MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 18/1993

The Arithmetic of Fields

18.– 24.4.1993

This conference, under the direction of Wulf-Dieter Geyer (Erlangen) and Moshe Jarden (Tel Aviv) was the second one on this subject held in Oberwolfach.

As in the first conference survey lectures were given on a recent central result in Field Arithmetic. This time it was the theorem of Fried and Völklein that each PAC Hilbertian field of characteristic 0 is ω-free. The lecturers were Geyer, Völklein, and Haran. Then special lectures were given. In one of them Pop announced his $\frac{1}{2}$ Riemann Existence Theorem which implies a generalization of the Fried-Völklein theorem to arbitrary characteristic. The other talks fell into six categories:

1. Galois groups (Efrat, Fried, Geyer, Jensen, Haran)
2. Real fields (Berr, Efrat, Königsmann, Macintyre, Schmid)
3. Model theory and logic (Delon, Macintyre, Pheidas)
4. Finite fields (Fried, Müller)
5. Local global principle (Jarden, Razon)
6. Diophantine equations (Ruppert)

R. Berr: Some applications of the theory of real holomorphy rings

Let K be a formally real field. By definition, the absolute real holomorphy ring $H(K)$ of K is the intersection of the real valuation rings of K. Thereby a valuation ring is called **real** if its residue field if formally real. For $H(K)$ the following description holds

$$H(K) = \{x \in K | \exists n \in N: n \pm x \in \sum K^2\}.$$

Using the ring $H(K)$ E. Becker showed that $x \in \sum K^2$ is a sum of $2n$th powers iff $v(x) \in 2n\Gamma_v$ for all valuations v of K. This result can by generelized as follows: Let $\mathcal{L} \subset \mathbb{N}$ and let

$$\sum_{\mathcal{L}} \sum K^{2n} = \{\sum x_i^{2n_i} | \, x_i \in K, \; n_i \in \mathcal{L}\}.$$

Then for $x \in \sum K^2$ we have: $x \in \sum_{\mathcal{L}} \sum K^{2n}$ iff $v(a) \in \bigcup_{\mu \in \mathcal{L}} 2\mu\Gamma_v$ for all real valuations v of K. For example, let $f = X^4(X+1)^6 \in \mathbb{R}(X)$. Then $f \in \sum \mathbb{R}(X)^4 + \sum \mathbb{R}(X)^6 + \sum \mathbb{R}(X)^{10}$. These results are based on the fundamental relation $H(K)^* \cap \sum K^2 \subset \sum K^{2n}$ for all $n \in \mathbb{N}$. This can be generelized as follows. Let $T \subset K$ be a quadratic preordering. Instead of $H(K)$ we now consider the ring $A(T) = \{x \in K | \, \exists n \subseteq \mathbb{N}: \, n \pm x \in T\}$. Let $S \subset K^*$ be a subgroup such that $K^2 \subset S$ and $T = \sum S = \{\sum s_i | \, s_i \in S\}$. Finally for $n \in \mathbb{N}$ let $\sum S^n = \{\sum s_i^n | \, s_i \in S\}$. If $n \in \mathbb{N}$ is odd we get the following results:

$$(1) \; A(T)^* \cap T \subset \sum S^n; \qquad (2) \; T^n \subset \sum S^n.$$

For example, let $K = \mathbb{R}(x)$ and let $T = \sum K^2 + X \sum K^2$. Then $\frac{1+x}{2+x} \in A(T)^* \cap T$. Now let $S = K^2 \cup XK^2$ in order to get $\frac{1+x}{2+x} \in \sum \mathbb{R}(x)^{2n} + x^n \sum \mathbb{R}(x)^2$ for all odd $n \in \mathbb{N}$.

Françoise Delon: Groups acting on valued groups

We are interested in retracts of fields, precisely in these structures consisting of the additive group K^+, a multiplicative subgroup G and the action of G on K^+. We add a valuation v from K^+ on G, commuting with the action of G:

$$\forall g \in G,\ \forall x \in K^+:\ v(g) = g,\ v(g \cdot x) = g \cdot v(x).$$

Let $\mathcal{L}$ be the corresponding language. We prove an Ax-Kochen Ershov principle for this kind of structures, with the following consequences.

PROPOSITION 1: *If (K, v, G) and (L, w, H) are two valued fields with cross-section, and having the same type of characteristic, then*

$$(K, v, G)\lceil\mathcal{L} \equiv (L, w, G)\lceil\mathcal{L} \text{ iff } \mid K/v \mid = \mid L/v \mid \text{ and } G \equiv H \text{ as ordered groups.}$$

$(K, v, G)\lceil\mathcal{L}$ is decidable iff G is as an ordered group.

PROPOSITION 2: *If k is a field and G an ordered group, let $k((G))$ be the skew power series field, defined as usual, with its natural valuation and cross-section. Suppose G is solvable and decidable as an ordered group. Then $k((G))\lceil\mathcal{L}$ is decidable.*

PROPOSITION 3: *If A is an abelian divisible group without torsion, or with $pA = 0$ for a prime p, and G an ordered solvable group, decidable as an ordered group, then the well-ordered Wreath-product $WO(AWB)$ is decidable.*

Ido Efrat: Profinite groups modulo the real core

The talk considered the quotient of a profinite group G by its real core N (i.e., N is the closed subgroup of G generated by all involutions). It was shown that if $G \cong G_K$ is the absolute Galois group of a field K, then G/N is torsion-free. For example, $\mathrm{Gal}(\mathbb{Q}^{tr}/\mathbb{Q})$ is torsien-free answering a question posed by M. Fried

and D. Haran. We presented a Galois-cohomological proof of the following: If G has a projective open subgroup of index ≤ 2 and if G satisfies certain conditions imposed on an absolute Galois group by Artin–Schreier theory, then G/N is projective (when $G = G_K(2)$, this has been proved by Ershov and Ware, independently, using field-theoretical tools). This enables proving a going up property for real projective groups, due to Haran, without using Artin–Schreier cohomology.

Mike Fried: Factoring Polynomials in finite fields

We give an example of an application of the arithmetic of covers that is not an addition to the inverse Galois problem. F. Chung introduced certain graphs: n fixed, k a finite field, K/k of degree n, $K = k(\zeta)$. Form of directed graph: Vertices are $\alpha \in K^\times$, $\alpha \to \beta$ if $\beta/\alpha = \zeta + a$ for some $a \in k$.

QUESTIONS:

(1) *Is the graph connected? (Do the* $\{\zeta + a\}_{a \in k}$ *generate* $K^\times$*?)*

(2) *What is the diameter? (Least integer such that* $\prod_{i=1}^{d}(\zeta + a_i)$ *runs through all* $K^\times$*.)*

Katz in Math. Ann. 286 (1990) 625–637 shows for some constant $B(n)$, if $|k| > B(n)$, $d = n + 2$ suffices. He gives as an unsolved problem if $d = n + 1$ does also ($d = n$ trivially does not). We give a quick proof of Katz's result, then we use Hurwitz spaces to show for each n there exists infinitely many k and $f \in k[x]$, f irreducible of degree n, for which $d = n + 1$ does not suffices a as diameter bound. The case $n = 3$ was quite explicit: the essential ingredient was construction of $\mathbb{P}^1 \to \mathbb{P}^1$ by $x \to m(x)$ of degree 4 with alternating group A_4, as geometric monodromy group and S_4 as arithmetic monodromy group.

Mike Fried: Reminiscences on a period of work on the Inverse Galois Problem

We gave some historical comments on the relations among the work of the speaker, Ax, Debes, Haran, (Mike) Artin, Harbater, Pop, Jarden, Shimura, Völklein, Serre, Jensen, Thompson. Here are some of the unsolved problems discussed in the talk.

Assume all fields are countable of characteristic 0.

1. Define K to be R(egular)G(alois)-Hilbertian if for each $L/K(t)$ Galois with $L \cap \bar{K} = K$ there exists infinitely many $t_0 \in K$ with $G(L_{t_0}/K) = G(L/K(t))$.

THEOREM (Fried-Völklein): *If K is PAC, K is RG-Hilbertian if and only if each finite group is a quotient of G_K.*

THEOREM (Fried-Völklein): *If K is PAC, K is Hilbertian if and only if G_K is pro-free*.*

Thus Hilbertian and RG-Hilbertian have a complete Galois theoretic characterization for the case K is PAC. There is a notion of real Hilberianity that allows us to characterize existence of certain quotients of $G(L/K(t))$ arising from specializations L_{t_0}/K. Consider the exact sequence:

$$1 \longrightarrow G(L/\hat{K}(t)) \longrightarrow G(L/K(t)) \xrightarrow{\text{res}} G(\hat{K}/K) \longrightarrow 1.$$

Here $\hat{K} = \bar{K} \cap K$. Let H^* be the largest subgroup of $G(\hat{K}/K)$ generated by images of involutions of $G(\bar{K}/K)$. Let G^* be the largest subgroup of $\text{res}^{-1}(H^*)$ generated by involutions. Then K is **real Hilbertian** if $G^* = G(L_{t_0}/K)$ for infinitely many $t_0 \in K$.

* Editorial comment: The easier direction, K PAC and G_K free profinite group implies K Hilbertian, is due to Roquette.

For example the field $\mathbb{Q}^{tr}$ is real Hilbertian. Find analogous theorems for fields that are RG-real Hilbertian and real Hilbertian. See [Fried-Haran-Völklein] for a pretty good start in this direction: $G_{\mathbb{Q}^{tr}}$ is freely generated by involutions.

2. There is a PAC field $P/\mathbb{Q}$ that is Galois with group $\prod_{n=2}^{\infty} S_n$. (Fried-Jarden): Thus,

$$(*) \qquad 1 \longrightarrow \hat{F}_\omega \longrightarrow G(\hat{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \prod_{n=2}^{\infty} S_n \to 1.$$

To get a truly natural field like P it is probably better to use in its place the composite $\mathbb{Q}^{symm}$ of all Galois extensions $L/\mathbb{Q}$ with $G(L/\mathbb{Q}) = S_n$ for some n. This, however, has the property that the group on the right of (*) is a little complicated. Better yet, try the composite $\mathbb{Q}^{alt}$ of all Galois extensions $L/\mathbb{Q}$ with $G(L/\mathbb{Q}) = A_n$ for some n.

THE PROBLEM: *Is* $\mathbb{Q}^{alt}$ *PAC?*

OTHER TOPICS IN THE TALK. $\mathbb{Q}^{tr}(i)$ (The field of complex multiplication); nonrealizatibility of D_p^∞ as a regular extension of $\mathbb{Q}(t)$ [Fried; Review of Serre's *Topics in Galois Theory*]; The lifting invariant for covers $X \to \mathbb{P}^1$ with branch cycles as 3-cycles (the two compenents of the Hurwitz space are both defined over $\mathbb{Q}$); and the appearance of arithmetic geometric group extensions coming from going to the Galois Closure.

W.-D. Geyer: Fundamental and Braid Groups

This was the first of several lectures about the Fried-Völklein paper on realizing groups as Galois groups using Hurwitz moduli spaces for covers of the Riemann sphere with given data. In this talk the basic definitions and properties of fundamental groups were developed, the Galois theorem of (unramified) covers was studied. This was applied to the theory of ramified covers of the Riemann sphere

$\mathbb{P}_1(\mathbb{C})$. Riemann's existence theorem and some corollaries and the branch cycle argument were explained. To deal with deformation of covers of $\mathbb{P}_1(\mathbb{C})$ different braid groups were introduced as fundamental groups of higher dimensional many folds. The full and the pure Artin braid group, and its projective counterpart, the full and pure Hurwitz braid group. The structure of these groups was explained, especially the operation of the braid group on the fundamental group of the punctured Riemann sphere.

W.-D. Geyer: Realization of l-groups over global fields

Scholz (1936) has shown that over $\mathbb{Q}$ every l-group, G with $l \neq 2$ is realizable as Galois groups. Reichardt (1937) has improved this proof, his version can be found in Serre's "Topics in Galois Theorey"(1992). All these proofs use the theory of cyclotomic extensions as an essential tool. Šafarevič (1954) gave another proof, overcoming the exception $l \neq 2$, by using the concept of a Scholz field but then developing a huge combinatorial apparatus to solve the occurring embedding problems. In this joint work with M. Jarden under report we try to translate first the result of Scholz to algebraic functions fields in one variable over a finite field. The cyclotomic extensions do not work there, we had to replace them by class field theory. The finite result give not only extensions with given l-group G, but we can very precisely control the ramification of the extension (which explodes in Šafarevič's approach), such that we can bound the number and (by Čebotarev's density theorem) the degree of the ramfied primes. As a consequence we get a bound to the genus of the field on which the group G acts (resp., to the discriminant, in the number field case). The precise result is as follows: Let K be a global field, let s be the rank of the global units, r be the l-rank of the class group. Assume l to be a prime such that $\zeta_l \notin K$. Then given a finite set S_0 of primes in K there is a set S_1 of $r+s$ exceptional primes such that: Given

an l-group G of order l^m there is a Scholz extension $L|K$ with Galois group G such that the ramified field primes in $L|K$ are contained in $S_1 \cup \{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$, where the $\mathfrak{q}_i$ are given by congruence conditions; moreover all primes in S_0 split completely in $L|K$.

D. Haran: The absolute Galois group of the field of totally real algebraic numbers $\mathbb{Q}^{tr}$

The main result: $G(\mathbb{Q}^{tr}) \cong \hat{D}_\omega$ = the free product of groups of order 2 over the Contor space X_ω. Furthermore, $\mathbb{Q}^{tr}$ is decidable.

This follows as $\mathbb{Q}^{tr}$ is PRC (Pop) and from this:

THEOREM: *Let K be a PRC field, L/K a Galois extension, L not formally real, H a finite group, $I \subseteq H$ a conjugacy domain of involutions, and π: $H \to G(L/K)$ an epimorphism such that*

$$\pi(I) = I(L/K) := \{\varepsilon \in G(L/K) |\ \varepsilon^2 = 1,\ L(\varepsilon) \text{ is not formally real }\}.$$

Then there exists a Galois extension F of $K(x)$, regular over L, and an isomorphism h such that

$$\begin{array}{ccc} G(F/K(x)) & \xrightarrow{\ h\ } & H \\ & {\scriptstyle \mathrm{res}_L} \searrow \quad \swarrow {\scriptstyle \pi} & \\ & G(L/K) & \end{array}$$

commutes and $h(I(F/K(x)) = I$.

To show this, we first construct a point q on the Hurwitz space $\mathcal{H}^{\mathrm{inn}}$ that represent the required extension and h is the case $K = \mathbb{R}$.

In the general case we partition the space of ordering $X(K)$ of K into clopen subsets $X_1, \ldots, X_m$, and construct appropriate points $q_1, \ldots, q_m \in H^{\mathrm{inn}}$ of the above type, each for a certain subgroup H_i, $i = 1, \ldots, m$, and a certain subset

$I_i \subseteq H_0$ of involutions. We then apply the PRC property to fined $p \in \mathcal{H}(K)$ such that p approximates q_i for each $P \in X_i$. This p gives the desired extension F and the isomorphism h.

D. Haran: Schur multiplier and the Conway-Parker Theorem

This talk gave the group-theoretical background for the work of Fried and Völklein. We defined the Schur multiplier of a finite group G and being "generated by commutators". Every finite group is a quotient of a group with the latter property. We proved the Conway-Parker Theorem for such groups.

Moshe Jarden: PAC Fields over Subrings

This is a report about a joint work with Aharon Razon.

Definition: A field M is said to be **PAC over a subring** O, if for every absolutely irreducible polynomial $f \in M[T, X]$ and every $0 \neq g \in M[T]$, there exist $a \in O$ and $b \in M$ such that $f(a, b) = 0$ and $g(a) \neq 0$.

THEOREM: *If O is a countable Hilbertian field and K is its quotient field, then for almost all $\sigma \in G(K)^e$, $K_s(\sigma)$ and $\tilde{K}(\sigma)$ are PAC over O.*

Example: $O = \mathbb{Z}$ and $K = \mathbb{Q}$. ∎

Remark: A PAC field over itself is just a "PAC field". ∎

The work shows that all algebraic extensions of $\mathbb{Q}$ which are known to be PAC, except $\tilde{\mathbb{Q}}(\sigma)$, are not PAC over $\mathbb{Q}$. In particular, $Q_{\mathbf{symm}}$ and any finite extension of $Q_{\mathbf{tr}}$ are not PAC. We don't know of any example of a Galois extension of $\mathbb{Q}$ which is PAC over O except $\tilde{\mathbb{Q}}$.

LOCAL GLOBAL PRINCIPLE.

Data: In the above notation suppose that O is a Dedekind domain, K is a global field, and M is an algebraic extension of K which is perfect and PAC over O. Let $\mathcal{V}_M$ be the set of all valuations of M which are integral over O and let $\mathcal{W}$ be a finite subset of $\mathcal{V}_M$. For each $v \in \mathcal{V}_M$ let $\hat{M}_v$ be the completion of M at v and let $\hat{O}_{M,v}$ be its valuation ring. Finally let $\mathcal{V}$ be an absolutely irreducible variety over M. ∎

THEOREM: *If $\mathcal{V}(\hat{O}_{M,v}) \neq \emptyset$ for each $v \in \mathcal{V}_M$, then $V(O) \neq \emptyset$. Moreover, for each finite subset $\mathcal{W}$ of $\mathcal{V}_M$, $V(O)$ is dense in $\prod_{w \in \mathcal{W}} V(\hat{O}_{M,w})$.*

C.V. Jensen: Prodidhedral extensions of finite number fields

The talk represented joint work with W.-D. Geyer. Let $L = K(\sqrt{d})$ be a quadratic extension of a number field K. Consider the two statements:

(1) Does there exists $\hat{D}_p$-extension of K which is $\hat{\mathbb{Z}}_p$-extension of L?

(2) L is not totally real.

Then (2) $\Rightarrow$ (1). Also (1) $\Leftarrow$ (2) if one assumes Leopoldts conjecture for L. Here $\hat{D}_p$ is the projective limit $\varprojlim D_{p^n}$ of the dihedral groups of order $2p^n$.

Several explicit examples and applications were given.

J. Koenigsmann: Valuations elementarily definable from multiplicative subgroups of fields

Given a multiplicative subgroup $M \leq K^\times$ in a field K and a compatible valuation v of K (i.e. $1+\mathfrak{m}_v \subseteq M$, where $\mathfrak{m}_v$ denotes the maximal ideal of the corresponding valuation ring O_v), the question when O_v is elementarily definable in terms of M has been asked in various centexts (e.g. by Diller, Dress, Berer, Jacob, Arason, Ware). If $[K^\times : M] = 2$ and $M + M \not\subseteq M$ (i.e. M is a "half-ordering" of K), one

can show by introducing a topology induced by M on K, that there always exists a valuation definable in terms of M. Using this, an explicit formula for a valuation compatible with finitely many orderings $P_1, \ldots, P_2$ (here $M = P_1 \cap \cdots \cap P_n$) can be given. Also, for any henselian non-euclidian field with n square classes, where $1 < n < \infty$, this method yields a henselian valuation which is 1^{st}-order definable in the language of fields.

Angus Macintyre: The Field of Real Exponential Algebraic Numbers

Joint work with A. J. Wilkie. Wilkie's proof of model completeness of the restricted exponential field is effectivise, by giving effective estimates for rates of growth for definable families of definable functions. Then Schanuel's Conjecture is used to embed the prime model of real exponentiation, the field of real exponential-algebraic numbers, into all models of a certain recursive model-complete subtheory of the real field. Combining this with Ressayre's methods allowing easy transition to unrestrected exponentiation, we prove:

THEOREM: *If Schanuel's Conjecture is true, the theory of the real exponential field is decidable.*

P. Müller: Exceptional Polynomials

An outline of the preprint "Schur covers and Carlitz's conjecture" by M. Fried, R. Guraling and J. Saxl was given. The main object of this work is to classify exceptional polynomials as close as possible, is particular close enough to prove Carlitz's conjecture. A polynomial f over in finite field k is exceptional if it induces a bijection on infinitely many finite extensions of k, of equivalently if no irreducible (over k) factor of $\frac{f(x)-f(y)}{x-y}$ is absolutely irreducible. The latter yields strong constraints about the points of the arithmetic and geometric monodromic groups of f. Besides possible exceptions in characteristics 2 and 3, the arithmetic

monodromy group of an indecomposible (one may assume this without loss of generality) is primitive of affine type q, where the degree is a power of char(k), this information proves Carlitz's which asserts that in odd characteristics the degree of an exceptional polynomial is odd. Finally, the first example of an exceptional polynomial with non-solvable arithmetic monodromic group recently constructed was given.

Thanases Pheidas: Solvability questions in function fields

We announced the new result: The existential theorey of the function field $F(t)$ with char(F) ≥ 5 in the language $\{0, 1, t, +, \cdot\}$ is undecidable.

We surveyed a number of relevant older results and gave outlines for the proofs in the case of $\mathbb{C}[t]$ and $\mathbb{R}[t]$ pointing out certain analogies. We asked a number of questions, manly:

(1) Is the theorey of $\mathbb{C}[t]$ decidable?

(2) Is the existential theory of $\mathbb{C}[t]$ decidable?

(3) Is "$\mathrm{ord}_0 x > 0$" definable in $\mathbb{C}[t]$? Exist. definable?

Florian Pop: $\frac{1}{2}$RET and Applications

Let K be henselian field with respect to a non-trivial valuations v and $S \subseteq \mathbb{P}^1_k$ a finite set of closed points. If $\bar{S} = S \times_K \bar{K} = \{x_1, \ldots, x_{n_s}\}$ ($n_s = 2n$, even) can be organized in pairs $p_k = (x_k, y_k)$ which are permuted by G_x and $x_k \approx y_k$ v-adically, then setting U for the complement of S one has:

$\frac{1}{2}$RET: *The canonical exact sequence* $1 \longrightarrow \pi_1(\bar{U}) \longrightarrow \pi_1(U) \longrightarrow G_K \longrightarrow 1$ *has canonically a quotient of the form* $1 \longrightarrow \bar{\Pi} \longrightarrow \Pi \xrightarrow{\rho_\Pi} G_K \longrightarrow 1$, *where*

$$\bar{\Pi} = \langle g_{x_1}, h_{y_1}, \ldots, g_{x_n}, h_{y_n} \mid g_{x_k} h_{y_k} = 1,\ g_{x_k}^{s_k} = 1 \rangle,$$

with s_k a supernatural number with all components ∞, but the one component to p, if $\mathrm{char}(K) = 0$, $\mathrm{char}(K_v) = p > 0$. Moreover, ρ_Π has a section α such that the action of G_K on Π via α is given by $(g_{z_k})^\sigma = g_{\sigma^{-1}z_k}\chi_{\mathrm{cycl}}(\sigma^{-1})$. Several applications of the above theorem were given, like:

(1) *If K is a countable Hilbertian PAC field then G_K is ω-free.*

(2) *If K is global field and K^Σ is the field of totally Σ-adic numbers for some finite subset $\Sigma \subseteq \mathbb{P}(K)$, then $G_{K^\Sigma,\mathrm{cycl}}$ is ω-free.*

(3) *With the notation from above one has*

$$G_{K^\Sigma} = \bigstar_{\mathfrak{p}\in\Sigma} G_{K_\mathfrak{p}}^W$$

when W is the Cantor space and $K_\mathfrak{p}$ is the completion of K with respect to $\mathfrak{p} \in \Sigma$.

Aharon Razon: The Local Global Principle for PAC fields over Subrings

This is a report about a joint work with Moshe Jarden. We have proved, following the methods of Roquette et al. for $\tilde{\mathbb{Q}}$, the local global principle for absolutely irreducible varieties defined over a perfect algebraic PAC field M over a Dedekind domain O with a global quotient field K.

The transition to non algebraically closed fields poses some difficulties, which we have succeeded to overcome. First, for each polynomial $h \in M[X]$ we have assured the existence of an M-rational root of a polynomial h' in $M[X]$ which is $\mathcal{T}$-close enough to h, where $\mathcal{T}$ is a Zariski-closed set of valuations of M which are integral over O. Second, for each $x \in \tilde{K}$ and each positive integer ε, we have showed the existence of a finite extension L of K which is contained in M such that for each $v \in \mathcal{T}$ and each $\sigma \in G(K)$ there exists $b \in L$ with $v(b - x^\sigma) > \varepsilon$. (If M/K is normal then this is trivial.) Third, for a function field

of one variable F over M and a function $f \in F$, we have proved the existence of an M-rational zero of a function g in F which is $\mathcal{T}$-close enough to f.

We have managed to overcome these three difficulties using the PAC property of M over O.

W. M. Ruppert: Solving algebraic equations in roots of unity

Let $f \in \mathbb{C}[x,y]$ be an irreducible polynomial of degree (d_1, d_2). The problem is to find all (ζ_1, ζ_2) where ζ_1, ζ_2 are roots of unity and $f(\zeta_1, \zeta_2) = 0$.

It is well known that there are infinitely many such solutions iff $f = c(x^{d_1} - \zeta y^{d_2})$ or $f = c(x^{d_1} y^{d_2} - \zeta)$ where ζ is a root of unity (Ihara, Serre, Tate, ...). If there exist only finitely many solutions in roots of unity a procedure was sketched how one can actually find them. A consequence is that the number of such solutions is $\leq 22 d_1 d_2 - 2d_1 - 2d_2$. The quality of the estimate is indicated by the polynomial $f(x,y) = x^{d_1} y^{d_2} + \frac{1}{2 \sin \frac{2\pi}{15}} (x^{d_1} - y^{d_2}) - 1$ which has $14 d_1 d_2$ solutions in roots of unity. For the general case, i.e. looking for solutions in roots of unity of $f_1(x_1, \ldots, x_n) = f_2(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0$ there exists also an algorithm how one can find them and a structure theorem how the Zariski closure of these solutions looks like.

Joachim Schmid: Sums of fourth powers of rational functions

In this talk the following theorem was presented: Let K be a formally real field such that 3 is a square in K and assume that $P_2(K) = 2$. Then $P_4(K) \leq 6$. Here $P_2(K)$ (resp., $P_4(K)$) is the 2nd (resp. 4th) Pythagaran number of the field K.

H. Völklein: Moduli spaces for covers of the Riemann sphere

These moduli spaces were originally constructed by Fried and Völklein (Math. Ann. 1991), extending earlier work of Fried (Comm. Algebra 1977). They are

generalizations of the classical moduli spaces for simple covers of $\mathbb{P}^1$ studied by Hurwitz. The talk described a new construction of these spaces that is not based on the generalized Riemann existence theorem.

Application include on exact sequence for $G_{\mathbb{Q}}$:

$$1 \longrightarrow F_\omega \longrightarrow G_{\mathbb{Q}} \longrightarrow \prod_{n=2}^{\infty} S_n \to 1$$

where $\hat{F}_\omega$ is the free profinite group of countable rank (Fried–Völklein, Annal. 1992). Further, Galois realizations over $\mathbb{Q}$ of the groups $\mathrm{GL}_n(q)$ and $\mathrm{PU}_n(q)$, n even $n \geq q$.

H. Völklein: Solvability of regular embedding problems and rational points on moduli spaces

We use the moduli spaces for covers of the Riemann sphere that were constructed in joint work with M. Fried. It is shown that the existence of k-rational points on certain twists of these spaces implies the solvability of certain regular embedding problems over k. This can be used to prove that all embedding problems over a Hilbertian PAC field of characteristic zero are solvable.

Berichtersatter: Aharon Razon

Tagungsteilnehmer

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

70109 Bucharest 1
ROMANIA

Prof.Dr. Pierre Debes
Problemes Diophantiens
Universite P. et M. Curie
Mathematiques, T. 45-46, 5ème et.
4 Place Jussieu

F-75252 Paris Cedex 05

Prof.Dr. Luc Belair
Dép. de Mathématiques et
Informatique
Université du Quebec à Montreal
C.P. 8888, Succ. A

Montreal H3C 3P8
CANADA

Prof.Dr. Françoise Delon
U. F. R. de Mathématiques
Case 7012
Université de Paris VII
2, Place Jussieu

F-75251 Paris Cedex 05

Dr. Ralph Berr
Fachbereich Mathematik
Universität Dortmund

D-44221 Dortmund

Ido Efrat
Fakultät für Mathematik
Universität Konstanz
Postfach 5560

D-78434 Konstanz

Prof.Dr. Zoe Chatzidakis
Department of Mathematics
Wesleyan University

Middletown , CT 06459-0128
USA

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

Irvine , CA 92717
USA

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

New Brunswick , NJ 08903
USA

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

D-91054 Erlangen

Dr. Dan Haran
School of Mathematical Sciences
Tel Aviv University
P.O. Box 39040

69978 Tel Aviv
ISRAEL

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

D-69120 Heidelberg

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

Tel Aviv , 69978
ISRAEL

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

GB-Oxford , OX1 3LB

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

D-50931 Köln

Peter Müller
Mathematisches Institut
Universität Erlangen
Bismarckstr. 1 1/2

D-91054 Erlangen

Prof.Dr. Christian Uwe Jensen
Matematisk Institut
Kobenhavns Universitet
Universitetsparken 5

DK-2100 Kobenhavn

Prof.Dr. Thanases Pheidas
Dept. of Mathematics
University of Crete
P. O. Box 1470

71406 Iraklion Crete
GREECE

Jochen Koenigsmann
Fakultät für Mathematik
Universität Konstanz
D 197
Postfach 5560

D-78434 Konstanz

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

D-69120 Heidelberg

Prof.Dr. Alexander Prestel
Fakultät für Mathematik
Universität Konstanz
D 197
Postfach 5560

D-78434 Konstanz

Joachim Schmid
Fachbereich Mathematik
Universität Dortmund

D-44221 Dortmund

Prof.Dr. Aharon Razon
Dept. of Mathematics
Tel Aviv University
Ramat Aviv
P.O. Box 39040

Tel Aviv , 69978
ISRAEL

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

Gainesville , FL 32611-2082
USA

Dr. Wolfgang M. Ruppert
Mathematisches Institut
Universität Erlangen
Bismarckstr. 1 1/2

D-91054 Erlangen

Prof.Dr. Carol Wood
Department of Mathematics
Wesleyan University

Middletown , CT 06459-0128
USA

Franz-Viktor Kuhlmann: On the valuation theoretical structure of nonarchimedean exponential fields

This talk was a report on the work of Salma Kuhlmann.

Every ordered field K admits a natural valuation v such that the value of an element is represented by its archimedean class. v is nontrivial iff the field is nonarchimedean. If the field admits an exponential f, then it induces a special structure on the value group G. Note that G as an ordered abelian group also has a natural valuation v_G. If f is just an order preserving isomorphism between the additive group of K and its multiplicative group of positive elements (a "weak exponential"), then it already follows that there exists an isomorphism φ between the negative part $G^{<0}$ of G and the rank $v_G(G)$ of G (as orders). If f satisfies certain growth axioms, then this may be expressed by the additional property of φ to satisfy $\forall \alpha \in G$: $\varphi(\alpha) < v_G(\alpha)$. Conversely, if the value group G admits an order isomorphism φ: $G^{<0} \to v_G(G)$, if K is countable and if its residue field $\overline{K}$ admits an exponential, then K admits a weak exponential. If φ has the above mentioned additional property, then K admits a weak exponential f satisfying additional growth axioms such as $\forall x$: $f(x) > 1 + x$.

The valuation theoretical interpretation of growth axioms for exponentials on nonarchimedean fields was given and the structure induced on the value group was discussed in detail. Moreover, we exploited the idea to split an exponential into a left, a middle and a right exponential according to a decomposition of the additive group into a lexicographical sum of three subgroups, the one on the right being the valuation ideal and the one on the left a group complement to the valuation ring. Then, the left exponential induces the special structure on the value group, and the middle exponential induces an exponential on the residue field.