Mathematisches Forschungsinstitut Oberwolfach

Report No. 6 / 2002

The Arithmetic of Fields

February 3rd – February 9th, 2002

The third conference on "Field Arithmetic" in Oberwolfach convened in 1998. In 2000 the Mathematical Reviews published a new Subject Classification. It includes the code 12E30 for "Field Arithmetic."

The fourth conference on "Field Arithmetic" in Oberwolfach took place from 3rd – 9th February, 2002. Twenty–four people from Austria, Denmark, France, Germany, Israel, Russia, and USA participated in the conference. The central topic of the conference was Galois theory and connections to covers. Here are some highlights:

Pierre Dèbes: $\hat{F}_\omega$ occurs as a Galois group over $\mathbb{Q}_p^{\mathrm{cycl}}(t)$.

Goetz Wiesend: A description the absolute Galois group of $\mathbb{Q}_p(t)$ as the fundamental group of a graph of profinite groups.

Jakob Stix: A result in an-abelian geometry of characteristic p: Let X and X' be geometrically connected smooth proper curves of genus at least 2 over a field K which is finitely generated over $\mathbb{F}_p$. Suppose one of the curves is not defined over a finite field and the geometric fundamental groups of X and X' are Galois-isomorphic. Then X and X' are isomorphic up to a Frobenius automorphism.

Jochen Koenigsmann: Application of model theory to prove Grothendieck's section conjecture over $\mathbb{Q}_p$.

Helmut Völklein: Every general curve of genus $g \geq 3$ covers $\mathbb{P}^1$ with monodromy group A_n for each $n \geq 2g+1$.

Michael Fried: Presented an isotriviality result for extensions $K((y))/K((x))$ of fixed ramification type, where K is an algebraically closed field of positive characteristic.

Michael Dettweiler: Constructed a new compatible geometric system of l-adic representations of the absolute Galois group of a number field K with images $\mathbb{Z}_l^\times \cdot SL_3(\mathbb{Z}_l)$ or $\mathbb{Z}_l^\times \cdot SU_3(\mathbb{Z}_e)$.

John Swallow: Considered a cyclic p-extension L/K with K a field containing all pth roots of unity and described the structure of $L^\times/(L^\times)^p$ as an $\mathbb{F}_p[\mathrm{Gal}(L/K)]$-module.

Bernd Heinrich Matzat: Presented a generalization of Abhyankar's conjecture to differential Galois theory in positive characteristic.

Peter Müller: Used Siegel's theorem to give a stronger version of Hilbert's irreducibility theorem under certain conditions. E.g. consider a number field K and an irreducible polynomial $f \in K(t)[X]$ such that the genus of the curve $f(t,X) = 0$ is positive and $\mathrm{Gal}(f(t,X), K(t))$ permutes the roots of $f(t,X)$ doubly transitive. Then there are only finitely many $a \in K$ such that $f(a,X)$ is defined and reducible.

Moshe Jarden: Proved that if the absolute Galois group of a field K is a pro-p group, then K is ample.

Walter Hofmann: Considered a square free integer a and computed the number of quadratic extensions K of $\mathbb{Q}(\sqrt{a})$ with the following property: For each positive integer n the field $\mathbb{Q}(\sqrt{a})$ has a cyclic extension of degree 2^n which contains K.

Abstracts

Infinite Inverse Galois Theory

Pierre Dèbes, Lille
(joint work with Bruno Deschamps)

We provide some tools to investigate the inverse Galois Problem for profinite groups: the notions of ψ-freeness and regular ψ-freeness, a general construction of infinite Galois extensions of $k(T)$ over a complete valued perfect field k. An application is that if the residue characteristic is 0 (e.g. $k = \mathbb{Q}((x))$), then the free profinite group $\widehat{F}_\omega$ with countably many generators is the Galois group of a regular extension of $k^{\mathrm{cycl}}(T)$. This result extends to the case k is henselian, even with residue characteristic $p > 0$ provided that $\widehat{F}_\omega$ is replaced by its maximal prime-to-p quotient $\widehat{F}_\omega^{(p')}$. We also show that, given a finite group G, if $\mathrm{char}\, k = 0$ (or if G is p-perfect), for almost all primes l, the universal l-Frattini cover of G is the Galois group of a regular extension of $k(T)$ (no adjunction of roots of unity is necessary here). In a parallel way our methods give rise to existence results of projective systems of rational points (over various valued fields) on certain infinite towers of moduli spaces of G-covers, like the modular towers of M. Fried.

On λ-adic representations of motives

Michael Dettweiler, Heidelberg
(joint work with Stefan Reiter)

The starting point of our considerations is the following result of Serre:

Theorem *Let E be an elliptic curve defined over a number field K, T_l its Tate module and $\rho_l : \mathrm{G}_K \to \mathrm{GL}(T_l)$ the induced representation of the absolute Galois group of K. If E has no complex multiplication, then the following holds:*

a) The image of ρ_l is equal to $\mathrm{Aut}_{\mathbb{Z}_l}(T_l)$ ($\simeq \mathrm{GL}_2(\mathbb{Z}_l)$) for almost all l.

b) The Zariski closure of the image of ρ_l in $\mathrm{Aut}_{\mathbb{Q}_l}(T_l)$ is equal to $\mathrm{Aut}_{\mathbb{Q}_l}(T_l)$ ($\simeq \mathrm{GL}_2(\mathbb{Q}_l)$) for every l.

c) The image of ρ_l is an open subgroup of $\mathrm{Aut}_{\mathbb{Z}_l}(T_l)$ for every l.

It is assumed (and proved in many cases) that similar statements hold for the Tate modules of abelian varieties of higher dimensions which are defined over a number field.

Motives are considered to serve as a substitute for the concept of Jacobians of curves (and their Tate modules) for higher dimensional varieties. One conjectures that also similar statements as in the elliptic curve case hold.

We give a criterion for Galois images to be irreducible and apply this to the *van Geemen-Top motive M*. The van Geemen-Top motive is a submotive of $h^2(\mathcal{X})$, where $\mathcal{X}$ is a certain surface. This surface was first studied by A. Ash and D. Grayson and later considered by B. van Geemen and J. Top. They use the λ-adic representations of M in order to provide evidence on a conjecture of Clozel. This conjecture predicts a compatible system of Galois representations associated to non-selfdual automorphic representations of adelic linear groups $\mathrm{GL}_n(\mathbb{A})$.

We derive further properties of the λ-adic realizations of M and, in particular, prove an analogue of Serre's theorem for the van Geemen-Top motive.

Theorem 1. *a) For almost all primes λ of $\mathbb{Q}(i)$*

$$\operatorname{im}(\rho_{M,\lambda}) = \mathrm{SL}_3(\mathbb{Z}_l)\cdot\mathbb{Z}_l \qquad \text{if } l = l(\lambda) \equiv 1 \mod 4,$$

resp.

$$\operatorname{im}(\rho_{M,\lambda}) = \mathrm{SU}_3(\mathbb{Z}_l)\cdot\mathbb{Z}_l \qquad \text{if } l \equiv 3 \mod 4.$$

b) Denote by G_λ the Zariski closure of $\operatorname{im}(\rho_{M,\lambda})$. Then

$$G_\lambda = \mathrm{SL}_3(\mathbb{Q}_l)\cdot\mathbb{Q}_l \qquad \text{if } l \equiv 1 \mod 4,$$

resp.

$$G_\lambda = \mathrm{SU}_3(\mathbb{Q}_l)\cdot\mathbb{Q}_l \qquad \text{if } l \equiv 3 \mod 4,$$

resp.

$$G_\lambda = \mathrm{GL}_3(\mathbb{Q}(i)_2)\cdot\mathbb{Q}_2 \qquad \text{if } l = 2.$$

c) For all primes λ of $\mathbb{Q}(i)$, with $l(\lambda) > 2$, $\operatorname{im}(\rho_{M,\lambda})$ is an open subgroup of $\mathrm{SL}_3(\mathbb{Q}_l)\cdot\mathbb{Q}_l$ if $l \equiv 1 \mod 4$, resp. an open subgroup of $\mathrm{SU}_3(\mathbb{Q}_l)\cdot\mathbb{Q}_l$ if $l \equiv 3 \mod 4$.

Then we use Faltings' trick and results of Harbater on Galois extensions unramified outside 2, to deduce that if there exists a system of compatible Galois representations which is associated to the Hecke eigenclass u, then it is equivalent to $\rho_{M,\lambda}$. This can be interpreted as evidence for a generalization of Serre's conjectures (conjecturally associating automorphic representations of $\mathrm{GL}_2(\mathbb{A})$ to odd 2-dimensional Galois representations) to the 3-dimensional case.

Arithmetic decomposition of K-rings of fields

Ido Efrat, Beer Sheva

Let F be a field and let $U \leq F^\times$. One defines $K_*^M(F)/U := \bigoplus_{r=0}^\infty K_r^M(F)/U$ by setting $K_0^M(F)/U = \mathbb{Z}$ and for $r \geq 1$,

$$K_r^M(F)/U = (F^\times/U)^{\otimes r}/\langle a_1U \otimes \cdots \otimes a_rU \mid \exists i \neq j : 1 \in a_iU + a_jU\rangle.$$

Questions:

(a) How is the arithmetic structure of F reflected in the algebraic structure of $K_*^M(F)/U$?
(b) What graded rings are realizable as $K_*^M(F)/U$ for some F, U?

As for question (a), we define a **local pair** on F to be a pair (λ, U) where λ is a **locality** (i.e. either a Krull valuation or an ordering), and $U \leq F^\times$. When λ is a valuation let G_λ be its group of principal units. When λ is an ordering let G_λ be its strictly positive cone. We call (λ, U) **Henselian** if $G_\lambda \leq U$. We call it **degenerate** if $\lambda = v$ is a valuation and $v(F^\times) = v(U)$. We set $(\lambda, U) \leq (\lambda', U')$ if $G_\lambda \leq G_{\lambda'}$ and $U \leq U'$. In this partial ordering one always has infima.

Theorem 1. Suppose:

- $(F^\times)^m \leq S \leq F^\times$, for $1 \leq m \in \mathbb{N}$.
- $(\lambda_1, U_1), \ldots, (\lambda_n, U_n)$ is a system of Henselian non-degenerate local pairs which has minimal length among all such systems with infimum $\inf(\lambda_i, U_i)$.
- $S = \bigcap_{i=1}^n U_i$

Then:

(a) $K_*(F)/S \equiv \bigoplus_{i=1}^{n} K_*(F)/U_i$

(b) $U_i = SG_{\lambda_i}$, $i = 1, \dots, n$

As for question (b), we define (following Bass-Tate) a **κ-structure** to be a graded ring $A = \bigoplus_{r=0}^{\infty} A_r$ with $A_0 = \mathbb{Z}$, $A = \langle A_1 \rangle$, and with a distinguished element $\varepsilon \in A_1$ such that $2\varepsilon = 0$ and for all $a \in A_1$, $a^2 = a\varepsilon = \varepsilon a$ (e.g. take $A = K_*(F)/U$, $\varepsilon = -U$).

Definition. Let $\mathcal{C}$ be the minimal class of κ-structures such that:

- $\kappa := \mathbb{Z}[X]/(2X) \in \mathcal{C}$
- $A, B \in \mathcal{C} \Rightarrow A \oplus_\kappa B \in \mathcal{C}$
- $A \in \mathcal{C} \Rightarrow A[\mathbb{Z}/2] \in \mathcal{C}$

(Here $\oplus_\kappa$ is the natural direct sum of κ-structures, and $A[\mathbb{Z}/2]$ is the naturally defined construction of the **extension** of A by the group $\mathbb{Z}/2$.)
Using Theorem 1 we prove:

Theorem 2. Let A be a κ-structure such that $|A_1| < \infty$, $2A = 0$, $\varepsilon \neq 0$, and A is reduced. Then $A \in \mathcal{C}$ if and only if there exists a field F and $U \leq F^\times$ such that $A \equiv K_*(F)/U$.

Related results about $G_F(2)$ for F Pythagorean were obtained by Jacob and others.

Wonderful extensions and class field theory

Yuri Ershov, Novosibirsk

The notion of a wonderful extension for the field $\mathbb{Q}$ of the rationals was defined in [E1]. There is a natural extension of it for a much wider class of multi-valued fields with orders. It was the notion of immediate extension for Prüfer rings and the notion of existentially closed structures from model theory. Under some reasonable conditions (near Booleans, finite absolute ramification, C-continuity of local elementary properties, ampleness in infinity at residue fields [E2]) it can be proved that such e-closed rings satisfy the local-global arithmetical principle G_A^+ and the maximality principle M.

A wonderful extension W of $\mathbb{Q}$ can be used in the definition of global class field theory taking for an algebraic number field K the group $\mathbb{C}_K \supseteq \mathbb{K}^\times/K^\times$, there $\mathbb{K} \supseteq KW$ as corresponding module. Using the decidability of the theory of wonderful extensions of $\mathbb{Q}$ it is possible to find a decidable wonderful extension W and to compute the reciprocity map effectively.

References

[E1] Yu.L. Ershov, Doklady Mathematics **62_1** (2000), 8–9.

[E2] Yu.L. Ershov, *Multi-Valued Fields*, Kluwer Academic/Plenum Publishers, 2001.

Configuration spaces for wildly ramified covers

Michael D. Fried, Irvine
(joint work with Ariane Mézard)

Take k to be an algebraically closed field of characteristic a prime p. The talk featured these key words: Ramification data, regular ramification data, $\mathcal{R}$-configuration space, families of $\cup_{ij}\mathcal{R}_{ij}$ covers. Given a family of covers of the projective line, their equations reveal discrete invariants about their ramification. For not necessarily Galois extensions we defined the ramification data of local ramified extensions. The first main result is a versal deformation space for local extensions $k((y))/k((x))$ having given ramification type $\mathcal{R}$. Call that $\mathcal{P}(\mathcal{R})$: This appears as an explicit open subspace of same affine space [FM, §1]. Each extension $k((y))/k((x))$ of type $\mathcal{R}$ corresponds to finitely many (though rarely just one) points in $\mathcal{P}(\mathcal{R})$.

Assume a given family's members have a fixed number, r, of branch points. Then assume its locally ramified points fall in a fixed set of ramification data: $\cup_{ij}\mathcal{R}_{ij}$. Locally in the finite topology the $\cup_{ij}\mathcal{R}_{ij}$ configuration space $\mathcal{P}(\cup_{ij}\mathcal{R}_{ij})$ is a natural target for the parameter space of any family having type $\cup_{ij}\mathcal{R}_{ij}$. Further, any family of this type is the pullback of this configuration map from a family over a finite cover of the parameter space image in the configuration space. This generalizes Grothendieck's tame version of the result [Gr]. A special case is an iso-triviality result: If a family has a constant map to the configuration space, after finite pullback it is a trivial family.

This result depends on a generalization of Garuti's result [Ga]. Garuti said briefly: You can't expect to lift a Galois wildly ramified cover $\phi : X \to \mathbb{P}^1$ to characteristic 0. [Ga] says a curve cover $\phi' : X' \to \mathbb{P}^1$ where X' has cusp singularities and normalization X is the special fibre of a curve over the Witt vectors of k. We discussed Galois closures of families, an essential (and subtle) necessity in our result. This applies to constructing families of wildly ramified covers starting from families of genus 0 curve covers. Well-known topics (like Schur covers and Davenport's problem) are about families of genus 0 covers. We understand these through their monodromy (Galois closure) groups. So, the theory has much potential application. The completed paper is at

`http://www.math.uci.edu/~mfried/psfiles/fr-mez.html` ([FM]).

References

[FM] M. D. Fried and Ariane Mézard, *Configuration spaces of wildly ramified covers*, MSRI Fall 1999 on Arithmetic fundamental groups, PSPUM series of AMS, to appear soon.

[Ga] M. Garuti, *Prolongement de revêtements galoisiens en géométrie rigide. [Extension of Galois coverings in rigid geometry]* Compositio Math. **104** (1996), no. 3, 305–331. MR 98m:14023

[Gr] A. Grothendieck, Revêtements étales et groupe fondamental (SGA I). Lecture notes in mathematics **224**, Springer-Verlag (1971).

Virtually free pro-p groups

Wolfgang Herfort, Wien
(joint work with Pavel A. Zalesskii)

The extension of a free pro-p group by a finite p group is called *virtually free pro-p.* **J.P.Serre** in 1965 proved that every torsion free virtually free pro-p group is itself free pro-p. Then **Serre-Stalling-Swan** proved the analogous result for the case of arbitrary discrete groups and after this **A.Karrass-V.Pietrowski-D.Solitar** (73), **D.Cohen** (73), **P.Scott** (74) gave a description of virtually free groups in terms of *fundamental groups of graphs of finite groups.* **D.Haran** (93), **I.Efrat** (95), **A.J.Engler** (95) gave generalizations of Serre's result to profinite groups with a free (pro-2) closed subgroup of index 2 under certain assumptions on involutions. In the present talk, using the generalization of **Bass-Serre** theory on groups acting on trees to profinite groups acting on profinite trees, due to **P.A.Zalesskii-O.V.Melnikov** (1989), the following result is presented.

Theorem. *The following on a topologically finitely generated pro-p group G is equivalent:*

(i) *G is virtually free pro-p;*
(ii) *G acts on a pro-p tree with finite stabilizers of uniformly bounded orders;*
(iii) *G is the fundamental group of a finite connected graph of finite p-groups;*
(iv) *G is the pro-p completion of an extension of a finitely generated discrete free group by some finite p-group.*

During the proof results of **C.Scheiderer** (99), **W.Herfort-Zalesskii-L.Ribes** (99) and **Herfort-Zalesskii** (99) for cyclic extensions of free pro-p groups have been used. A counter-example shows that one cannot dispense with the assumption of finite generation in the Theorem.

Cyclic embedding problems for quadratic number fields

Walter Hofmann, Erlangen

Let $k = \mathbb{Q}(\sqrt{a})$ with a square free integer a be a quadratic extension of $\mathbb{Q}$. We are interested in quadratic extensions $K|k$ which fulfill the following embedding condition:

(*) For every $n \in \mathbb{N}$ there is a cyclic extension $L|k$ of degree 2^n with $L \supseteq K$

Note that for two such extensions $L_n|k$ and $L_m|K$ with different $n > m$ we do *not* require that $L_n \supseteq L_m$.

To analyse $(*)$ we need two steps: We first check that the embedding can be done locally at all places and then (in certain cases) we also need to check a global condition.

I will start by outlining the local conditions. Let $\mathfrak{p}$ be a (finite) prime of k, and let $\chi_{\mathfrak{p}} : k_{\mathfrak{p}}^{\times} \to \mu_\infty$ be a character which describes the cyclic extension $K_{\mathfrak{p}}|k_{\mathfrak{p}}$. Then one can show that the local embedding problem has a solution if and only if $\chi_{\mathfrak{p}}(\zeta) = 1$ for all $\zeta \in k_{\mathfrak{p}}$ with $\zeta^m = 1$. The latter condition means that all m-th roots of unity, which are in $k_{\mathfrak{p}}$, must be norms in the extension $K_{\mathfrak{p}}|k_{\mathfrak{p}}$.

Looking globally, we need to take into account an affect which is due to the Grunwald-Wang theorem: In certain "special" cases we need to check if an idele class c_0 given by the Grunwald-Wang theorem is a norm in the extension $K|k$. This special case only matters if we ask for extensions of order 2^n, not for other prime powers. This makes this case particularly interesting.

The local conditions demand that $K|k$ is at most ramified over two. Hence we need to find quadratic extensions of k which are only ramified over 2 ("2-ramified"). This can be achieved in the following way: The theory of genera gives a list of unramified quadratic extensions. Using a formula by Šafarevič one can compute the number of 2-ramified quadratic extensions.

Checking these candidate extensions means computing Hilbert symbols over local fields. Doing this one finds that the number $\psi = m+\delta$ of quadratic extensions of $k = \mathbb{Q}(\sqrt{a})$ which fulfil $(*)$ is equal to the number m of prime factors of a, plus an integer $\delta \in \{0, 1, 2\}$ where δ depends on whether a is positive, the congruence class of $a \mod 16$, the congruence class of the primes dividing a and the congruence class of x, where (x, y) is a solution of $a = x^2 - 2y^2$ (if such a solution exists).

New Ample Fields

MOSHE JARDEN, TEL AVIV

A field K is ample if it is existentially closed in $K((t))$. Alternatively: Every algebraic function field of one variable over K with a prime divisor of degree 1 has infinitely many prime divisors of degree 1.

PAC, real closed fields and Henselian fields are ample. So are fields with a local global principle like PRC, PpC and PSC fields.

Theorem. Every field K whose absolute Galois group is pro-p is ample.

Colliot-Thélène proved this theorem when K is perfect.

A remark on real radical extensions

CHRISTIAN U. JENSEN, KOBENHAVN

Let n be an odd integer > 2 and $f(x)$ an irreducible polynomial in $\mathbb{Q}[X]$ of degree n with the dihedral group D_n of order $2n$ as Galois group. Then $f(x)$ has a root α expressible by real radicals iff α is the only real root and every prime divisor of n is a Fermat prime.

An application to class fields:

Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic number field and L its absolute class field. As known from complex multiplication, $L = \mathbb{Q}(j(\omega), \sqrt{-D})$, where 1, ω, $(\Im(\omega) > 0)$ form an integral basis of K and j is the modular invariant. $j(\omega)$ is a real algebraic number. Here holds: $j(\omega)$ is expressible by real radicals iff every odd prime divisor of the class number h_K of K is a Fermat prime.

On the 'Section Conjecture' in anabelian geometry

JOCHEN KOENIGSMANN, KONSTANZ

The Section Conjecture, due to Grothendieck, says that there is a 1-1 correspondence between the K-rational points $X(K)$ of a smooth complete curve X/K of genus > 1 and the conjugacy classes of sections of the canonical projection $\pi_1(X) \twoheadrightarrow G_K$, where $\pi_1(X)$ is the arithmetic fundamental group of X/K and where K is finitely generated over $\mathbf{Q}$. The birational version of this conjecture says that (for $K/\mathbf{Q}$ f.g.) all sections of the canonical epimorphism $G_{K(X)} \twoheadrightarrow G_K$ are induced by points in $X(K)$.

We prove the birational section conjecture for all smooth complete curves over p-adic local fields and, as a corollary, show that for any curve X over a number field K, sections of $G_{K(X)} \twoheadrightarrow G_K$ can only occur when $X(\hat{K}) \neq \emptyset$ for all completions $\hat{K}$ of K. Moreover, we prove a Galois characterization of K-rational points on any X over almost arbitrary fields K. In particular, this implies the birational fundamental conjecture in an-abelian geometry whenever the fundamental conjecture holds. As another application we obtain a purely group-theoretic criterion for the solvability by radicals of polynomial equations in several variables over almost arbitrary fields.

The Differential Abhyankar Conjecture

BERND HEINRICH MATZAT, HEIDELBERG

In the lecture a differential Galois theory in positive characteristic based on iterative derivations (introduced by H. Hasse and F. K. Schmidt) has been outlined. Then it has been shown that every reduced linear algebraic group over an algebraically closed field K of characteristic $p > 0$ can be realized as Galois group over $K(t)$ solving the inverse problem. Moreover, any such group which is generated by its unipotent subgroups admits a realization with at most one singular point. This generalizes the Abhyankar conjecture for algebraic extensions proved by M. Raynaud for differential Galois extensions.

REFERENCES

[MP1] B. H. Matzat and M. van der Put, *Iterative differential equations and the Abhyankar conjecture*, preprint 2001.

[M] B. H. Matzat, *Differential Galois theory in positive characteristic*, IWR-Preprint 2001-35.

[MP2] B. H. Matzat and M. van der Put, *Constructive differential Galois theory*, IWR-Preprint 2002-02.

Finiteness Results for Hilbert's Irreducibility Theorem

PETER MÜLLER, HEIDELBERG

Let $f(t, X) \in k(t)[X]$ be an irreducible polynomial over a number field k. We provide several sufficient conditions which guarantee that $\mathrm{Red}_f(\mathcal{O}_k) = \{a \in \mathcal{O}_k |\ f(a, X) \text{ is reducible}\}$ is a finite set, where $\mathcal{O}_k$ is the ring of integers of k. The results are based on Siegel's theorem about algebraic curves with infinitely many $\mathcal{O}_k$-points and group theory. A typical example, for which we give the essential steps, is the following:

Suppose that $\mathrm{Gal}(f/k(t))$ permutes the roots of $f(t, X)$ doubly transitively and that the genus of the curve $f(t, X) = 0$ is positive. Then $|\mathrm{Red}_f(\mathcal{O}_k)| < \infty$.

Other results of this flavour require the knowledge of the primitive permutation groups which contain a cyclic subgroup with at most 2 orbits. Using the classification of the finite simple groups, we determined these groups and obtain further applications to Hilbert's irreducibility theorem.

Skolem Density Problems for $\tilde{\mathbb{Q}}[\sigma_1, \dots, \sigma_e] \cap \mathbb{Q}_{\mathrm{tot},\mathcal{S}}$

Aharon Razon, Beer Sheva
(joint work with Moshe Jarden and Wulf-Dieter Geyer)

Let K be a global field, $\mathcal{V}$ an infinite proper subset of the set of all primes of K, and $\mathcal{S}$ a finite subset of $\mathcal{V}$. Denote the maximal Galois extension of K in which each $\mathfrak{p} \in \mathcal{S}$ totally splits by $K_{\mathrm{tot},\mathcal{S}}$. Let M be an algebraic extension of K. A data for an $(\mathcal{S},\mathcal{V})$-Skolem density problem for M consists of a finite subset $\mathcal{T}$ of $\mathcal{V}$ containing $\mathcal{S}$, polynomials $f_1, \dots, f_m \in \tilde{K}[X_1, \dots, X_n]$ satisfying $|f_i|_{\mathfrak{q}} = 1$ for each non-archimedean prime $\mathfrak{q} \in \tilde{\mathcal{V}} - \tilde{\mathcal{T}}$, a point $\mathbf{a} \in M^n$, and a positive real number γ. A solution to the problem is a point $\mathbf{x} \in M^n$ such that $|x_i - a_i|_{\mathfrak{p}} < \gamma$ for each $\mathfrak{p} \in \tilde{\mathcal{T}}$ and $|x_i|_{\mathfrak{q}} \le 1$, $|f_j(\mathbf{x})|_{\mathfrak{q}} = 1$ for each non-archimedean prime $\mathfrak{q} \in \tilde{\mathcal{V}} - \tilde{\mathcal{T}}$, $i = 1, \dots, n$, $j = 1, \dots, m$.

For $\sigma = (\sigma_1, \dots, \sigma_e) \in \mathrm{Gal}(K)^e$ let $K_s(\sigma) = \{x \in K_s \mid \sigma_i(x) = x,\ i = 1, \dots, e\}$. Denote the maximal Galois extension of K inside $K_s(\sigma)$ by $K_s[\sigma]$. Then, for almost all $\sigma \in \mathrm{Gal}(K)^e$ (with respect to the Haar measure), each $(\mathcal{S},\mathcal{V})$-Skolem density problem for $K_s[\sigma] \cap K_{\mathrm{tot},\mathcal{S}}$ has a solution.

This result generalizes a previous work in which $\mathcal{V}$ corresponds to the set of all nonzero prime ideals of $\mathcal{O}_K$ (in particular, $\mathcal{V}$ does not contain archimedean primes). There we prove for almost all $\sigma \in \mathrm{Gal}(K)^e$ that each $(\mathcal{S},\mathcal{V})$-Skolem density problem for the maximal purely inseparable extension of $K_s(\sigma) \cap K_{\mathrm{tot},\mathcal{S}}$ has a solution.

Duality theorems for tori over p-adic curves

Claus Scheiderer, Duisburg

Let k be a p-adic field, let C be a regular projective curve over k and $j \colon V \subset C$ an open subcurve. Let T be a torus over V. We define modified étale cohomology groups of T with compact supports, denoted $H^q_{cc}(V,T)$. They are different from the usual groups $H^q_c(V,T) = H^q(C, j_!T)$ only in degree $q = 1$, and the difference is well understood. The following theorem is joint work with J. van Hamel. It generalizes Lichtenbaum–Tate duality $\mathrm{Pic}(C) \times \mathrm{Br}(C) \to \mathbb{Q}/\mathbb{Z}$:

Theorem. *Let T' be the dual torus of T. There are unique pairings*

$$H^q_{cc}(V,T) \times H^{3-q}(V,T') \to \mathbb{Q}/\mathbb{Z} \quad (q \in \mathbb{Z}) \qquad (*)$$

which are compatible with the cup product pairings

$$H^i_c(V, {}_nT) \times H^{4-i}(V, {}_nT') \to H^4_c(V, \mathbb{Q}/\mathbb{Z}(2)) = \mathbb{Q}/\mathbb{Z}$$

via the Kummer exact sequences. The pairing $(*)$ is non-degenerate on the left for $q \neq 3$, and non-degenerate on the right for $q \neq 2$. The induced pairings

$$\widehat{H^0_{cc}(V,T)} \times H^3(V,T') \to \mathbb{Q}/\mathbb{Z},$$

$$\widehat{H^1_{cc}(V,T)} \times H^2(V,T') \to \mathbb{Q}/\mathbb{Z}$$

and

$$H^2_{cc}(V,T) \times \widehat{H^1(V,T')} \to \mathbb{Q}/\mathbb{Z}$$

are perfect ($\widehat{\ }$ denoting profinite completion). Examples show that the pairings may be degenerate in the excluded cases.

In the second part we sketch some applications. If now T denotes a torus over $K = k(C)$, we use the duality theorem just described to establish a natural exact sequence

$$\begin{aligned} & H^2(K,T')^\vee \to H^1(K,T) \to \prod_P \big(H^1(K_P,T),\ H^1_{\mathrm{nr}}(K_P,T)\big) \\ \to\ & H^1(K,T')^\vee \to H^2(K,T) \to \prod_P \big(H^2(K_P,T),\ H^2_{\mathrm{nr}}(K_P,T)\big) \end{aligned}$$

In particular, there is a duality of finite abelian groups between the Tate-Shafarevich groups $Ш^1(K,T)$ and $Ш^2(K,T')$. Other applications are to weak approximation for T, i.e. to the deviation of $T(K)$ from being dense in $\prod_P T(K_P)$.

Defining Integrality at Primes over Function Fields.

ALEXANDRA SHLAPENTOKH, GREENVILLE

Let C be a product formula field. Let P be a prime of C and assume that the set of elements of C integral at P has a Diophantine definition I over C. Let K be a function field whose constant field is C. We discuss how one can use I to obtain sets of elements of K integral at various primes of K and some consequences of such a construction.

Relative Brauer groups and n-torsion

JACK SONN, HAIFA
(joint work with E. Aljadeff and H. Kisilevsky)

Let K be a field, $\mathrm{Br}(K)$ its Brauer group. If L/K is a field extension, let $\mathrm{Br}(L/K)$ denote the kernel of the restriction map from $\mathrm{Br}(K)$ to $\mathrm{Br}(L)$. If n is a positive integer, let $\mathrm{Br}_n(K)$ denote the n-torsion subgroup of $\mathrm{Br}(K)$. Is it true that $\mathrm{Br}_n(K) = \mathrm{Br}(L/K)$ for some algebraic extension L of K? In general the answer is no, and a counterexample can be given with $n = 2$ and $K = k((t))$ a power series field over a local field k containing the fourth roots of unity. For number fields K no counterexample has been found, and the following positive result has been proved; let K be a number field Galois over the rational field $\mathbb{Q}$ and assume that n is prime to the class number of K. Then there exists an abelian extension (of exponent n) L/K with $\mathrm{Br}_n(K) = \mathrm{Br}(L/K)$. For n odd the hypothesis K Galois over $\mathbb{Q}$ is unnecessary.

Logarithmic van Kampen Theorem and Projective Anabelian Curves in Positive Characteristic

JAKOB STIX, BONN

The Theorem. Let X/K be a smooth, geometrically connected, proper curve over a field K with algebraic closure $\overline{K}/K$, and let $X_{\overline{K}}$ denote the base extension to $\overline{K}$. Its fundamental group has naturally to be considered as an extension

$$1 \to \pi_1(X_{\overline{K}}) \to \pi_1(X) \to G_K \to 1\ ,$$

or as the associated exterior Galois representation $\rho_X : G_K \to \mathrm{Out}(\pi_1(X_{\overline{K}}))$. The two points of view are equivalent in case $\pi_1(X_{\overline{K}})$ is centerfree, i.e., X is of genus $g \geq 2$.

Due to neglecting basepoints π_1 becomes a functor only when considered as such G_K-representations in the category of pro-finite groups with continuous morphisms up to composition with inner automorphisms. The following question arises: To what extent does the $\pi_1(X)$ as described above determine the curve X/K ?

Let K be of characteristic $p > 0$. The relative Frobenius map $F_K : X \to X_{(1)} := X \times_{K,\mathrm{Frob}} K$ is a universal homeomorphism. Hence $\pi_1(F_K)$ is an isomorphism although X may not be isomorphic to its "Frobeniustwist" $X_{(1)}$. Therefore denote a curve iso-trivial iff $X_{\overline{K}}$ is defined over $\overline{\mathbb{F}}_p$. Then the following theorem holds.

Theorem. *Let $K/\mathbb{F}_p$ be finitely generated. Let $X/K, X'/K$ be smooth, geometrically connected, proper curves of genus $g \geq 2$ such that at least one of them is not iso-trivial. Then there is a natural bijection*

$$\pi_1 : \mathrm{Isom}_{K,F_K^{-1}}(X, X') \longrightarrow \mathrm{Isom}_{G_K}\left(\pi_1(X_{\overline{K}}), \pi_1(X'_{\overline{K}})\right) .$$

Here $\mathrm{Isom}_{K,F_K^{-1}}(X, X')$ has to be understood as isomorphisms of schemes over K after formally inverting F_K. Isomorphisms of the G_K-modules are up to composition with inner automorphisms.

This was known in characteristic 0 due to Tamagawa and Mochizuki. Tamagawa also dealt with affine curves over finite fields. For a generalization of the latter see the author's Diplomarbeit which is to appear in *Compositio.*

The use of moduli spaces. Injectivity holds by a result of Serre on automorphisms of abelian varieties and $\pi_1(X_{\overline{K}})^{\mathrm{ab},l} \cong \mathrm{T}_l \, \mathrm{Jac}_X(\overline{K})$. Surjectivity amounts to construct geometric isomorphisms from group theoretical ones.

Consider X/K as a generic fibre of a smooth proper family $\mathscr{X}/S$ where $S/\mathbb{F}_p$ is of finite type. In principle this is described by a representing map $\xi : S \to \mathscr{M}$ of the base into some moduli space. If $\mathscr{M}$ is even a fine moduli space then $\xi = \xi'$ is equivalent to an isomorphism $\mathscr{X} \cong \mathscr{X}'$ over S. We use $\mathscr{M} = \mathscr{M}_g[N]$, the moduli space of smooth, proper, genus g curves endowed with an N-level structure (already around for proving injectivity).

The map ξ is controlled in two steps. We describe group theoretical specialization of π_1 and then use an-abelian geometry over finite fields. The latter holds only up to a Frobenius twist, i.e, ξ is pointwise at closed points only controlled up to composition by a power of Frobenius. The exponent a priori depends on the point. But this does not happen by the following.

Theorem. *Let $S, \mathscr{M}$ be of finite type over $\mathbb{F}_p$, S be irreducible and reduced, and let $\xi, \xi' : S \to \mathscr{M}$ be maps such that $\xi_{top} = \xi'_{top}$, i.e., they coincide on the underlying topological spaces.*

Then ξ and ξ' differ only by a power of the Frobenius map.

Furthermore the finite field case deals only with affine hyperbolic curves. Hence we need to specialize into the π_1^{tame} of an open part of the closed fibres.

Degeneration, log geometry. One of the guiding principles in anabelian geometry is to work equivariantly with covers, i.e., open subgroups, and take quotients. By a theorem of Tamagawa we may therefore assume that for a fixed closed point $s \in S$ (eventually "shrink" S) there is a cover $\mathscr{Y} \to \mathscr{X}$ with non-smooth but stable reduction $\mathscr{Y}_s$ at s.

Stable curves carry a natural log-structure and behave as smooth objects in the log world. Isabelle Vidal has proven a log analogue of specialization. According to a van Kampen theorem for log-schemes the $\pi_1^{\log}$ of the log-geometric special fibre $\mathscr{Y}_{\bar{s}}$ is the fundamental group of a graph of groups (compare Saïdis "Revêtements modérés ...") with π_1^{tame}(components of $\mathscr{Y}_s-$double points) as vertex groups and $\hat{\mathbb{Z}}(1) \times \hat{\mathbb{Z}}(1)/\mathrm{diagonal}(\overline{K})$ as edge groups, such that $G_K^{\mathrm{tame}} = \pi_1^{\log}$(log point) still acts. Together with a group theoretical control of log specialization this allows to control the π_1^{tame} of an open part of $\mathscr{X}_s$ as required.

Galois module structure of $K^\times/K^{\times p}$ for cyclic p-extensions K/F.

John Swallow, Davidson
(joint work with Ján Mináč)

We decompose, for K/F a cyclic p-extension over a field F containing a primitive pth root of unity ξ_p, the pth power class group $J = K^\times/K^{\times p}$:

Theorem. Let $G = \mathrm{Gal}(K/F) = \langle\sigma\rangle$, let $N = 1 + \sigma + \cdots + \sigma^{p-1}$ be the norm. Then as an $\mathbb{F}_p[G]$-module, $J = X \oplus Y \oplus Z$, where

X is indecomposable, of dimension 1 if $\xi_p \in N(K^\times)$, of dimension 2 if $\xi_p \notin N(K^\times)$ and $p \neq 2$, and 0 otherwise;

Y is a free $\mathbb{F}_p[G]$-submodule with $Y^G = N(J)$; and

Z is a trivial $\mathbb{F}_p[G]$-submodule.

The general curve covers $\mathbb{P}^1$ with monodromy group A_n

Helmut Völklein, Gainesville
(joint work with G. Frey and K. Magaard)

Let C be a general curve of genus $g \geq 2$. Then C has a cover to $\mathbb{P}^1$ of degree n iff $2(n-1) \geq g$. If C has a cover to $\mathbb{P}^1$ of degree n then it has such a cover that is *simple*. This is classically known.

Question: Does C admit other types of covers to $\mathbb{P}^1$?

It was shown by Guralnik and various co-authors that if C admits a primitive cover to $\mathbb{P}^1$ of degree n, then its *monodromy group* is S_n or A_n (provided $g \geq 4$). It was not known whether A_n actually occurs. This is answered to the positive in this paper.

Theorem. Let $g \geq 3$. Then C admits a cover to $\mathbb{P}^1$ with monodromy group A_n such that all inertia groups are generated by double transpositions iff $n \geq 2g + 1$.

The Galois group of a function field of one variable over an henselian discretely valued field

Götz Wiesend, Erlangen

Let K be a henselian discretely valued field with residue class field $\bar{K}$. Let $X|K$ be a smooth projective curve with function field F.

The aim is to describe the absolute Galois group G_F of F.

Let $\mathcal{X}$ be a normal, proper, flat model of X over $\mathrm{Spec}(\mathcal{O}_K)$ where $\mathcal{O}_K$ is the valuation ring of K. Let $\bar{X} = \mathcal{X} \times_{\mathcal{O}} \bar{K}$ be the special fibre of $\mathcal{X}$.

Let P run through the closed points of $\bar{X}$: Let $F_P = \mathrm{Quot}(\mathcal{O}^{hen}_{\mathcal{X},P})$, $G_P = G_{F_P} < G_F$.

Let C run through the irreducible components of $\bar{X}$: Let $F_C = \mathrm{Quot}(\mathcal{O}^{hen}_{\mathcal{X},C})$, $G_C = G_{F_C} < G_F$.

Let Z run through the branches of the components C in the points P (Z consists of a point P together with a branch of a component C at P): Let F_Z be the henselisation of F_P at the discrete valuation induced by Z on F_P. F_Z equals the residue field extension of F_C by henselisation of its residue class field $\kappa(C)$ at Z. F_Z is a Henselian valued field with value group $\mathbb{Z} \times \mathbb{Z}$ and residue class field a finite extension of $\bar{K}$. Let G_Z be the absolute Galois group of F_Z.

G_P, G_C, G_Z are defined only up to conjugation in G_F.

Define the following bipartite graph Γ of profinite groups:

Let the vertices be the points P and the components C together with the groups G_P and G_C. Let the edges be the branches Z: Every branch Z gives a point P and a component C. Let these be the endpoints of the edge. Associate to the edge Z the group G_Z.

To complete the definition of the graph of groups Γ one has to give maps $G_Z \to G_P, G_C$. Then one can associate to Γ its fundamental group $\pi_1(\Gamma)$.

Theorem 1. *There are maps $G_Z \to G_P, G_C$ such that*

$$\pi_1(\Gamma) \cong G_F$$

Remark: Since the graph is infinite, to be precise one has to say something about the ramification groups in the definition of $\pi_1(\Gamma)$.

Edited by Walter Hofmann

Participants

Prof. Dr. Pierre Debes
pde@ccr.jussieu.fr
UFR de Mathematiques
Universite Lille I
F-59655 Villeneuve d'Ascq. Cedex

Dr. Michael Dettweiler
michael.dettweiler@iwr.uni-heidelberg.de
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368
69120 Heidelberg

Prof. Dr. Ido Efrat
efrat@math.bgu.ac.il
Dept. of Mathematics
Ben-Gurion University of the Negev
Beer Sheva 84 105 - Israel

Prof. Dr. Yuri L. Ershov
ershov@math.nsc.ru
Institute of Mathematics SO RAN
Akademic Koptyug prospect 4
630090 Novosibirsk 90 - Russia

Prof. Dr. Michael David Fried
mfried@math.uci.edu
Dept. of Mathematics
University of California at Irvine
Irvine, CA 92697-3875 - USA

Prof. Dr. Wulf-Dieter Geyer
geyer@mi.uni-erlangen.de
Mathematisches Institut
Universität Erlangen
Bismarckstr. 1 1/2
91054 Erlangen

Prof. Dr. Dan Haran
haran@post.tau.ac.il
School of Mathematical Sciences
Tel Aviv University
Ramat Aviv
Tel Aviv 69978 - Israel

Prof. Dr. Wolfgang Herfort
herfort@tuwien.ec.at
Institut für Angewandte und
Numerische Mathematik
Technische Universität Wien
Wiedner Hauptstraße 8 - 10
A-1040 Wien

Walter Hofmann
hofmannw@mi.uni-erlangen.de
Mathematisches Institut
Universität Erlangen
Bismarckstr. 1 1/2
91054 Erlangen

Prof. Dr. Moshe Jarden
jarden@post.tau.ac.il
School of Mathematical Sciences
Tel Aviv University
Ramat Aviv
Tel Aviv 69978 - Israel

Prof. Dr. Christian Ulrik Jensen
cujensen@math.ku.dk
Matematisk Afdeling
Kobenhavns Universitet
Universitetsparken 5
DK-2100 Kobenhavn

Dr. Jochen Koenigsmann
Jochen.Koenigsmann@uni-konstanz.de
Fachbereich für Mathematik und
Statistik
Universität Konstanz
78457 Konstanz

Prof. Dr. B. Heinrich Matzat
matzat@iwr.uni-heidelberg.de
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368
69120 Heidelberg

Dr. Peter F. Müller
peter.mueller@iwr.uni-heidelberg.de
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368
69120 Heidelberg

Prof. Dr. Alexander Prestel
Alex.Prestel@uni-konstanz.de
Fachbereich Mathematik u. Statistik
Universität Konstanz
Postfach 5560
78434 Konstanz

Dr. Aharon Razon
razon@exp-math.uni-essen.de
razon@math.tau.ac.il
Dept. of Mathematics
Ben-Gurion University of the Negev
Beer Sheva 84 105 - Israel

Prof. Dr. Luis Ribes
lribes@math.carleton.ca
luis.ribes@uam.es
Departamento de Matematicas
Facultad de Ciencias
Universidad Autonoma de Madrid
E-28049 Madrid

Prof. Dr. Claus Scheiderer
scheiderer@math.uni-duisburg.de
claus@uni-duisburg.de
Fachbereich Mathematik
Universität-GH Duisburg
47048 Duisburg

Prof. Dr. Alexandra Shlapentokh
shlapentokha@mail.ecu.edu
Dept. of Mathematics
East Carolina University
Greenville, NC 27858 - USA

Prof. Dr. Jack Sonn
sonn@math.technion.ac.il
Department of Mathematics
Technion
Israel Institute of Technology
Haifa 32000 - Israel

Jakob Stix
stix@math.uni-bonn.de
Mathematisches Institut
Universität Bonn
Beringstr. 1
53115 Bonn

Prof. Dr. John Swallow
joswallow@davidson.edu
Davidson College
Box 7046
209 Ridge Road
Davidson NC 28035-7046 - USA

Prof. Dr. Helmut Völklein
helmut@math.ufl.edu
Dept. of Mathematics
University of Florida
358 Little Hall
P.O.Box 118105
Gainesville, FL 32611-8105 - USA

Dr. Götz Wiesend
wiesend@mi.uni-erlangen.de
Mathematisches Institut
Universität Erlangen
Bismarckstr. 1 1/2
91054 Erlangen