MODEL THEORY AND GEOMETRY OF REPRESENTATIONS OF RINGS OF INTEGERS

B.ZILBER AND L. SHAHEEN

ABSTRACT. The aim of this project is to attach a geometric structure to the ring of integers. It is generally assumed that the spectrum Spec($\mathbb{Z}$) defined by Grothendieck serves this purpose. 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 Spec($\mathbb{Z}$).

Our approach is based on the generalisation of constructions applied by the first author for similar purposes in non-commutative (and commutative) algebraic geometry.

The current version is quite basic. We describe a category of certain representations of 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 the category of representations is a multisorted structure which we prove to be super-stable 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

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 Spec($\mathbb{Z}$). Conventionally, one thinks of 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. As Yu.Manin points out in [1], it is not understood even what Spec($\mathbb{Z}$) × Spec($\mathbb{Z}$) is. Manin also speculates in [1] on what dim 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 [3]) 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 Spec($\mathbb{Z}$) can be seen embedded in the arithmetic site.

Our work makes use of the above ideas and visions but approaches the problem from a somewhat different systematic model-theoretic point of view. This approach has been presented in the general setting in [4] and in more concrete applications in [5] for quantum algebras at roots of unity, in [6], [7] for a quantum-mechanical setting and in ongoing projects in the setting of schemes and stacks as well as C^*-algebras. The leading idea of this approach is that the respective "coordinate algebra" encodes a syntactic description of a semantically presentable "geometric structure", which is

supposed to be a *geometry* in a sense generalising the notion of Zariski geometry (see [9]) to the level of corresponding formal languages. One obvious advantage of this model-theoretic approach is that the resulting object is a structure in the model-theoretic sense (usually on a multi-sorted universe) and so therein direct products, projections, as well as various dimensions are well-defined. Another advantage is the availability of the toolbox of model-theoretic methods (quantifier-elimination, stability theory and the theory of Zariski geometries).

We start by associating with the ring of integers O_K of a number field K a very simple two-sorted structure on sorts A_K and Sp_K, where the standard universe for Sp_K is just the conventional $\mathrm{Spec}(O_K)$ as a set, and A_K is a sort that is projected on Sp_K by a map pr, the fibres of the projection, $\mathrm{pr}^{-1}(\mathfrak{p})$ having the 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, "monoid-representations of 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 $\mathrm{pr}^{-1}(\mathfrak{p})$ induce the norm map $\mathbb{F}_{\mathfrak{p}} \to \mathbb{F}_{\mathfrak{q}}$ for prime ideals $\mathfrak{p} \supseteq \mathfrak{q}$ 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 [8] 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 non-standard point $v \in \mathrm{Sp}_K$ in a saturated 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 multisorted structure and determine the dimensions (which we take to be just the U-ranks) of closed, and more generally definable, subsets. In particular,

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

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 [1]).

Another interesting result is that 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 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 $\mathbb{F}_w$.

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, for the sake of brevity denoted by Sp_K, is the collection of all prime ideals of O_K. Equivalently, (for Dedekind rings) the collection of maximal ideals, equivalently, the collections of irreducible representations of O_K.

The prime ideals are called the 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 Fb_p which we consider as a monoid-module, that is we ignore the additive structure on Fb_p but do distinguish the zero element $0 \in \mathrm{Fb}_p$.

Since K acts on Fb_p 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 $a_p \in \mathrm{Fb}_p$ we can identify Fb_p with $\mathbb{F}_q.a_p$, where the action of $\mathbb{F}_q^*$ on $\mathrm{Fb}_p^* = \mathrm{Fb}_p \setminus \{0\}$ is free.

The characteristic property of Fb_p is that

$$\mathrm{An}_{O_K}(\mathrm{Fb}_p) = p,$$

the annihilator of Fb_p (in fact, of any non-zero point in Fb_p) is equal to the ideal in O_K generated by p.
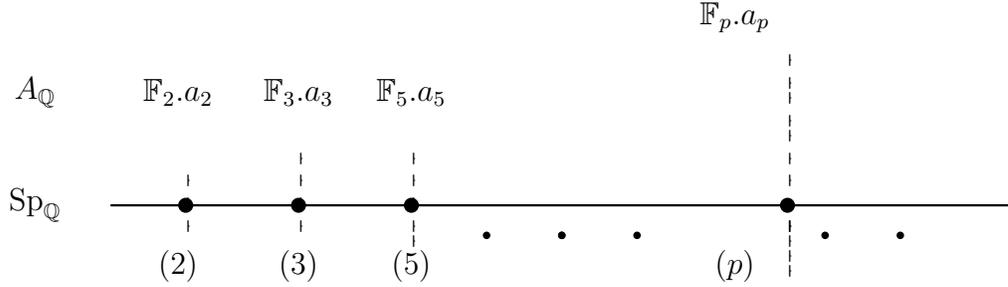
2.1. **The arithmetic plane over K.** We define the 2-sorted (standard) universe (A_K, Sp_K) with the projection

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

where

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

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

$$\mathbb{F}_p.a_p$$

$$A_{\mathbb{Q}} \qquad \mathbb{F}_2.a_2 \quad \mathbb{F}_3.a_3 \quad \mathbb{F}_5.a_5$$

$$\mathrm{Sp}_{\mathbb{Q}}$$

$$(2) \qquad (3) \qquad (5) \qquad\qquad\qquad (p)$$

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

Thus, the Fb_p^* are fibres of the projection. Note that for each standard fibre $O_K \cdot a_p = \mathrm{Fb}_p$, 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 Fb_{pK}.

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 $\bigcup_{p|m} \mathrm{Fb}_p$. 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 4.12.

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 $K, L \in \mathcal{R}$, $O_L \subseteq O_K$.

We will also use notation for definable maps

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

defined by

$$\pi_{K,L}^{\mathrm{Sp}}(pK) = pL \Leftrightarrow \mathrm{Fb}_{pK} \subseteq \pi_{K,L}(\mathrm{Fb}_{pL})$$

3.2. **Notation.** Let $\mathfrak{q} \subset O_K$ and $\mathfrak{p} \subset O_L$ are prime ideals of the corresponding rings $O_L \subseteq O_K$ such that $\mathfrak{q} \supset \mathfrak{p}$. In this case we usually use notations $pK := \mathfrak{q}$ and $pL := \mathfrak{p}$ thus we have by this notation

(1) $$pK \supseteq pL,$$

that is always "pK lies over pL in O_K".

Recall that the ring homomorphism

$$\mathrm{res}_{pK} : O_K \to O_K/pK =: \mathbb{F}_{pK}$$

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 pK. Here $\mathbb{F}_{pK} \cong \mathbb{F}_{p^m}$ for some positive integer m, which depends on K. We define

$$|pK| := p^m.$$

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

We will often refer to res_{pK} as a **naming homomorphism** as it associates elements $\gamma \in O_K$ (which we see as "names") with elements in $\mathbb{F}_{pK}$.

3.3. **Orbits.** For each prime ideal pK we associate a unique orbit Fb_{pK} on which O_K acts, for each $\gamma \in O_K \setminus pK$ and $x \in \mathrm{Fb}_{pK}$

$$x \mapsto \gamma \cdot x \in \mathrm{Fb}_{pK}$$

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

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

and we assume that the action is transitive. Thus, by definition, for any $\gamma \in O_K$ and $a \in \mathrm{Fb}_{pK}$,

(2) $$\gamma \cdot a = \bar{\gamma}_{pK} \cdot a$$

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

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

$q = q'$ **iff** for any $\gamma_1, \gamma_2 \in O_K \ \forall x \in \mathrm{Fb}_{q^K} \ \forall x' \in \mathrm{Fb}_{q'^K} \ \gamma_1 \cdot x = \gamma_2 \cdot x \leftrightarrow \gamma_1 \cdot x' = \gamma_2 \cdot x'$.

Note also that, given $a \in \mathrm{Fb}_{pK}$ we can represent any element $b \in \mathrm{Fb}_{pK}$ as

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

We will also write accordingly

$$\mathrm{Fb}_{pK} = \mathbb{F}_{pK} \cdot a_{pK},$$

where $pK \mapsto a_{pK}$ is a cross-section $\mathrm{Sp}_K \to A_K$

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

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

by its action on each orbit

$$\pi_{K,L} : \mathrm{Fb}_{pK} \to \mathrm{Fb}_{pL},$$

for each prime pK over pL, which is defined once the sections $a_{pK} \in \mathrm{Fb}_{pK}$ and $a_{pL} \in \mathrm{Fb}_{pL}$ are given: for $\eta \in \mathbb{F}_{pK}$
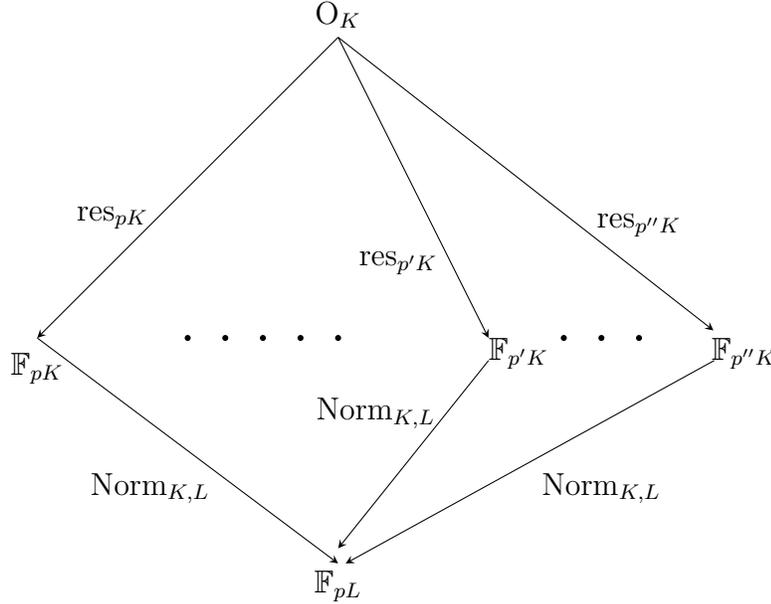
$$\pi_{K,L}(\eta \cdot a_{pK}) := \mathrm{Norm}_{K,L}(\eta) \cdot a_{pL}.$$

Note that this definition applies to all primes $p'K$ in O_K over pL and morphisms

$$\pi_{K,L} : \mathrm{Fb}_{p'K} \to \mathrm{Fb}_{pL}.$$

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 Fb_{pK}.

Naming homomorphisms:

3.7. **Lemma.** *The action of O_K on Fb_{pK} induces via $\pi_{K,L}$ an action of O_K on Fb_{pL}.*
  This action extends the action of O_L on Fb_{pL}.
  This action does not depend on the sections a_{pK} and a_{pL}.
  Proof. Given $\gamma \in O_K$ and $b \in \mathrm{Fb}_{pL}$ define

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

This is clearly an action since norm is multiplicative. We will write it without the subscript pK when the latter is clear from the context.

For $\gamma \in O_L$ we have $\bar{\gamma}_{pK} \in \mathbb{F}_{pL}$ and $\bar{\gamma}_{pK} = \bar{\gamma}_{pL}$ since $pK \cap O_L = pL$. Hence $\mathrm{Norm}_{K,L}(\bar{\gamma}_{pK}) = \bar{\gamma}_{pL}$ 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

$$(4) \qquad\qquad \pi_{K,L}(\gamma \cdot a_{pK}) = \gamma \cdot \pi_{K,L}(a_{pK}) = \gamma \cdot a_{pL}.$$

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

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

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

3.9. Corollary. *The actions* $\cdot_{pK}$ *and* $\cdot_{p'K}$ *on* Fb_{pL} *by* O_K *coincide if and only if* $p'K = pK$

Indeed, to see that the actions differ when $p'K \neq p^K$ consider a $\gamma \in p'K \setminus pK$. Then by definition for any $b \in \mathrm{Fb}_{pL}$, $\gamma \cdot_{p'K} b = 0$ and $\gamma \cdot_{pK} b \neq 0$.

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

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

It follows that for a non-zero $y \in \mathrm{Fb}_{pL}$

$$(5) \qquad |\pi_{K,L}^{-1}(y) \cap \mathrm{Fb}_{pK}| = \frac{|pK| - 1}{|pL| - 1}.$$

Now note that one can determine, for $y \in A_L$, the number $|\pi_{K,L}^{-1}(y)|$ once one knows that $y \in \mathrm{Fb}_{pL}$ and one knows all the $p'K$ which lie over pL in O_K.

3.11. Special predicates on Sp_L**.** We consider the $\pi_{K,L}$**-multiplicities** of points $y \in A_L$ to be the numbers $|\pi_{K,L}^{-1}(y)|$. For positive integers N we set

$$\psi_{K,L}^N := \{y \in A_L : |\pi_{K,L}^{-1}(y)| \leq N\},$$

definable subsets of A_L.

Define

$$\Psi_{K,L}^N := \mathrm{pr}(\psi_{K,L}^N) = \{p \in \mathrm{Sp}_L : \exists y \in A_L \left(|\pi_{K,L}^{-1}(y)| \leq N \ \& \ \mathrm{pr}(y) = p\right)\}$$

Given $pL \in \mathrm{Sp}_L$ set

$$N_{pL} = \min\{N : pL \in \Psi_{K,L}^N\}.$$

3.12. Lemma. *Assume that the extension* $(K : L)$ *is Galois. Then*

$$N_{pL} = \frac{|pL|^{d_F} - 1}{|pL| - 1} d_p, \quad d_F := \deg(\mathbb{F}_{pK} : \mathbb{F}_{pL}) \ \text{and} \ d_p \ \text{divides} \ |K : L|.$$

Proof. This is a direct consequence of (5). $\square$

3.13. Remark. The case $d_F = 1$ corresponds to the fact that the minimal polynomial of α over L splits into linear factors modulo pL. Then, except for finitely many such pL (over which pK ramifies) there are exactly $|K : L|$ distinct prime ideals pK over pL and thus $d_p = |K : L|$.

Since for prime $p \in \mathbb{Z}$, $|pL| \geq p$, we have:

3.14. Corollary. *There is an N such that $N_{pL} \leq N$ for infinitely many $pL \in \mathrm{Sp}_L$ if and only if there are infinitely many $pL \in \mathrm{Sp}_L$ such that $\mathbb{F}_{pK} = \mathbb{F}_{pL}$. In this case the minimal such N is equal to $\mathrm{d}(K, L) := |K : L|$ and the minimal polynomial f_K over O_L splits into linear factors modulo pL.*

The set $\Psi_{K,L}^{\mathrm{d}(K,L)}$ is infinite and for every $N \geq \mathrm{d}(K, L)$,

$$\Psi_{K,L}^N = \Psi_{K,L}^{\mathrm{d}(K,L)} \cup P_N, \text{ some finite } P_N.$$

We will write $\Psi_{K,L}$ for $\Psi_{K,L}^{\mathrm{d}(K,L)}$.

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

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

The Chebotarev density theorem ([2], 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 $\mathfrak{p}$ has a density. Moreover, it determines the density in terms of the structure of $\mathrm{Gal}(K/L)$.

An immediate corollary to the Chebotarev density theorem is that

$$\mathrm{dn}\, \Psi_{K,L} = \frac{1}{\#\mathrm{Gal}(K/L)} = \frac{1}{|K : L|}.$$

(Note that the density of finite subsets is 0, so $P_N = 0$.)

In particular, $\Psi_{K,L}$ is infinite, as is its complement.

Moreover, since for two Galois extensions K_1 and K_2 the splitting fields for f_{K_1} and f_{K_2} modulo $\mathfrak{p}$ is the composite of the splitting fields for each of those, and is equal to the splitting field of f_K, for $K = \mathbb{Q}[\alpha_1, \alpha_2]$, we get that

$$\Psi_{K_1,L} \cap \Psi_{K_2,L} = \Psi_{K,L}$$

and so any intersection of the $\Psi_{K_i,L}$ has a well-defined positive density.

3.16. Corollary. An intersection of finite family of special subsets of Sp_L is nonempty:

$$\bigcap_{i \in I} \Psi_{K_i,L} = \Psi_{K,L} \neq \emptyset.$$

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

Proof. First we note that it is enough to prove the theorem for the intersection

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

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

Secondly, as shown above $\bigcap_{i \in \{i_1, \ldots i_m\}} \Psi_{K_i,L}$ can be replaced by some $\Psi_{K,L}$.

Now we prove,

Claim. The density of the set of the form

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

is well-defined.

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

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

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

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

This proves the claim.

Now it remains to see that

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

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

Remark. The density is a measure on the respective boolean algebra.

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

Consider the formula with free variables q,q' in sort Sp_K :
(6)

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

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

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

Under our assumptions $\mathrm{Norm}_{\mathbb{F}_q,\mathbb{F}_p}:\mathbb{F}_q\to\mathbb{F}_p$ 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 $\bar\alpha_q=\mathrm{res}_q(\alpha)\in\mathbb{F}_p$.

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

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

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

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

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

---

[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

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 $\mathrm{res} : \mathrm{O}_K \to \mathbb{F}_{pK}$ can be seen as assigning names in O_K to elements in $\mathbb{F}_{pK}$. We will consider elements of O_K as extra constant symbols and $\mathbb{F}$ a structure in the **language of rings with names in O_K.** We denote the language $L_{\mathrm{rings}}(K)$.

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

We assume that for finite $\mathbb{F}_q$,

$$(7) \qquad\qquad\qquad\qquad \mathbb{F}_q \cong \mathbb{F}_{q'} \Leftrightarrow q = q$$

We also assume that,

$$(8) \qquad \text{for every prime } pK \subset \mathrm{O}_K \text{ there is } q \in \mathcal{PF}_K \text{ such that } \mathbb{F}_q = \mathbb{F}_{pK} := \mathrm{O}_K/pK.$$

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

$$(9) \qquad\qquad \mathrm{Norm}_{K/L} : \mathbb{F}_{pK} \to \mathbb{F}_{pL}, \quad j_{K/L} : \mathbb{F}_{pL} \to \mathbb{F}_{pK} \text{ for } \mathbb{F}_{pK} \supseteq \mathbb{F}_{pL}.$$

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

Note that

$$(10) \qquad\qquad\qquad\qquad \mathrm{Nm}_{K/L} \text{ is surjective}$$

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

We also assume that

$$(11) \qquad\qquad\qquad \mathbb{F}_{pK} = \mathbb{F}_{pL}(\bar{\alpha}), \text{ for } \alpha \text{ such that } K = L(\alpha)$$

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

4.2. Remarks.

(i) Note that $\mathbb{F}_{pK}$ is determined by (11) uniquely, up to the naming, and we have one-to-one correspondence between extensions of $\mathbb{F}_{pL}$ in the language $L_{\mathrm{rings}}(K)$ and the residued maps res_{pK}.

(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 q separately.

4.3. Lemma.

There exists a bijection

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

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

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

and for any $\gamma \in \mathrm{O}_K, \; x \in A_K$

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

Proof. For each $L \subset K$ choose the sections $Sp_L \to A_L$, $pL \mapsto a_{pL}$. Then

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

determines the map with required properties. □

4.4. **The space of pseudofinite fields. Corollary.** *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*

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

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 $pL \in \mathrm{Sp}_L \cap M$ we have $\mathrm{pr}^{-1}(pL) \subset M$,
   (iii) and for any $K \supseteq L$ every $pK \in \mathrm{Sp}_K$ such that $pL \subseteq pK$ 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 $pK \in \mathrm{Sp}_K$, such that $pK = \mathrm{pr}(x)$. In its turn $\mathrm{cl}(pK)$ contains, for every $L \subseteq K$, the point $pL = \pi^{\mathrm{Sp}}_{K,L}(pK)$. But, at the same time, by definition $pK \in \mathrm{cl}(pL)$. Summarising, one gets $\mathrm{cl}(x) = \mathrm{cl}(pK)$ by starting from $p \in \mathrm{Sp}_{\mathbb{Q}}$, the unique prime in $\mathbb{Z}$ under pK, and then adjoining all primes pL over p, for all L, along with $\mathrm{pr}^{-1}(pL)$.

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 $\varphi(v_1, \ldots, v_n)$ 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) Fb_{pK} with monoid homomorphism $\pi_{K,L} : \mathrm{Fb}_{pK} \to \mathrm{Fb}_{pL}$ 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 pK in all sorts. Hence the embedding reduces to the family of embeddings $\mathrm{Fb}_{pK} \subseteq \mathrm{Fb}'_{pK}$. The Tarski-Vaught test verifies that this is an elementary embedding, $\mathrm{cl}(a) \preceq \mathrm{cl}(a)'$. □

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 $\mathbb{F}_{pK}$ and its definable subfields $\mathbb{F}_{pL}$. Each of these is a finite extension of $\mathbb{F}_{p\mathbb{Q}}$, the minimal field in $\mathrm{cl}(a)$, and so interpretable in $\mathbb{F}_{p\mathbb{Q}}$. The latter is supersimple of finite rank. $\qquad\square$

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 $a \in \mathbb{F}_q$ for some pseudofinite field $\mathbb{F}_q$, for $q = q(a) \in \mathrm{Sp}_K$, some number field K. The type $\mathrm{tp}(a, \mathbb{F}_q)$ of $\mathbb{F}_q$ 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 $\mathbb{F}_q$ and all the other fields in $\mathrm{cl}(a)$ are pseudofinite, each formula in $\mathrm{tp}(a, \mathbb{F}_q)$ is realised by some pair with a finite field $\mathbb{F}_{p^n}$ in place of $\mathbb{F}_q$. It implies that the same collection of formulas is a type in $(\mathcal{AF}'_K, \mathcal{PF}'_K)$, and so has a realisation $a', \mathbb{F}_{q'}$. 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 $\mathbf{e}$. $\qquad\square$

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

For the last part of the statement see [10].

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

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

and, for q infinite,

$$(15) \qquad \mathrm{tp}(q/N) = \mathrm{tp}(q'/N) \Leftrightarrow \text{ for all } L \supset K : \ q \in \Psi_{L,K} \leftrightarrow q' \in \Psi_{L,K}$$

(14) follows from 4.4, 4.8 and 4.9.

In order to prove (15) invoke Kiefe's criterium (see [10], 4.7): $\mathbb{F}_{pK} \equiv \mathbb{F}_{p'K}$ in the language $L_{\text{rings}}(K)$ if and only if for every irreducible polynomial $f(x)$ over K,

$$\mathbb{F}_{pK} \vDash \exists x\, f(x) = 0 \Leftrightarrow \mathbb{F}_{p'K} \vDash \exists x\, f(x) = 0,$$

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

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

Since $K^{alg} \cap \mathbb{F}_{pK} : K$ is Galois (for any pseudofinite field containing K), the assumption $\mathbb{F}_{pK} \vDash \exists x\, f(x) = 0$ for an irreducible f is equivalent to the assumption that $f(x)$ splits into linear factors over $K^{alg} \cap \mathbb{F}_{pK}$. Let $L \supset K$ be the splitting field of $f(x)$. Then we have just proved that $L \subseteq \mathbb{F}_{pK}$ via the naming homomorphism. By 3.13 this means that $pK \in \Psi_{L,K}$. $\qquad\square$

4.11. **Corollary.** *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 $\text{pr}(v) = p$ over $p \in \text{Sp}_K$ is 0 or 1 depending on whether p 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 $\text{cl}(a)$. If a 1-type contains a formula $\text{pr}(v) = p$ for a parameter p, then it is a type of an element of the fibre Fb_p, which is either finite, if p is finite, or strongly minimal, so of U-rank 1. The unique complete 1-type which negates all formulas $\text{pr}(v) = p$ is of U-rank 2. $\qquad\square$

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

- $v \in \text{Sp}_K$,
- $v = q$, for $q \in \text{Sp}_K$, finite,
- $v \in \Psi_{K,L}$

and

- *existential formulas $\varphi(v_1, w_1, \ldots, v_n, w_n, p)$ 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 $\text{cl}(p)$, $p \in \text{Sp}_{\mathbb{Q}}$, $L_1, \ldots, L_n \in \mathcal{R}$.*

Proof. By 4.6 and 4.10(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. $\qquad\square$

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 $\Psi_{K,L}$, singletons and their finite unions, for all Galois extension K of L.

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

- the graph of pr restricted to $A_L \times \text{Sp}_L$, $L \in \mathcal{R}$;

- the graph of $\pi_{K,L}$, for $K, L \in \mathcal{R}$;
- subsets of A_L of the form $\psi_{K,L}$ and subsets of Sp_L of the form $\Psi_{K,L}$, $L \in \mathcal{R}$;
- 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 $\varphi(v_1, w_1, \ldots, v_n, w_n, p)$ relativised to $\mathrm{cl}(p)$, $p \in \mathrm{Sp}_{\mathbb{Q}}$, $L_1, \ldots, L_n \in \mathcal{R}$.

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 $\pi_{K,L}^{-1}(S)$ 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 $\Psi_{M,L}$.

Claim.

$$\pi_{K,L}^{-1}(\Psi_{M,L}) = \Psi_{KM,K}$$

where KM is the composite of fields.

Proof. Let $pL \in \Psi_{M,L}$, $M = L[\alpha]$, $f \in L[x]$ the minimal polynomial for α and $\alpha_1, \ldots, \alpha_n$ are Galois conjugates of α over L. Then we have $KM = K[\alpha_i]$, for $i = 1, \ldots, n$ and

(16) $$f(\alpha_i) \in pL, \ i = 1, \ldots, n.$$

Then

(17) $$f(\alpha_i) \in pK, \ i = 1, \ldots, n \text{ for every prime } O_K \supset pK \supseteq pL$$

which implies $pK \in \Psi_{KM,K}$. This proves

$$pL \in \Psi_{M,L} \Rightarrow pK \in \Psi_{KM,K} \text{ for every prime } O_K \supset pK \supseteq pL.$$

Now we prove the converse. Suppose

$$pK \in \Psi_{KM,K} \text{ for every prime } pK \supseteq pL.$$

This is equivalent to say that $\mathbb{F}_{pKM} = \mathbb{F}_{pK}$ and so to (17). But

$$\bigcap_{pK \supseteq pL} pK = pL$$

and hence we proved (16) and $pL \in \Psi_{M,L}$. This finishes the proof of the claim and of the lemma. $\qquad\square$

5.2. Compact models. Note that the sorts Sp_L and A_L are not compact since the intersection $\bigcap_{i \in I} \Psi_{K_i,L}$, 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 3.16.

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

(18) $$\bigcap_{K:L \text{ Galois}} \Psi_{K,L}$$

in each sort Sp_L. 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 repre-
    sentations;

(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

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

5.3. 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 $pL \in \mathrm{Sp}_L(\mathfrak{M})$ 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 $\mathbb{F}_{pL}$ over such an infinite prime pL is characterised as a pseudo-finite field containing $\mathbb{Q}^{alg}$ with a naming homomorphism

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

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

(d) The fibres over infinite pL have the form

$$\mathrm{Fb}_{pL}(\mathfrak{M}) = \mathbb{Q}^{alg} \cdot a_{pL}$$

for a non-zero element a_{pL} of the fibre.

Proof. We use the analysis in 3.13 for finite primes in $\Psi_{K,L}$ and extend the conclusions to infinite primes satisfying the same first-order condition. The Tarski-Vaught test along with the statement of theorem 4.12 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 and so $d_p = \deg(K : L)$, that is $\mathbb{F}_{pK} = \mathbb{F}_{pL}$ and $\mathrm{Norm}_{K,L}$ is the identity map. The d_p distinct prime ideals $p^{(i)}K \in \mathrm{Sp}_K$, $(i = 1, \ldots, d_p)$ lying over pL give rise to d_p naming homomorphisms

$$\mathrm{res}_{p^{(i)}K} : \mathrm{O}_K \to \mathbb{F}_{pL}, \quad \ker(\mathrm{res}_{p^{(i)}K}) = p^{(i)}K$$

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

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

The distinct prime ideals $p^{(i)}K$ extending pL 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 [10]).

(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). $\square$

5.4. The minimal complete model. We call $\mathcal{N}$ 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

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

5.5. 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 pK over pL, for K/L Galois, are conjugated under the action of Galois group $\mathrm{Gal}(K : L)$.

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

$$E_{pL} = \mathbb{Q}^{alg} \cap \mathbb{F}_{pL}$$

and the naming homomorphism

$$\mathrm{res}_{pL} : O_L \to E_{pL}.$$

(c) The fibres over infinite pL have the form

$$\mathrm{Fb}_{pL}(\mathfrak{N}) = E_{pL} \cdot a_{pL}$$

for a non-zero element a_{pL} of the fibre.

Proof. Same arguments as in 5.3.$\square$

5.6. 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 [9].

6. The universal cover

6.1. The coarse cover. Let $O_{\mathcal{R}} = \bigcup\{O_K : O_K \in \mathcal{R}\}$. 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 $\pi_{K,L}^{\mathrm{Sp}}$, $K \supset L$, determine a projective system.

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

By definition we will have maps

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

satisfying

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

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

$$(19) \qquad \forall x_1, x_2 \in A_{\mathcal{R}} \; x_1 = x_2 \leftrightarrow \bigwedge_K \pi_{\mathcal{R},K}(x_1) = \pi_{\mathcal{R},K}(x_2)$$

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

$$\mathbb{F}_{\tilde{p}} = \bigcup\{\mathbb{F}_{pK} : \pi_{\mathcal{R},K}(\mathrm{Fb}_{\tilde{p}}) = \mathbb{F}_{pK}.a_{\pi_{\mathcal{R},K}(\tilde{p})}\},$$

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

$$\mathrm{res}_{\tilde{p}} : O_{\mathcal{R}} \to \mathbb{F}_{\tilde{p}}.$$

Clearly,

$$A_{\mathcal{R}} := \bigcup\{\mathrm{Fb}_{\tilde{p}} : \tilde{p} \in \mathrm{Sp}_{\mathcal{R}}\}.$$

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

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

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_p and $\mathrm{res}'_p : O_\mathcal{R} \to \mathbb{F}_{\tilde{p}}$, there is a $\sigma \in \mathcal{G}_\mathbb{Q}$ such that $\mathrm{res}'_p = \mathrm{res}_p \circ \sigma$. In other words $\mathcal{G}_\mathbb{Q}$ acts transitively on the fibre and

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

Note that

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

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

6.3. Question.

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

6.4. The fibre of $A_\mathcal{R}$ over the infinite splitting prime.

In this case $\tilde{p}$ lies over an infinite splitting prime $\mathbf{p}$ (which is unique up to its first-order type) and $O_\mathcal{R}$ contains all integral extensions, we have that $O_\mathcal{R} \subset \mathbb{Q}^{alg}$ is the ring of all integral algebraic numbers, $\pi_{\mathcal{R},1}$ is an isomorphism and $\mathbb{F}_{\tilde{p}} = \mathbb{F}_\mathbf{p}$, a pseudo-finite field which contains $\mathbb{Q}^{alg}$ and the latter is equal to the subfield of named elements of $\mathbb{F}_\mathbf{p}$ (see 5.3).

Again we will have as many points $\tilde{p}$ over $\mathbf{p}$ as there are naming homomorphisms $\sigma : O_\mathcal{R} \to \mathbb{Q}^{alg} \subset \mathbb{F}_\mathbf{p}$. 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 $(\pi^{\mathrm{Sp}}_{\mathcal{R},1})^{-1}(\mathbf{p})$

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

6.5. Proposition.

The action of a $\sigma \in \mathcal{G}_\mathbb{Q}$ on the fibre $(\pi^{\mathrm{Sp}}_{\mathcal{R},1})^{-1}(\mathbf{p})$ 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. $\square$

7. 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 5.3) 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 [3]. 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 [11] the first author introduced polynomial invariants of definable subsets in totally categorical theories and in [12] 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] Yu.Manin, *The Notion of Dimension in Geometry and Algebra*, Bull. of the AMS, 43 (2), 2006, 139-161.

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

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

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

[5] 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

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

[7] B.Zilber, *The semantics of the canonical commutation relation*, In preparation.

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

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

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

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

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

MATHEMATICAL INSTITUTE, UNIVERSITY OF OXFORD, OXFORD