rceil$ which, according to 3.2, can be represented as $\lceil \mathrm{F}_{\tilde{q}} \rceil = \mathbb{F}_{\tilde{q}}.a_{\tilde{q}}$ for some $a_{\tilde{q}} \in \lceil \mathrm{F}_{\tilde{q}} \rceil$, where by definition

$$\mathbb{F}_{\tilde{q}} = \bigcup \{ \mathbb{F}_{\mathfrak{q}} : \pi_{\mathcal{R},K}(\lceil \mathrm{F}_{\tilde{q}} \rceil) = \mathbb{F}_{\mathfrak{q}}.a_{\pi_{\mathcal{R},K}(\tilde{q})} \},$$

the union of the tower of named fields below $\tilde{q}$. The naming means that $\mathbb{F}_{\tilde{q}}$ is given along with a naming homomorphism

$$\mathrm{res}_{\tilde{q}} : \mathrm{O}_{\mathcal{R}} \to \mathbb{F}_{\tilde{q}}.$$

Clearly,

$$A_{\mathcal{R}} := \bigcup \{ \lceil \mathrm{F}_{\tilde{q}} \rceil : \tilde{q} \in \mathrm{Sp}_{\mathcal{R}} \}.$$

The topology on $A_{\mathcal{R}}$ and $\mathrm{Sp}_{\mathcal{R}}$ is defined as the projective limit of topologies on the A_K and Sp_K, that is a subset $S \subseteq \mathrm{Sp}_{\mathcal{R}}$ is defined to be closed if $\pi_{\mathcal{R},K}(S)$ is closed for all large enough K.

In particular, the fibre $(\pi^{\mathrm{Sp}})^{-1}_{\mathcal{R},K}(q) \subset \mathrm{Sp}_{\mathcal{R}}$ is closed for any K and $q \in \mathrm{Sp}_K$.

6.2. The fibre of $A_{\mathcal{R}}$ over a finite prime. In case when $\tilde{q}$ lies over a standard prime q, that is $\pi^{\mathrm{Sp}}_{\mathcal{R},1}(\tilde{q}) = q \in \mathbb{Z}$, and $\bigcup \mathcal{R} = \mathbb{Q}^{alg}$ we have $\mathbb{F}_{\tilde{q}} = \mathbb{F}_q^{alg}$. However, for the same q we will have as many points $\tilde{q}$ over q as there are naming homomorphisms $\mathrm{O}_{\mathcal{R}} \to \mathbb{F}_{\tilde{q}}$. Note that the naming homomorphisms in this case are just residue maps of p-adic valuation on $\mathbb{Q}^{alg}$. In other words, setwise

$$(\pi^{\mathrm{Sp}}_{\mathcal{R},1})^{-1}(q) = \{q\text{-adic valuations on } \mathbb{Q}^{alg}\} \cong \{\mathrm{res}_q : \mathrm{O}_{\mathcal{R}} \to \mathbb{F}_q^{alg}\}.$$

Let $\mathcal{G}_{\mathbb{Q}} := \mathrm{Gal}(\tilde{\mathbb{Q}} : \mathbb{Q})$. Then, it follows from the general theory of valuations that, for any two homomorphisms res_q and $\mathrm{res}'_q : \mathrm{O}_{\mathcal{R}} \to \mathbb{F}_{\tilde{q}}$, there is a $\sigma \in \mathcal{G}_{\mathbb{Q}}$ such that $\mathrm{res}'_q = \mathrm{res}_q \circ \sigma$. In other words $\mathcal{G}_{\mathbb{Q}}$ acts transitively on the fibre and

$$(\pi^{\mathrm{Sp}}_{\mathcal{R},1})^{-1}(q) = \tilde{q} \cdot \mathcal{G}_{\mathbb{Q}}.$$

Note that

$$\ker(\mathrm{res}_q \circ \sigma) = \sigma^{-1}\{\ker(\mathrm{res}_q)\}$$

and so the subgroup of $\mathcal{G}_{\mathbb{Q}}$ fixing $\tilde{q}$ is equal to the stabiliser $\mathcal{D}(\tilde{\mathfrak{q}})$ of the prime ideal $\tilde{\mathfrak{q}} := \ker(\mathrm{res}_{\tilde{q}})$ of $\mathrm{O}_{\mathcal{R}}$, known as the *decomposition group of* $\tilde{\mathfrak{q}}$. The decomposition group $\mathcal{D}(\tilde{\mathfrak{q}})$ acts on $O_{\mathcal{R}}/\tilde{\mathfrak{q}} = \mathbb{F}_{\tilde{q}} \cong \mathbb{F}_q^{alg}$ inducing all the automorphisms of $\mathbb{F}_q^{alg}$, which determines a canonical surjective homomorphism $\mathcal{D}(\tilde{\mathfrak{q}}) \to \mathcal{G}_{\mathbb{F}_{\tilde{q}}}$ onto the absolute Galois group of $\mathbb{F}_{\tilde{q}}$.

6.3. Question. *Is the action of $\sigma \in \mathcal{G}_{\mathbb{Q}}$ on $(\pi^{\mathrm{Sp}}_{\mathcal{R},1})^{-1}(q)$ over a finite prime continuous?*

6.4. The fibre of $A_{\mathcal{R}}$ over the infinite splitting prime. In this case $\tilde{q}$ lies over an infinite splitting prime q (which is unique up to its first-order type) and $\mathrm{O}_{\mathcal{R}}$ contains all integral extensions, we have that $\mathrm{O}_{\mathcal{R}} \subset \mathbb{Q}^{alg}$ is the ring of all integral algebraic numbers, $\pi_{\mathcal{R},1}$ is an isomorphism and $\mathbb{F}_{\tilde{q}} = \mathbb{F}_q$, a pseudo-finite field which contains $\mathbb{Q}^{alg}$ and the latter is equal to the subfield of named elements of $\mathbb{F}_q$ (see 5.8).

Again we will have as many points $\tilde{q}$ over q as there are naming homomorphisms $\sigma : \mathrm{O}_{\mathcal{R}} \to \mathbb{Q}^{alg} \subset \mathbb{F}_q$. Note that the naming homomorphisms in this case can be identified with automorphisms of the field $\mathbb{Q}^{alg}$. In other words, $\mathcal{G}_{\mathbb{Q}}$ acts freely and transitively on $(\pi^{\mathrm{Sp}}_{\mathcal{R},1})^{-1}q$

$$(\pi^{\mathrm{Sp}}_{\mathcal{R},1})^{-1}(q) = \tilde{q} \cdot \mathcal{G}_{\mathbb{Q}}.$$

6.5. Proposition. *The action of a $\sigma \in \mathcal{G}_{\mathbb{Q}}$ on the fibre $(\pi^{\mathrm{Sp}}_{\mathcal{R},1})^{-1}(q)$ over the infinite splitting prime is continuous.*

Proof. The action on each layer Sp_K is definable by formula (6) which also defines a continuous map according to our definition of topology. □

Concluding remarks and further directions

As was noted in the introduction this version of the structure is the most basic one. We would like to indicate several direction in which the construction and the analysis may develop.

First remark concerns the similarity with the basic ingredients of Arakelov's geometry. The minimal compact model of the arithmetic plane over K (see 5.8) is quite similar to Arakelov's plane over the projective line. The limit fibres in our case corresponds to $\mathbb{Q}^{alg}$, whereas in Arakelov's setting it is $\mathbb{C}$ or $\mathbb{R}$, depending on the number field, and K embeds in the limit fibres (it is worth noting that in our structure the number of embedding morphisms is $\deg(K : \mathbb{Q})$ just as Arakelov's theory predicts). One way of closing this gap is to consider $\mathbb{Z}$ and the general rings O_K for Galois extension as "$*$-algebras", that is with the involution $*$, complex conjugation induced by an embedding $K \subset \mathbb{C}$. In particular, $\mathbb{Z}$ consists of self-adjoint operators. Respectively, we replace in the limit fibres $\mathbb{Q}^{alg}$ by its completion $\mathbb{C}$ or by its self-adjoint part $\mathbb{R}$.

The other connection is with the work of A.Connes and C.Consani [1]. Our current understanding is that to come to their arithmetic site from our arithmetic plane we need to extend our notion of representations of $\mathbb{Z}$ from $\mathbb{Z}/p$, for prime p, to the more general $\mathbb{Z}/n$, for arbitrary $n > 1$. The points of the arithmetic site then can be seen as the limits of such representations.

Finally, the model theorist reader would have already noted that the geometry of our structure is of trivial type in the sense of model theoretic trichotomy (the one by Connes and Consani is non-trivial locally modular type). This raises the question if such a geometry can contain any really interesting mathematical information. To turn this doubt around we note that geometries of trivial and locally modular types may allow much stronger *counting functions* than the non-locally ones. In [16] the first author introduced polynomial invariants of definable subsets in totally categorical theories and in [9] it was proved that the same polynomial invariants in the context of certain combinatorial geometries of trivial type are equivalent to classical graph polynomials of very general kind.

References

[1] A. Connes and C. Consani, *Geometry of the arithmetic site*, arXiv:1502.05580

[2] Z. Chatzidakis, *Model theory of finite fields and pseudo-finite fields*, Annals of Pure and Applied Logic, 88 (1997) 95–108

[3] G. Cherlin, L. van den Dries, and A. Macintyre, *The elementary theory of regularly closed fields*, preprint, 1980.

[4] J.A. Cruz Morales and B. Zilber, *The geometric semantics of algebraic quantum mechanics*, Phil. Trans. R. Soc. A, 2015

[5] J. Derakhshan and A. Macintyre, *Some supplemenys to Feferman-Vaught related to the model theory of adeles*, arXiv:1306.1794

[6] C.A. Guido Ruiz, In preparation, 2017

[7] W. James A Gray, *Coding Complete Theories in Galois Groups*, PhD thesis, University of Edinburgh, 2003

[8] M. Jarden *Elementary statements over large algebraic fields*, Transactions of AMS., V 164, 1972, pp. 67–91

[9] T. Kotek, J. Makowsky and B. Zilber, *On Counting Generalized Colorings*, Lect Notes in Computer Sc., V 5213, 2008, pp.339–353

[10] Yu. Manin, *The Notion of Dimension in Geometry and Algebra*, Bull. of the AMS, 43 (2), 2006, 139-161

[11] Yu. Manin and A. Panchishkin, **Introduction to Modern Number Theory**, 2nd Ed., Springer, 2007

[12] B. Zilber, *On syntax – semantics dualities in logic, geometry and physics*, In preparation

[13] B. Zilber, *A class of quantum Zariski geometries*, In: **Model Theory with applications to algebra and analysis, I and II** (Z. Chatzidakis, H.D. Macpherson, A. Pillay, A.J. Wilkie editors), Cambridge University Press, Cambridge. 2008

[14] B. Zilber, *The semantics of the canonical commutation relation*, arxiv.org/abs/1604.07745

[15] B. Zilber, **Zariski geometries.** CUP, 2010

[16] B. Zilber, *Strongly minimal countably categorical theories, II* Siberian Math.J., 25. 3:71–88, 1984

Mathematical Institute, University of Oxford, Oxford