MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 45/1990

Arithmetik der Körper

21.10. bis 27.10.1990

This conference, under the direction of Moshe Jarden (Tel Aviv) and Peter Roquette (Heidelberg), was the first one on this subject held in Oberwolfach. The main topics, treated during the morning sessions, were:

(i) Galois strartification;

(ii) The absolute Galois group of pseudo p-adically closed fields;

(iii) Pop's results on the characterization of p-adically closed fields by means of their absolute Galois groups.

Vortragsauszüge

Wulf-Dieter Geyer

The arithmetic of fields

Der Vortrag stellte Ideen vor, das undefiniert fließende Tagungsthema "Arithmetic of Fields" zu umreißen an Hand dessen, was Diophant und Kronecker unter Arithmetik verstanden, und an Hand des Inhalts der Bücher "L'Arithmetique des corps" von Ribenboim (1972) und "Field Arithmetic" von Fried–Jarden (1986). Zunächst wurden folgende 3 Gesichtpunkte hervorgehoben:

(a) Körper, insbesonders endlich erzeugte Körper, können reichhaltige arithmetische Strukturen tragen, die durch Begriffe wie "Ganzheitsring", "Bewertung", "Anordnung" angedeutet werden. Die Arithmetik in eigentlichen Sinne ist hier zu Hause.

(b) Das Studium der Polynome in 1 Variablen, d.h. das Studium algebraische Probleme mit endlich vielen Lösungen, führt zur Galoistheorie: Jeder Körper K ist seine absolute Galoisgrouppe G_K, eine proendliche Gruppe, zugeordnet, die die separablen Körpererweiterungen von K beschreibt. Damit können gruppentheoretische Methoden, aber auch maßtheoretische Hilfsmittel (durch das eindeutige Haarsche Maß auf G_K) zum Studium der Körpertheorie eingeschetzt werden. Die Beziehungen zwischen diesen, den Körpern zugeordneten algebraischen Strukturen und der inneren arithmetischen Struktur sollten ebenfalls dem Gebiet "Arithmetic of Fields" zugeordnet werden. Ein zentrales aktuelles Problem ist hier z.B. die Frage, ob endlich erzeugte nichtendliche Körper K durch ihre Galoisgruppe G_K bis auf Isomorphie bestimmt sind (Sätze von Neukirch, Uchida, Pop).

(c) Das Studium der Polynome in mehreren Variablen über einem Körper K führt zur algebraischen Geometrie über K. Hat K eine ausgeprägte arithmetische Struktur (z.B. K endlich erzeugt), so führt das Zusammenspiel von Arithmetik und algebraische Geometrie zur "Arithmetischen Algebraischer Geometrie", die durch die Sätze von Weil (Kurven über endlichen Körper), Siegel (ganze Punkte auf affine Kurven), Mordell–Faltings (rationale Punkte auf Kurven über Zahlkörper) repräsentiert sei und die heute ein renomiertes Forschungsgebiet (Probleme sind z.B. die Übertragung des Satzes von Mordell–Faltings auf höhere Dimensionen, oder effektive Schranken für Endlichkeitsätze) mit Verbindungen z.B. zur Differentialgeometrie ist. Das Gebiet "Arithmetic of Fields" sollte engen Kontakt zu dieser Richtung der algebraischen Geometrie haben, obschon die Zielrichtung unterschiedlich ist: "Arithmetic of Fields" wird die algebraische Geometrie als Hilfsmittel heranziehen, um körpertheoretische Resultate zu erzielen, während die arithmetische algebraische Geometrie die geometrischen Objekte selbst aus arithmetischen Augen betrachtet.

Die Geschichte der Arithmetik zeigt (vgl. das Hasse-Prinzip), daß zum Studium endlicher Zahlkörper riesige Körper einfacherer Struktur (die p-adischen Zahlkörper als Geschwister des reellen Zahlkörper) geschaffen werden, desen Studium zum besseren Verständnis der komplizierteren endlichen Zahlkörper betrug. Im zweiten Teil des Vortrags werden so die direkt für die Bedürfnisse der Arithmetik nützlichen Klassen von Körpern betrachtet: Die algebraisch abgeschlossenen Körper, die reell abgeschlossenen Körper, die p-adisch abgeschlossenen Körper (etwa soweit geht das Buch von Ribenboim), die Hilbertschen Körper, die PAC-Körper (pseudo-algebraisch-abgeschlossen) und ihre Verwandten, die PRC-Körper (pseudo-reel-abgeschlossen) und die PpC-Körper (pseudo-p-

adisch-abgeschlossen), die das Buch von Fried-Jarden und darauf aufgebaute Arbeiten behandeln. Bei der Betrachtung derartiger Körperklassen ist (implizit mit Artins Lösung des 17. Hilbertschen Problems) ein neues Hilfsmittel in diesem Gebiet aufgetaucht und mit Erfolg eingeordnet worden: die Modelltheorie, die durch Analyse der formalen Sprache und ihrer Syntax (Diophant war der erste, der Symbole für die unbekannte Größe und die Gleichheit benutzte, also die erste Schritte zu einer formalen Sprache tat!) den Gültigkeitsumfang von Aussagen klären kann, und deren Kompaktheitsatz auch ein wichtiges algebraisches Konstuktionsmittel ist. Die modelltheoretichen Ergebnisse über die genannte Körperklassen zur Quantorenelimination, zur Entscheidbarkeit (bzw. Unentscheidbarkeit) und zu Entscheidungsverfahren sind wesentlich für zahlreiche arithmetische Fragen, wie wir auch auf dieser Tagung sehen werden. Die Verbindungen zur Galoistheorie (Kennzeichnung von Körperklassen durch den Typ der Galoisgruppe) liefern zahlreiche Sätze wie offene Fragen, speziell über die p-adisch abgeschlossenen Körper werden wir hier auf der Tagung mehreren Vorträge haben (Thesis von Pop), ebenso zur Galoisgruppe von Hilbertschen PAC-Körpern (Fried–Völklein). Die geschichtliche Entwicklung dieser Körperklasse wird nur in der Anfängen (Ax, Ax-Kochen and Ershov, Jarden) skizziert.

Moshe Jarden

Galois stratification for the elementary theory of finite fields

Galois stratification is a procedure which was invented by M. Fried in 1974 and published for the first time jointly with G. Sacerdote in the Annals of Math. 104 (1976). The procedure uses Galois theory and constructive algebraic geometry in order to decide whether a given sentence φ in the elementary language of rings is true in almost all fields $\mathbb{F}_p$ and also finds the finite set of exceptional primes. Two fundamental theorems underlie the procedure: the Bertini-Noether theorem and the non-regular analog of the Chebotarev density theorem.

The basic concept that the procedure introduces is that of a *Galois stratification* of the affine space $\mathbb{A}^n$:

$$\mathcal{A} = \langle \mathbb{A}^n, C_i/A_i, \mathrm{Con}(A_i), l \rangle_{i \in I}$$

where

(1) I is a finite set;

(2) $A_i = V_i - V(g_i)$, where $V_i = V(f_{i1}, \ldots, f_{im_i})$ is a $\mathbb{Q}$-irreducible variety defined by given polynomials f_{ij} with coefficients in $R = \mathbb{Z}[l^{-1}]$ (let $\mathbf{x}$ be a generic point of V_i) and $g_i \in$

$R[X_1, \ldots, X_n]$ is a polynomial which does not vanish identically on V_i such that the coordinate ring $R[A_i] = R[\mathbf{x}, g_i(\mathbf{x})^{-1}]$ is integrally closed;

(3) $C_i = R[Z_i, z]$ is the integral closure of $R[A_i]$ in a finite Galois extension $\mathbb{Q}(A_i)$ and the discriminant of z over $\mathbb{Q}(A_i)$ is a unit of $R[A_i]$;

(4) $\mathrm{Con}(A_i)$ is a conjugacy subdomain of $\mathcal{G}(C_i/A_i)$; and

(5) for each prime p which does not divide $l = l(\mathcal{A})$, $\mathbb{A}^n(\tilde{\mathbb{F}}_p)$ is the disjoint union of $\mathbb{A}_i(\tilde{\mathbb{F}}_p)$, $i \in I$.

If p is a prime as in (5), then each $a \in A^n(\mathbb{F}_p)$ belongs to a unique $A_i(\mathbb{F}_p)$. Let $\mathbf{x}$ be a generic point of A_i. Then the specialization $\mathbf{x} \to \mathbf{a}$ uniquely extends to a homomorphism φ_0: $R[A_i] \to \mathbb{F}_p$. Extend φ_0 further to an epimorphism φ of C_i onto a finite Galois extension N of $\mathbb{F}_p$. Let φ^* be the isomorphism of $G(N/\mathbb{F}_p)$ onto the decomposition group of $\mathrm{Ker}(\varphi)$ that φ induces. Denote the Frobenius automorphism $x \to x^p$ by Frob_p. We denote the conjugacy class of $\varphi^*(\mathrm{Frob}_p)$ by $\mathrm{Ar}(A_i, p, \mathbf{a})$. We write $\mathrm{Ar}(\mathcal{A}, p, \mathbf{a}) \subset \mathrm{Con}(\mathcal{A})$ if $\mathrm{Ar}(A_i, p, \mathbf{a}) \subset \mathrm{Con}(A_i)$.

The main step of the procedure is the elimination of the existential quantifier. One starts from a stratification $\mathcal{A}$ of A^{n+1} and produces a stratification $\mathcal{B}$ of $\mathbb{A}^n$ such that if p does not divide $l(\mathcal{B})$ and $\mathbf{b} \in \mathbb{A}^n(\mathbb{F}_p)$, then $\mathrm{Ar}(\mathcal{B}, p, \mathbf{b}) \subset \mathrm{Con}(\mathcal{B})$ if and only if there exists $c \in \mathbb{F}_p$ such that $\mathrm{Ar}(\mathcal{A}, p, (\mathbf{b}, c)) \subset \mathrm{Con}(\mathcal{A})$.

E. Becker

On the arithmetic of formally real Fields

In this talk a report is given on what could be called "arithmetic" of formally real fields. List of contents: 1) The real holomorphy ring, 2) Sums of powers and orderings of higher level, 3) Real closures, 4) General signatures. By definition, the real holomorphy ring $H(K)$ of a formally real field K is the intersection of all valuation rings with formally real residue field. Another fundamental notion is the topological space M of all real places $\lambda : K \to \mathbb{R} \cup \infty$. If $K/\mathbb{R}$ is a function field then M and H are related to the system of all smooth projective models of $K/\mathbb{R}$. The study of the group of units $H^\times$ of $H = H(K)$ shows a powerful relationship with the sums of powers in K, e.g., one has $\sum K^{2n} = (H^\times \cap \sum K^2)(\sum K^2)^n$. It also allows to derive the following result: $\sum K^{2n} = \bigcap P$, P ranging over the set of all orderings of level n, i.e. those subsets $P \subseteq K$ satisfying $P + P \subseteq P$, $P \cdot P \subseteq P$, $K^{2n} \subseteq P$, $K^\times/P^\times$ cyclic. Quite recently R. Berr has found a more general notion which allows to characterize sums of mixed powers, i.e. $\sum_i \sum K^{2n_i}$, in an analog manner. If K is equipped with an ordering P of higher level n one naturally studies its real closure

$(R,\tilde{P})$, i.e. a maximal algebraic extension of (K,P) subject to $[K^\times : P^\times] = [R^\times : \tilde{P}^\times]$. These real closures have distinguished properties as to their valuation theory as well as model theory, the latter fact allowing deeper results on affine algebraic geometry problems. In the last section a class of characters $\chi : K^\times \to S^1$, the (general) signatures, is dealt with. They are characterized by the fact that the ring $A(\chi) = \{a \in K \mid \exists n \in \mathbb{N} : n \pm a \in \operatorname{Ker}\chi\}$ is a valuation ring.

Florian Pop

Fields of totally Σ-adic numbers

Using the approach of Roquette to the Rumely Local-Global Principle we proved:

Theorem 1(Local Existence theorem): *Let K be a local field and F/K a function field of one variable, which is conservative and has a K-rational place. Then for any positive divisor $D > 0$ there exist $n > 0$ and functions $f \in F$ satisfying $(f)_\infty = nD$ and having all zeroes K-rational and simple.*

Theorem 2: *Let K be an arbitrary field and Σ a finite set of places of local type of K. Suppose F/K is a conservative function field which has K_g-rational places for all $g \in \Sigma$. Then for any positive divisor $D > 0$ of F/K there exist functions $f \in F$ satisfying $(f)_\infty = nD$ (for some $n > 0$) and all zeroes distinct and totally Σ-adic (Equivalently: F has totally Σ-adic places).*

As corollaries one gets: The field of totally real, or p-adically, or Σ-adically numbers is PRC, PpC or respectively PΣC.

Jochen Königsmann

Half-ordered fields

A half-ordering (h.o.) on a field K is a multiplicative subgroup $M \leq K^\times$ of index $[K^\times : M] \leq 2$ which is not additively closed, i.e., $M + M \not\subseteq M$. For example, $(\mathbb{F}_q^\times)^2$ is a h.o. of $\mathbb{F}_q$ provided $q = p^n, p \neq 2$, or, if $v: K \to \mathbb{Z} \cup \{\infty\}$ is a valuation on K, then $v^{-1}(2\mathbb{Z})$ is a h.o. on K. In analogy to ordered fields, an "Artin-Schreier-Theory" for h.o. fields can be developed, charcterizing h.o. fields of char. $\neq 2$ which are algebraically maximal with respect to a given h.o. as perfect fields K with $\mathcal{G}(\tilde{K}/K) \cong \mathbb{Z}_2$. Within the class of h.o. fields which are compatible with a valuation v (i.e., $1 + m_v \subseteq M$) a criterion for the isomorphism of two h.o. closures can be given. As a result, the theory of maximal h.o fields with compatible valuation has nice model-theoretic properties. There remains, however, the question whether a maximally h.o. field is either PAC or Henselian.

Dan Haran

The absolute Galois group of a pseudo p-adically closed (PpC) field

The talk reported on the article:

D. Haran, M. Jarden, *The absolute Galois group of a PpC field*, J. reine angew. Math. 383 (1988), 147–206,

which contains the following results:

Theorem 1: *The absolute Galois group $G(K)$ of a PpC field K is p-adically projective.*

Theorem 2: *For every p-adically projective group G there exists a PpC field K such that $G(K) \cong G$.*

The talk was primarily concerned with:

(a) (a slightly improved version of) the proof of Theorem 1;

(b) definition of *sites* and $G(\mathbb{Q}_p)$-*structures*;

(c) A sketch of the proof of Theorem 2 using these concepts.

Helmut Völklein

The embedding problem over a Hilbertian PAC-field

This is a joint work with M. Fried. We prove the following conjecture on Hilbertian PAC-fields P of characteristic 0:

Every finite embedding problem over P is solvable.

For countable P this, combined with a result of Iwasawa, implies that the absolute Galois group of P is ω-free; that is $G(\bar{P}/P)$ is the free profinite group of countably infinite rank, denoted $\hat{F}_\omega$.

By a result of Fried and Jarden, every countable Hilbertian field k of characteristic 0 has a Galois extension P with P Hilbertian and PAC, and $G(P/k) \cong \prod_{n=2}^{\infty} S_n$ (where S_n is the symmetric group).

From the above, $G(\bar{k}/P) = G(\bar{P}/P) \cong \hat{F}_\omega$ and we get the exact sequence

$$1 \to \hat{F}_\omega \to G(\bar{k}/k) \to \prod_{n=2}^{\infty} S_n \to 1 \; .$$

Michael Fried

Hilbertian + PAC ⇒ ω-free

Comments on Diophantine properties: H(ilbert's) I(rreducibility) T(heorem), the Čebotarev Density Theorem, the Riemann Hypothesis for function fields, Siegel's theorem, Weil's decomposition theorem: these are some of the diophantine tools that influenced the arithmetic investigations of my early career. Yet, as much as I used these and studied other problems with them, I had the feeling of missing connections between these diophantine properties. This was especially true of HIT. It was generally available in many forms, applied over many types of fields. But, except for one point, its relation to the absolute Galois group was a mystery. The exception was an observation at the end of an early paper that the *nonregular* analog of the Čebotarev theorem implies an arithmetic progression form of HIT (that was effective). On this I was influenced by Andrej Schinzel. For me, the book **Field Arithmetic** with Moshe Jarden was inspired by the idea that very weak forms of these diophantine properties might be related by considering the collection of subfields of $\bar{\mathbb{Q}}$ (the algebraic numbers) that satisfy these properties. While results of Kuyk and Weissauer were inspiring, even at the publication of the book in 1986, my feeling was that I still had no understanding of HIT.

A point of explanation of the technique: Therefore, of the previously unsolved problems in the book the one that most epitomized this goal – perhaps first formulated by Schmidt-Göttsch – was whether the Hilbertian and pseudo-algebraically closed properties for a field P together imply that the absolute Galois group of P is pro-free on a countable number of generators. This is a corollary of work with Helmut Völklein that will appear in **The inverse Galois problem and rational points on moduli spaces** and in **The embedding problem over a Hilbertian PAC-field.** The method is truly classical arithmetic geometry whereby there is constructed a moduli space $\mathcal{H}^{in}(G,r)$ associated to any finite group G for the existence of exact sequences

$$(*) \qquad 1 \to G(L/\hat{K}(x)) \to G(L/K(x)) \to G(\hat{K}/K) \to 1$$

with these properties: the corresponding point $p \in \mathcal{H}^{in}(G,r)$ generates K over $\mathbb{Q}$; $G(L/\hat{K}(x))$ is isomorphic to G; the extension $L/\hat{K}(x)$ has exactly r points of ramification; and $\hat{K}$ is the algebraic closure of K in L. The toughest point of the proof is solving extension problems for $G(\bar{P}/P)$ where P is a given Hilbertian PAC field. The wild idea of the proof is this: given a Galois extension P'/P and a group G we want to construct $(*)$ so that $\hat{K} = P'$ and $K = P$ and the extension $(*)$ turns out to be exactly what we desire. There are many group theoretic reductions, but our moduli space allows us to exactly do that.

Further applications related to the conference: For PAC fields P, P has the (weaker) R(egular) G(alois)-Hilbertian property – Hilbert's irreducibility theorem applies to those Galois extensions $L/P(x)$ for which L is regular over P – exactly when each finite group is a quotient of $G(\tilde{P}/P)$. Furthermore, the method is pretty certain to be extendable to characterize those Hilbertian fields P which are PRC (pseudo-real closed) or PpC (pseudo-p-adically closed) discussed by Efrat, Haran, Königsmann, Pop, Prestel, et. al.

Jürgen Ritter

The Artin-Hasse power series and group ring units

In this talk which reports on joint work with Klaus Hoechsmann from Vancouver the following is known. Let A be an abelian finite p-group with p odd, U the unit group in the p-adic group ring $\mathbb{Z}_pA$, and $U_1^+ \leq U$ the group of those units which have augmentation 1 and which are stable under the automorphism that is induced by $z \mapsto z^{-1}$, $z \in A$. Then U_1^+ has a $\mathbb{Z}_p$-basis consisting of values of the Artin-Hasse power series E, namely of the elements $E(z-1)E(z^{-1}-1)$, $1 \neq z \in A$; here $E(T) = \exp P(T) \in \mathbb{Z}_p[[T]]$ with $P(T) = T + T^p/p + T^{p^2}/p^2 + \cdots \in \mathbb{Q}[[T]]$.

Ido Efrat

Algebraic realization of p-adically projective groups

This was a report on a paper by Moshe Jarden. It was shown that the elementary theory of all PpC fields coincides with the elementary theory of all PpC fields algebraic over $\mathbb{Q}$. The proof used two results:

(i) If L is algebraic over a PpC field K, then L is PpC iff for each p-adic closure $\bar{K}$ of K, either $L \subseteq \bar{K}$ or $L\bar{K} = \tilde{K}$.

(ii) Each p-adically projective group of rank $\leq \aleph_0$ is the absolute Galois group of a PpC field algebraic over $\mathbb{Q}$ (or any other countable Hilbertian p-adically valued field).

Michael Spiess

Report on a theorem proved by Florian Pop in his thesis

We call a profinite group G p-adic, if G is isomorphic to the absolute Galois group of a finite extension of $\mathbb{Q}_p$.

Theorem: *Let (K,v) be a henselian field such that* $\operatorname{char} K_v = q > 0$ *and G_K p-adic. Then (K,v) is p-adically closed and $p = q$.*

Lou van den Dries

Definable sets over finite fields I

Theorem: *Each existential formula $\varphi(Y_1,\ldots,Y_n)$ in the language of rings is equivalent, uniformly for all pseudo-algebraically closed fields, to a conjunction of formulas of the form*

$$\exists T(g(Y_1,\ldots,Y_n,T) = 0).$$

A proof of this result was sketched. One application is as follows:

Given polynomials $f_1(Y),\ldots,f_k(Y) \in \mathbb{Z}[Y]$, $Y = (Y_1,\ldots,Y_n)$, the set of primes p such that the congruence $f_1(Y) \equiv \cdots \equiv f_k(Y) \equiv 0 \bmod p$ is solvable is the intersection of finitely many sets of the form $\{p\colon \exists t\ g(t) \equiv 0 \bmod p\}$, where $g(T) \in \mathbb{Z}[T]$ is a one variable polynomial.

(This improves a result of J. Ax in Annals of Math., 1967.) The theorem is also needed to obtain a positive quantifier elimination for finite fields, see abstract by Macintyre.

Angus Macintyre

Definable sets over finite fields II

The elimination theory described in van den Dries' talk is further sharpened in the case of pseudo-finite fields.

One adjoins, for each n, constants c_{ni} $(0 \leq i < n)$, to satisfy the axiom that

$$c_{n0} + c_{n1}t + \cdots + c_{n,n-1}t^{n-1} + t^n = 0$$

defines the unique extension of dimension n. In this enriched language, uniformly for all pseudo-finite fields, every formula is equivalent to a positive boolean combination of equations and formulas $(\exists T)(g(Y,T) = 0)$.

This is applied to prove the following "Lang-Weil" theorem:

Theorem: *For every $\Phi(X_1,\ldots,X_m,Y_1,\ldots,Y_n)$ there exists a constant $c > 0$, integers $d_1,\ldots,d_e(\leq n)$ and positive rationals $\lambda_1,\ldots,\lambda_e$ such that for all $\mathbb{F}_q$ and $A \in \mathbb{F}_q^m$, if $\Phi(A,\mathbb{F}_q^n) \neq \emptyset$ then for some i*

$$|\text{card } \Phi(A,\mathbb{F}_q^n) - \lambda_i q^{d_i}| \leq c \cdot q^{d_i - 1/2} .$$

Moreover, the A for which an alternative (d_i,λ_i) holds form a definable set.

Ido Efrat

Maximal pseudo p-adically closed fields

We prove that there is a unique profinite group $\bar{D}_e$ with the following properties:

(1) $\bar{D}_e$ is p-adically projective;

(2) There is a representatives system $\Gamma_1,\ldots,\Gamma_e$ for the conjugacy classes of

$$\{\Gamma \leq \bar{D}_e \mid \Gamma \cong G(\mathbb{Q}_p)\} \quad ;$$

(3) $\bar{D}_e = \langle \Gamma_1^{\sigma_1},\ldots,\Gamma_e^{\sigma_e}\rangle$ for all $\sigma_1,\ldots,\sigma_e \in \bar{D}_e$.

We call $\bar{D}_e$ the **p-adically e-minimal group**. It arises naturally from model-theoretic considerations:

Theorem: *The theory of fields with $0 \leq e < \infty$ p-adic valuations has a model-companion. Its models are the structures $(K,O_1,\ldots,O_e)$ such that:*

(1) *K is pseudo p-adically closed;*

(2) *$O_1,\ldots,O_e$ are distinct p-adic valuation rings on K;*

(3) *$G(K) \cong \bar{D}_e$.*

Structure Theorem: *Let A be a profinite group A, let q be a prime number and let $\varphi_i \colon \Gamma_i \to A$, $i = 1,\ldots,e$, be continuous homomorphisms such that $\varphi_1(\Gamma_1),\ldots,\varphi_e(\Gamma_e)$ are pro-q groups. Then the following conditions are equivalent:*

(a) *There exists a unique continuous epimorphism $\eta\colon \bar{D}_e \to A$ extending $\varphi_1,\ldots,\varphi_e$;*

(b) *$A = \langle \varphi_1(\Gamma_1),\ldots,\varphi_e(\Gamma_e)\rangle$ and is a pro-q group.*

Thus, $\bar{D}_e$ is a p-adic analog of the free pro-2 product $(\mathbb{Z}/2\mathbb{Z}) *_2 \cdots *_2 (\mathbb{Z}/2\mathbb{Z})$ of e copies of $G(\mathbb{R})$.

Using the notion of p-adically minimal groups we solve the inverse Galois problem for certain pseudo p-adically closed fields:

Corollary: *If K is a pseudo p-adically closed field with infinitely many p-adic valuations then each finite group is realizable as a Galois group over K.*

E. Becker

Report on results of Pop on the characterization of p-adically closed fields via Galois groups

Main theorem: *K p-adically closed $\Leftrightarrow$ $\tilde{K} = K\tilde{\mathbb{Q}}$, G_K p-adic.*

(The algebraic closure of a field F is denoted by $\tilde{F}$). This theorem is deduced from the following

Theorem A: *K p-adically closed, E/K any extension of transcendence degree 1. Then, if G_E is l-adic, $l = p$ and E is p-adically closed.*

Theorem A heavily relies on the following local-global principles for the Brauer group:

Theorem B: *K as in Theorem A, F/K regular function field. Then the natural map* $\mathrm{Br}(F) \to \prod_{P \in \mathbb{P}(F)} \mathrm{Br}(F_p)$ *is injective.*

Theorem B': *E/K as in Theorem A, then the natural map* $\mathrm{Br}(E) \to \prod_{w/v} \mathrm{Br}(E^h_w)$ *is injective.*

Here, $\mathbb{P}(F)$ denotes the set of prime divisors of F/K, F_p the completion of F at P, v is the natural p-valuation of K and E^h_w the henselian closure of E at w. Furthermore, the results reported in the talks of Spiess and Frey are also used.

Johan Pas

The invariance of certain p-adic Poincaré series

We show that a generalization of Igusa's local zeta function to integrals over sets defined in a first order language of valued fields, is an invariant function (in the sense of Meuser) of the class of unramified extensions of a p-adic field. As a corollary we prove the invariance of certain Poincaré series, which was conjectured by Fried and Jarden in the book 'Field Arithmetic' (Problems 21 and 22).

Luc Lauwers

e-fold ordered Frobenius fields

A projective Artin-Schreier structure **G** such that for each finite structure $\mathbf{B} \in \operatorname{Im} G$ for all epimorphisms π: $\mathbf{B} \to \mathbf{A}$ and φ: $\mathbf{G} \to \mathbf{A}$ there exists an epimorphism λ: $\mathbf{G} \to \mathbf{B}$ such that $\pi \circ \lambda = \varphi$, is said to be superprojective.

We treat e-fold ordered fields (M,P) for which the absolute Galois structure

$$\mathbf{G}(M_s/M) = \langle G = G(M_s/M), G(M_s/M(\sqrt{-1})), X = X(M_s/M), d\colon X \to G\rangle ,$$

is superprojective. Hereby is M_s the separable closure of M, G the absolute Galois group, X the space of the maximal ordered subfields $(M_s(\varepsilon), P')$ with ε an involution and P' an ordering of $M_s(\varepsilon)$ which extends some P_i; the map d is defined by $d(M_s(\varepsilon), P') = \varepsilon$. Such a field is said to be *Frobenius*. Apparently a Frobenius field is *pseudo real closed*: i.e., every absolute irreducible variety over M which has an M_r-rational point in each real closure M_r of M, has an M-rational point. By means of the Galois stratification the theory of e-fold ordered Frobenius fields is reduced to an "Artin-Schreier structure"-theoretical decision problem. The notion of embedding cover is translated to Artin-Schreier structures and this decision problem is solved.

This induces the main theorem:

The theory of e-fold ordered Frobenius fields is decidable (in a primitive recursive way).

Franz-Viktor Kuhlmann

<u>**Henselian rationality of valued function fields**</u>

Let (F,v) a valued function field over a valued field (K,v). It is called *henselian rational* if it satisfies $(F,v)^h = (K(\mathcal{T}),v)^h$ for some transcendence basis $\mathcal{T}$, and *henselian almost rational*, if $(F,v)^h$ is a tame unramified extension of a henselian rational function field. We describe the significance of henselian rationality for the model theory of valued fields, in particular for the proof of embedding lemmata. We consider two cases:

(A) $(F,v)/(K,v)$ not immediate, but $v(F)/v(K)$ torsion free and $\bar{F}/\bar{K}$ regular and tr.deg.$F/K =$ rational rank$(v(F)/v(K))+$ tr.deg. $\bar{F}/\bar{K}$; then if (K,v) is a field without defect extensions (is "defectless") so is (F,v) and (F,v) is henselian rational over $(K,v)^h$. If (K,v) is not defectless, one may measure how far (F,v) is from being hens. rational by introducing the defect for henselian rational by introducing the defect for henselian function fields.

(B) $(F,v)/(K,v)$ is immediate of tr.deg. 1. Then for (K,v) henselian finitely ramified or tame or semi-tame, (F,v) is henselian rational. But this is not true for (K,v) algebraically complete (= henselian and defectless) in general. We give a sketch of the proof for a tame constant field (K,v), including a "pull down" principle for henselian rationality through tame extensions of the constant field. For this, a theory of henselian generators is developed, in particular the question

$[K(x)^h : K(y)^h] =?$ for $y \in K(x)^h$ is considered. Another ingredient is a certain property which characterizes the Galois groups of tame Galois extensions, called the *valuation independence* which is an analogue (and indeed related to) the usual valuation independence of elements in an extension of valued fields.

N. Klingen

Arithmetical equivalence and projective designs

This talk deals with the problem, whether or to what extent algebraic number fields are determined by the way primes decompose in them. Two main concepts are discussed: the weak Kronecker-equivalence and the stronger arithmetical equivalence of number fields. During the last years, using the classification of all finite simple groups, striking results were obtained, showing that a lot of fields are already determined by their Kronecker sets (Guralnick 1990). There is another connection with the classification theorem via projective (=symmetric balanced incomplete block) designs. This connection arises for fields K with a Z-transitive Galois group $G(\tilde{K}/K)$ of the Galois closure $\tilde{K}$ (Teit 1970). For such fields Kronecker equivalence implies arithmetical equivalence, and one is able to compare the class numbers of the relevant fields in terms of the invariants of the design. Since all Z-transitive designs are known, one has a fairly explicit list of the Galois groups of such fields, which include *all* Kronecker equivalent fields of prime degree. For the latter ones the class numbers can only differ by a power of a single prime.

Berichterstatter: I. Efrat

Tagungsteilnehmer

Prof.Dr. Serban A. Basarab
Dept. of Mathematics
University of Bucharest
Str. Academiei 14

70109 Bucharest
ROMANIA

Prof.Dr. Francoise Delon
Institut für Mathematische Logik
Universität Freiburg
Albertstr. 23b

7800 Freiburg

Prof.Dr. Eberhard Becker
Fachbereich Mathematik
Universität Dortmund
Postfach 50 05 00

4600 Dortmund 50

Prof.Dr. Lou P. D. van den Dries
Department of Mathematics
University of Illinois
Altgeld Hall
1409, West Green Street

Urbana , IL 61801
USA

Prof.Dr. Luc Belair
Dept. of Mathematics and
Informatics
University of Quebec at Montreal
C.P. 8888, Succ. A

Montreal, Quebec H3P 3P8
CANADA

Ido Efrat
Dept. of Mathematics
Tel Aviv University
Ramat Aviv
P.O. Box 39040

Tel Aviv , 69978
ISRAEL

Prof.Dr. Zoe Chatzidakis
U. E. R. de Mathematiques
T. 45-55, 5eme etage
Universite de Paris VII
2, Place Jussieu

F-75251 Paris Cedex 05

Prof.Dr. Gerhard Frey
Institut für Experimentelle
Mathematik
Universität-Gesamthochschule
Ellernstr. 29

4300 Essen 12

Prof.Dr. Gregory L. Cherlin
Dept. of Mathematics
Rutgers University
Busch Campus, Hill Center

New Brunswick , NJ 08903
USA

Prof.Dr. Mike D. Fried
Dept. of Mathematics
University of California at Irvine

Irvine , CA 92717
USA

Prof.Dr. Wulf-Dieter Geyer
Mathematisches Institut
Universität Erlangen
Bismarckstr. 1 1/2

8520 Erlangen

Ivan Kausz
Fakultät für Mathematik
Universität Regensburg
Universitätsstr. 31
Postfach 397

8400 Regensburg

Prof.Dr. Barry W. Green
Mathematisches Institut der
Universität Heidelberg
Im Neuenheimer Feld 288

6900 Heidelberg 1

Prof.Dr. Norbert Klingen
Mathematisches Institut
Universität Köln
Weyertal 86-90

5000 Köln 41

Dr. Dan Haran
Dept. of Mathematics
Tel Aviv University
Ramat Aviv
P.O. Box 39040

Tel Aviv , 69978
ISRAEL

Jochen Koenigsmann
c/o Prof. Dr. A. Prestel
Fakultät für Mathematik
Universität Konstanz
Postfach 5560

7750 Konstanz 1

Prof.Dr. Moshe Jarden
Dept. of Mathematics
Tel Aviv University
Ramat Aviv
P.O. Box 39040

Tel Aviv , 69978
ISRAEL

Dr. Franz-Viktor Kuhlmann
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288/294

6900 Heidelberg 1

Prof.Dr. Wolfram Jehne
Mathematisches Institut
Universität Köln
Weyertal 86-90

5000 Köln 41

Dr. Luc Lauwers
Fakulteit Economie
van Evenstraat 2B

B-3030 Leuven

Prof.Dr. Angus John Macintyre
Mathematical Institute
Oxford University
24 - 29, St. Giles

GB- Oxford , OX1 3LB

Prof.Dr. Jürgen Ritter
Institut für Mathematik
Universität Augsburg
Universitätsstr. 8

8900 Augsburg

Dr. Margarita Otero
Mathematical Institute
Oxford University
24 - 29, St. Giles

GB- Oxford , OX1 3LB

Prof.Dr. Peter Roquette
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288/294

6900 Heidelberg 1

Dr. Johan Pas
Departement Wiskunde
Faculteit der Wetenschappen
Katholieke Universiteit Leuven
Celestijnenlaan 200 B

B-3030 Leuven

Michael Spieß
Fakultät für Mathematik
Universität Regensburg
Universitätsstr. 31
Postfach 397

8400 Regensburg

Dr. Florian Pop
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288/294

6900 Heidelberg 1

Prof.Dr. Helmut Völklein
Dept. of Mathematics
University of Florida
201 Walker Hall

Gainesville , FL 32611
USA

Prof.Dr. Alexander Prestel
Fakultät für Mathematik
Universität Konstanz
Postfach 5560

7750 Konstanz 1

Prof.Dr. Alfred Reinhold Weiss
Dept. of Mathematics
University of Alberta
632 Central Academic Building

Edmonton, Alberta T6G 2G1
CANADA