Model Theory of Adele Rings over Number Fields

Joint work with Jamshid Derakhshan.
Issues of Axiomatization joint with Paola D'Aquino

Basic Notions and Notation Concerning Number Fields

Our basic first-order language is that of ring theory with $+$, -, ., 0 and 1.
A number field $\mathbb{K}$ is a finite-dimensional extension of $\mathbb{Q}$.
$\mathbb{O}_K$ is the ring of integers of $\mathbb{K}$.
Absolute values of K are of basic importance (See Cassels and Frohlich, Algebraic Number Theory, for all one needs to know).
On $\mathbb{Q}$ these (after a natural normalization) correspond to nonzero prime ideals of $\mathbb{Z}$ and to the standard absolute value given by the embedding of $\mathbb{Q}$ in $\mathbb{R}$. For the prime p the corresponding absolute value is the map sending x $p^{-v_p(x)}$ where v_p is the standard p-adic valuation.

General $\mathbb{K}$

For general $\mathbb{K}$ we replace the prime numbers p by prime ideals $\mathfrak{P}$ of $\mathbb{O}_K$, and the real embedding of $\mathbb{Q}$ by complex (including real) embeddings of $\mathbb{K}$, with suitably normalized absolute values. To $\mathfrak{P}$ there corresponds a (suitably normalized) valuation $v_{\mathfrak{P}}$, extending v_p,
where (p) is the restriction of $\mathfrak{P}$ to $\mathbb{Z}$. Moreover, any (p) extends to finitely many $\mathfrak{P}$. These give the nonarchimedean absolute values. In
addition, the real absolute value of $\mathbb{Q}$ extends to at most finitely many (generally complex) absolute values. This behaviour under extension persists for all extensions of
number fields. Note that in the nonarchimedean cases the extension/restriction corresponds to extension and restriction of valuations.

Residue Fields, Value Groups, Completions for Nonarchimedean Valuations

Let (p) and $\mathfrak{P}$ be as on previous page. Clearly v_p is the standard p-adic valuation on $\mathbb{Q}$, with residue field $\mathbb{F}_p$ and value group $\mathbb{Z}$ with $v_p(p) = 1$. $v_{\mathfrak{P}}$ has residue field a finite extension of $\mathbb{F}_p$ and value group a finitely ramified extension of $\mathbb{Z}$.
All valuations occurring as above have completions, which are henselian and immediate extensions of the valuations on the $\mathbb{O}_K$.
We write these as $K_{\mathfrak{P}}$.
In the archimedean case the completions are either $\mathbb{R}$ or $\mathbb{C}$ (and the absolute values are suitably normalized).
We write V_K for the set of normalized absolute values of K, and note the restriction/extension phenomenon for extensions of number fields.

Basic Structure on $V_{\mathbb{K}}$

$V_{\mathbb{Q}}$ is the union of the set of p-adic absolute values and the singleton containing the real absolute value. We write ∞ for the real absolute value, and have the decomposition of $V_{\mathbb{Q}}$ as the union of the set of nonarchimedean absolute values $nonarchimedean_{\mathbb{Q}}$ and the set of archimedean absolute values $archimedean_{\mathbb{Q}}$, whose only member is ∞.

We naturally index $nonarchimedean_{\mathbb{Q}}$ by the primes p.

For general $\mathbb{K}$ one defines $nonarchimedean_{\mathbb{K}}$ and $archimedean_{\mathbb{Q}}K$ in the same way. The latter is always finite.

Each inclusion $\mathbb{K} \to \mathbb{L}$ of number fields induces a ring inclusion from $\mathbb{O}_K$ to $\mathbb{O}_L$, and a surjective restriction maps from $nonarchimedean_{\mathbb{L}}$ to $nonarchimedean_{\mathbb{K}}$ and from $archimedean_{\mathbb{L}}$ to $archimedean_{\mathbb{K}}$. Moreover, each map is finite to one.

Finally, these restrictions are functorial.

The adele rings $\mathbb{A}_K$. 1

It will simplify notation if we use $v_{\mathfrak{P}}$ for an arbitrary element of $\mathbb{V}_K$ and $K_{\mathfrak{P}}$ for the corresponding completion.
Note that the latter are exactly the locally compact fields of characteristic 0.
To $\mathbb{K}$ we first associate a relatively uninteresting von Neumann regular topological ring, namely the product of the family $(K_{\mathfrak{P}} : v_{\mathfrak{P}} \in \mathbb{V}_K)$.
This is not locally compact, but well understood model-theoretically by Ax and Feferman-Vaught.
A more interesting subring is the corresponding product of the valuation rings $\mathbb{O}_{K_{\mathfrak{P}}}$ of the $K_{\mathfrak{P}}$.

The adele rings $\mathbb{A}_K$ 2

This is compact, and has a well-understood model theory by Derakhshan-Macintyre using Ax, Feferman-Vaught , and joint work with Cluckers and Leenknecht on a (nearly existential) uniform ring definition of the valuation rings used.
But the right ring for number theory is the intermediate $\mathbb{A}_K$, the ring of all f in the full product , such that $f(v_{\mathfrak{P}})$ is in the valuation ring for all but finitely many many elements of $\mathbb{V}_K$. This is locally compact. It is called the adele ring over $\mathbb{K}$

The adele rings $\mathbb{A}_K$ 3

These have, for each $\mathbb{K}$ a very well-understood model theory in the language of rings. The basic results
(not in the simple ring formalism) were obtained around 1978 by Weisspfenning, but much generalized and clarified in the work of D-M over the last ten years.
The work uses the notion of restricted product from the work of Feferman-Vaught (1959).
The analyses are uniform in K, modulo the index sets. Each individual $\mathbb{A}_K$ is decidable, and with well-understood definability theory, but the work does not yield
decidability of the class of all $\mathbb{A}_K$ because of very difficult problems about unbounded ramification.

Decoding $\mathbb{K}$ from $\mathbb{A}_K$

$\mathbb{K}$ is diagonally embedded in $\mathbb{A}_K$. In the idelic situation where the group of units of the adeles gets the idelic topology, the multiplicative group of
$\mathbb{K}$ is discretely embedded embedded in the group of ideles of norm 1, and the quotient is compact, a fact deeply connected to Finiteness of Class Number.
Early on one asked if $\mathbb{K}$ is determined up to isomorphism by its adele ring (which subtly encoded the local structure of $\mathbb{K}$)
In this talk we look at logical aspects of this issue, and relate them to the main discoveries of number theorists like Iwasawa, Perlis, et al.
We point out at the outset that $\mathbb{K}$ is undecidable, whereas $\mathbb{A}_K$ is decidable, so there is no definition of the number field in its adele ring.But this has no
implications for the decoding problem.

Refined Undecidability

In many cases $\mathbb{K}$ has undecidable universal-existential theory by the deep work of Koenigsmann and Park. This is known for all $\mathbb{K}$ under the assumption of part of Tate-Shafarevich Conjecture (by Mazur and Rubin).

Coding $\mathbb{V}$ by idempotents in $\mathbb{A}_K$

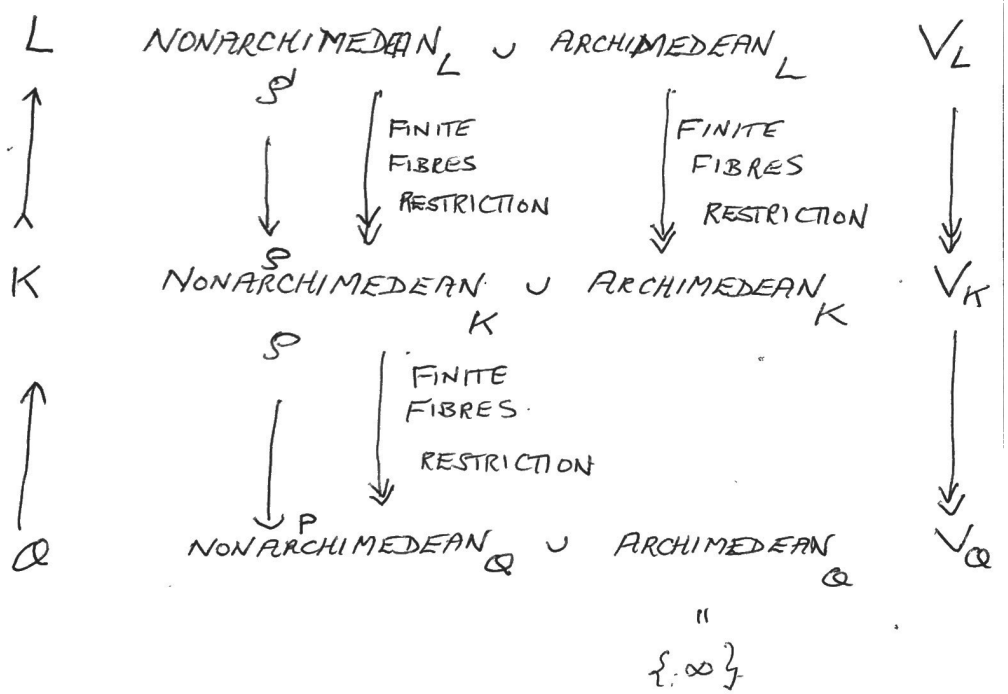
The key point is that the ring $\mathbb{A}_K$ has enough idempotents to code the elements of the index set $\mathbb{V}_{\mathbb{K}}$, namely the f which take value 1 at a single
element of the index set, and take value 0 elsewhere. These are in fact the minimal idempotents of the index set. Moreover, once one makes this identiication, one can easily interpret,
ring- theoretically , the notion of the fibre at an element of the index set , and the notion of the residue field of that fibre, and the notion of the valuation ring at that fibre (appealing to DMCL). All details can be found in DM. In particular, for each standard prime p , the following notion is definable:
The residue field at $v_{\mathfrak{P}}$ has characteristic p.
In each adele ring $\mathbb{A}_K$ the preceding set is finite , for each p.
It will be crucial for us to understand the finer structure of such sets.

THE DIAGRAM SO FAR

V_L WILL BE THE INDEX SET

FOR

$\mathbb{A}_L$ (adele ring).



Relating Definability to Extension and Restriction of Absolute Values 1

Fix $\mathbb{K}$ and p as above. Continuing the identification of minimal idempotents and fibres, we write $p - Fib$ for the finite set of minimal idempotents where the fibre has characteristic p. This set is definable, for fixed p, uniformly in $\mathbb{K}$. If we take an elementary property of valued fields, we get a corresponding elementary property of $\mathbb{K}$ by considering the elements of $p - Fib$ whose fibres satisfy that property. Another way to get an elementary property is to say that there are exactly m elements of $p - Fib$ whose fibre satisfies the elementary property.
We should not forget the archimedean absolute values and their fibres, which can be either $\mathbb{R}$ or $\mathbb{C}$ (and it is an elementary condition on a minimal idempotent which kind of fibre it has. We cannot dispense with considering these, but the p case is much more important, and we concentrate on it.

Relating Definability to Extension and Restriction of Absolute Values 2

We approach the notion of a p-pattern.
Again fix $\mathbb{K}$. Consider the ideal $p\mathbb{O}_{K_{\mathfrak{P}}}$ in the ring of integers of $\mathbb{K}$. It factors, essentially uniquely, into a product of powers of distinct prime ideals $P_1^{e_1} \cdots P_g^{e_g}$. Each such prime extends (p), and every extension of (p) occurs. This gives us the right way to look at $p - Fib$. For each extension $v_{\mathfrak{P}}$ we have its residue field $k_{v_{\mathfrak{P}}}$ of dimension $f_{v_{\mathfrak{P}}}$ over $\mathbb{F}_p$. We have also the ramification degree $e_{v_{\mathfrak{P}}}$. which is the same as the exponent to which the corresponding prime divides p . Note first that for each m it is an elementary condition on (the idempotent corresponding to) $v_{\mathfrak{P}}$ that the corresponding f is $\leq m$, and similarly for the ramification exponent.

p-patterns

It is also an elementary condition, for each g, that there are exactly g primes extending p . The main obstruction to progress is to understand how the f, e and g introduced above depend on $\mathbb{K}$.

We attach to p and $\mathbb{K}$ a so-called p-pattern $\Sigma_{p,\mathbb{K}}$ as follows. Suppose p has g distinct extensions , and enumerate the corresponding f in order (perhaps with repetitions) as $< f_1, \ldots, f_g >$. This sequence is the p-pattern. Note that for now we have no reference to the ramification (though there is no obstruction to bringing it in now).

Basic Equality

Let $n = [\mathbb{K} : \mathbb{Q}]$. Fix p, and let $(P)_1, ...(P)_g$ be the distinct extensions of (p) to $\mathbb{O}_{\mathbb{K}}$. Let
$f_1, ...f_g$ and $e_1, ...e_g$ be the corresponding inertia and ramification degrees as above. Then (See Cassels-Frohlich) we have the fundamental

$$\sum_{j=1}^{g} f_j e_j = n.$$

Immediate consequences for our analysis are

1. $g \leq n$
2. $f_j \leq n$
3. $e_j \leq n$

This makes it clear that it would be of basic importance to show that the condition on $\mathbb{A}_{\mathbb{K}}$ that the dimension of $\mathbb{K}$ is n , is IN SOME NATURAL SENSE elementary , for fixed n, uniformly in $\mathbb{A}_{\mathbb{K}}$

Using Cebotarev's Theorem

Fix $\mathbb{K}$, of dimension n , and let $\mathbb{L}$ be the normal closure of $\mathbb{K}$. By *Cebotarev* there are infinitely many p which are unramified in $\mathbb{L}$ and split completely (i.e have residue field dimension 1). Pick such a p and consider $p - Fib$ in the adeles of $\mathbb{K}$. That set has cardinality n.
Now, for any p, it is an elementary condition on $\mathbb{A}_{\mathbb{K}}$ (depending on p!) that $p - Fib$ satisfies the above Cebotarev condition. Thus, we have our first theorem (well-known to number-theorists in a different formulation).

Theorem
If $\mathbb{A}_{\mathbb{K}_1} \equiv \mathbb{A}_{\mathbb{K}_2}$ *then*

$$[\mathbb{K}_1 : \mathbb{Q}] = [\mathbb{K}_2 : \mathbb{Q}]$$

IMPORTANT NOTE: We have not shown the existence of a single sentence of ring theory detecting fixed dimension n.

Normal $\mathbb{K}$

Cebotarev's Theorem gives

Theorem

If $\mathbb{K}$ is normal, then if $\mathbb{L}$ has adele ring elementarily equivalent to that of $\mathbb{K}$, then $\mathbb{L} = \mathbb{K}$.

What is not properly understood is the nature of the sets of primes splitting completely in $\mathbb{K}$, as $\mathbb{K}$ varies.

The Perlis Formalism

Recall the definition of $\Sigma_{p,\mathbb{K}}$, the p-pattern of $\mathbb{K}$. It is a sequence of numbers (with monotonicity constraint) not mentioning p and $\mathbb{K}$, and one must eventually try to figure out which such sequences can occur as p and $\mathbb{K}$ vary.
For now we just work abstractly with a sequence $< f_1, ...f_g >$ subject only to the monotonicity constraint, and call such a thing a splitting type.
Following Perlis, we write A for a splitting type., and then define:

$$\mathbb{P}_{\mathbb{K}}(\mathbb{A}) = \{p : \Sigma_{p,\mathbb{K}} = \mathbb{A}\}$$

.
Note that by the Basic Lemma there are, for fixed $\mathbb{K}$ only finitely many $\Sigma_{p,\mathbb{K}}$, and so $\mathbb{P}_{\mathbb{K}}(\mathbb{A})$ is empty for all but finitely many $\mathbb{A}$.

Arithmetic Equivalence of Number Fields, and Elementary Equivalence of their Adele Rings

It is clear that if If $\mathbb{A}_{\mathbb{K}_1} \equiv \mathbb{A}_{\mathbb{K}_2}$ then, for each $\mathbb{A}$, $\mathbb{P}_{\mathbb{K}_1}(\mathbb{A}) = \mathbb{P}_{\mathbb{K}_2}(\mathbb{A})$. This latter condition is called here Decomposition Equivalence of the fields.

Perlis calls it " Arithmetic Equivalence", but we find this unnatural, due to its failure to incorporate consideration of ramification.

A Big Theorem of Perlis

Theorem

$\mathbb{K}_1$ and $\mathbb{K}_2$ are Decomposition equivalent if and only if they have the same zeta function.

Another

Theorem

Suppose $\mathbb{A}_{\mathbb{K}_1}$ *is Decomposiion equivalent to* $\mathbb{A}_{\mathbb{K}_2}$.
Then

1. $\mathbb{K}_1$ *and* $\mathbb{K}_2$ *have the same discriminant.*
2. $\mathbb{K}_1$ *and* $\mathbb{K}_2$ *have the same number of real(respectively complex) absolute values.*
3. $\mathbb{K}_1$ *and* $\mathbb{K}_2$ *have the same normal closure.*
4. $\mathbb{K}_1$ *and* $\mathbb{K}_2$ *have isomorphic unit groups.*

The proof is quite nontrivial.
Corollary For fixed $\mathbb{K}$ there are only finitely many $\mathbb{L}$ such that $\mathbb{K}$ and $\mathbb{L}$ have elementarily equivalent (indeed, Decomposition equivalent) adele rings.
Proof. By (1) and Hermite- Minkowski Finiteness Theorem for Discriminants. Alternatively, one can use 3.

The Role of Ramification. Enriched p-Patterns

Note that we have not yet used the ramification exponents in our proofs. But we have observed that significant things about local ramification can be expressed in the ring language for adeles. Thus we now pass from p-patterns to $Enrichedp - Patterns$. The setting is that where we first defined p-patterns.
p and $\mathbb{K}$ are given. We attach to p and $\mathbb{K}$ first a so-called p-pattern $\Sigma_{p,\mathbb{K}}$ as follows. Suppose p has g distinct extensions , and enumerate the corresponding$f$ in order (perhaps with repetitions) as $< f_1, \ldots, f_g >$. We get the enriched p-pattern as a $2g$ tuple $< f_1, e_1, ..., f_g, e_g >$, but the f_j may not be exactly the f_j of the original pattern. We look at all pairs , f , e occurring, where the e is the ramification corresponding to the inertia f. We now lexicographically order the set of pairs , as $< f_j, e_j >$,and the sequence $< f_1, e_1, ..., f_g, e_g >$ is defined as the enriched p-pattern. The basic equality bounds the enriched p-patterns uniformly in terms of the dimension of $\mathbb{K}$, uniformly in K and p.

Elementary Equivalence and Isomorphism 1

We define enriched splitting types completely analogously to splitting types. We denote by $Enriched\Sigma_{p,\mathbb{K}}$ the enriched p-pattern (i.e enriched splitting type). We now use $\mathbb{A}$ for enriched splitting types, and define
$Enriched\mathbb{P}_{\mathbb{K}}(\mathbb{A})$ as the set of p whose enriched p-pattern in $\mathbb{K}$ is $\mathbb{A}$.
We define (Decomposion+ Ramification) Equivalence for $\mathbb{K}$ and $\mathbb{L}$ to mean that

$$Enriched\mathbb{P}_{\mathbb{K}} = Enriched\mathbb{P}_{\mathbb{L}}$$

.
We observe that just as elementary equivalence of adele rings implies inertial equivalence of the fields, so does it imply inertial-ramification equivalence.

Elementary Equivalence and Isomorphism 2

Suppose that $\mathbb{K}$ and $\mathbb{L}$ are Decomposition-Ramification equivalent (for example, that they have elementarily equivalent adele rings). Let p be prime, and choose some $v_{\mathfrak{P}}$ in $\mathbb{V}_{\mathbb{K}}$ extending p. By IR-equivalence there is a $v_{\mathfrak{P}'}$ in $\mathbb{V}_{\mathbb{L}}$ with the same decomposition and ramification. This does not quite determine that the completions at $v_{\mathfrak{P}}$ and $v_{\mathfrak{P}'}$ are the same, and to go further we now assume that the adele rings are elementarily equivalent. The completion at $v_{\mathfrak{P}'}$ needs, beyond the inertia and ramification, the data of which one variable monic polynomials over $\mathbb{Q}$ are solvable and it is well-known that that there are finitely many such polynomials whose solvability determine the completion uniquely.

Elementary Equivalence and Isomorphism 3

It is an elementary ring condition on the fibre at $v_{\mathfrak{P}}$ which polynomials single out the isomorphism type. By elementary equivalence of the adeles there must be a $v_{\mathfrak{P}'}$ satisfying the same condition, and giving isomorphism of the completions. Moreover the number of $v_{\mathfrak{P}}$ in $\mathbb{K}$ giving this completion must be the same as the number of $v_{\mathfrak{P}'}$ in $\mathbb{L}$ giving this condition. Thus, by a basic theorem of Iwasawa, one has

Theorem

Elementary equivalence of adele rings implies isomorphism

The Negative Results

It has been known for many years since Gassmann in the 1920's that isomorphism of $\mathbb{A}_K$ and $\mathbb{A}_L$ does not imply isomorphism of $\mathbb{K}$ and $\mathbb{L}$. By now one has found a variety of examples where the nonisomorphism is manifested by $\mathbb{K}$ and $\mathbb{L}$ differing on some significant number- theoretic property, e.g the cardinality of the class number. A striking example was given by de Smit and Perlis, with $\mathbb{K} = \mathbb{Q}(\sqrt[8]{-33})$ and $\mathbb{L} = \mathbb{Q}(\sqrt[8]{-33 \cdot 16})$.
On the other hand, Cebotarev's Theorem can easily be used to show that elementary equivalence of the adele rings of normal $\mathbb{K}$ and $\mathbb{L}$ implies isomorphism of $\mathbb{K}$ and $\mathbb{L}$. Another recent positive result is that of Linowitz, McReynolds and Miller showing that elementary equivalence of adele rings implies isomorphism of Brauer groups of the number fields.

Gassmann's Contribution

Gassmann's achievement was to translate Decomposition equivalence into a group-theoretic condition. It is relatively easy (see Perlis Theorm) to show that inertial equivalence implies that the fields have the same normal closure, and this then suggests the notion (in which Cebotarev is hidden) of Gassmann equivalence of finite groups.

Definition *Finite groups* $\mathbb{H}_1$ *and* $\mathbb{H}_2$ *are Gassmann - equivalent subgroups of the finite group* $\mathbb{G}$ *if they are subgroups of* $\mathbb{G}$ *and for each conjugacy* C *of a single element* c $C \cap \mathbb{H}_1$ *and* $C \cap \mathbb{H}_2$ *have the same cardinality.*

Gassmann proved that $\mathbb{K}$ and $\mathbb{L}$ are inertia equivalent if and only if $Gal(N||\mathbb{K})$ and $Gal(N||\mathbb{L})$ are Gassmann equivalent in $Gal(N||\mathbb{Q})$ where $\mathbb{N}$ is the common normal closure of $\mathbb{K}$ and $\mathbb{L}$.

This is involved in the proof of the Perlis Theorem. The basic idea has been used in many publications on the topic. Quite a wide variety of Gassmann situations is known.

Adelic Elementary Equivalence

The de Smit - Perlis example shows that elementary equivalence of adeles does not guarantee equality of class numbers. However, it does guarantee isomorphism of Brauer groups.
Are there natural extensions of adelic equivalence, with tame model theory, which can capture equality of class numbers ?

Are there stronger positive results?

Let us take a closer look at the discussion of the dimension of $\mathbb{K}$ over $\mathbb{Q}$, and the discriminant of $\mathbb{K}$.
Fix an integer n. What can one say, adelically, about the $\mathbb{K}$ with dimension n , or discriminant n ?

An example

In fact, dimension 1 can be characterized by a single sentence. $\mathbb{Q}$ is of course the only example, and one readily gets a sentence of ring theory that distinguishes
$\mathbb{A}_Q$ from $\mathbb{A}_K$ for any other $\mathbb{K}$. That sentence just says that there is only a single minimal idempotent which is archimedean.
We have not had time to look into more general issues of this kind. The topic appears quite challenging.

Bigger Issues Under Investigation

We want to understand definability and decidability in $\mathbb{A}_K$ as $\mathbb{K}$ varies. The preceding "pattern analysis" gives a new and clearer treatment of the decidability
of each individual $\mathbb{A}_K$, and uniformities in the Feferman-Vaught analysis give us a strong hold on definability. Moreover, with he kind assistance of Hrushovski, we are
able to get hold of exact consistency conditions for realization of patterns in dimension n number fields, and thereby to get hold of the basics of unltraproducts of adele rings of
adele rings $\mathbb{A}_K$ of bounded dimension. One can show
Theorem. Fix n .The theory of all adele rings $\mathbb{A}_K$ for $\mathbb{K}$ of dimension $\leq n$ is decidable.
The biggest problem is to remove the restriction on dimension. There is good reason to believe that decidability of the class of all adele rings is equivalent to the decidability,
prime p , of the class of all finite algebraic extensions of $\mathbb{Q}_p$.

A notion of pseuo-adelic ?

Techniques for generalizing Feferman-Vaught , developed by Paola D'A and Macintyre, for solving a problem of Zilber on quotient rings of models of arithmetic, allow one to get
at axioms for the theory of ultraproducts of adele rings, and there is hopw of obtaining some adelic analogues of Ax's pseuofinite field results.