**16th COLLOQUIUMFEST**

# Arithmetic and Valuation Theory

Heidelberg, 24-25 July, 2015

**Organizers:** Franz-Viktor Kuhlmann, Florian Pop, Alexander Schmidt

## Program

### Friday, July 24:

14:30 - 15:30 **Moshe Jarden** (Tel Aviv)
*Sliceable groups and towers of fields*

15:30 - 16:15 Coffee Break

16:15 - 17:15 **Jakob Stix** (Frankfurt)
*Altes und Neues über die Grothendiecksche Schnittvermutung*

17:30 - 18:30 **Jochen Koenigsmann** (Oxford)
*Fields with the absolute Galois group of* $\mathbb{Q}$

19:30 **Social Dinner**

Dorfschänke, Lutherstr. 14, 69120 Heidelberg-Neuenheim, 06221 41 90 41

### Saturday, July 25:

09:30 - 10:30 **Alexander Prestel** (Konstanz)
*Definable henselian valuation rings*

10:30 - 11:00 Coffee Break

11:00 - 12:00 **Stefan Wewers** (Ulm)
*Lifting automorphisms of curves and differential equations in characteristic p*

12:05 - 12:50 **Franz Lemmermeyer** (Ellwangen)
*Reziprozitätsgesetze*

12:50 - 14:30 **Lunch**

14:30 - 15:30 **Claus Diem** (Leipzig)
*Diskrete Logarithmenprobleme über Erweiterungskörpern*

15:30 - 16:00 Coffee Break

16:00 - 17:00 **Hagen Knaf** (Wiesbaden)
*Lokale Uniformisierung*

# Abstracts

## **Claus Diem**: *Diskrete Logarithmenprobleme über Erweiterungskörpern*

**Zusmmenfassung:** Diskrete Logarithmenprobleme in Familien endlicher Gruppen sind grundlegend für die moderne Kryptographie. Daneben sind sie auch vom komplexitätstheoretischen Gesichtspunkt aus interessant. Von besonderem Interesse sind diskrete Logarithmenprobleme in den multiplikativen Gruppen endlicher Körper und in den Punktgruppen elliptischer Kurven über endlichen Körpern. In beiden Fällen sind in den letzten Jahren Algorithmen für die entsprechenden Probleme über Erweiterungskörpern entwickelt worden, die überraschend performant sind. In dem Vortrag werden diese Algorithmen überblicksartig dargestellt.

## **Moshe Jarden**: *Sliceable groups and towers of fields*

**Abstract**: Recall that a topological group $G$ is called sliceable, if it has finitely many closed subgroups of finite index $H_i$ such that $G = \cup_i H_i^G$. The aim of the talk is to present some recent common work by Sigrid Böge, Alex Lubotzky, and myself concerning sliceable groups which appear in an arithmetical context. Precisely, we show that every division algebra over $\mathbb{Q}_\ell$ is sliceable. To the contrary, for $\ell \neq 2$, the groups $\mathrm{GL}_2(\mathbb{Q}_\ell)$ have no open subgroups which are sliceable, and I will indicate some relations of this fact with Galois theory. Finally, time permitting, I will also comment on the so called infinite sliceability of $\mathrm{GL}_2(\mathbb{Q}_\ell)$.

## **Hagen Knaf**: *Lokale Uniformisierung*

## **Jochen Koenigsmann**: *Fields with the absolute Galois group of* $\mathbb{Q}$

**Abstract**: We shall explain why an arbitrary field $K$ whose absolute Galois group is isomorphic to that of the field $\mathbb{Q}$ of rational numbers shares most of its arithmetic with $\mathbb{Q}$. This relates nicely to the birational Section Conjecture in Grothendieck's Anabelian Geometry.

## **Franz Lemmermeyer**: *Reziprozitätsgesetze*

**Zusammenfassung**: Wer einmal eine Vorlesung in Zahlentheorie besucht hat, kennt das quadratische Reziprozitätsgesetz in der Form, in der es Legendre aufgestellt hat, nämlich $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Die Eulersche Formulierung dieses Gesetzes, nämlich $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ für alle $a \in \mathbb{Z}$, $a \neq 0$, und positive Primzahlen $p \equiv q \pmod 4$ ist dagegen weitgehend unbekannt geblieben. Wir wollen zeigen, dass die Eulersche Formulierung in allen wesentlichen Punkten derjenigen von Legendre deutlich überlegen ist, und werden einen Zugang zum quadratischen Reziprozitätsgesetz skizzieren, der die Analogie zu Entwicklungen in der modernen Zahlentheorie sichtbar werden lässt.

## **Alexander Prestel**: *Definable henselian valuation rings*

**Abstract**: A valuation ring $A$ of a field $K$ is usually called definable in $K$, if there exists a first order formula in the ring language that applies to exactly the elements of $A$. Our talk will report about the existence, uniformity and quantifier complexity of such formulas in the case where $A$ is henselian. The methods of proof will be partly of model theoretic and partly of algebraic nature.

**Jakob Stix**: *Altes und Neues über die Grothendiecksche Schnittvermutung*

**Zusammenfassung**: Die Schnittvermutung aus Grothendiecks Brief an Faltings aus dem Jahre 1983 schlägt vor, rationale Punkte hyperbolischer Kurven über Zahlkörpern durch Galoistheorie zu beschreiben, und zwar als Schnitte der Fundamentalgruppensequenz. Auch über 30 Jahre nach ihrer Formulierung ist diese Vermutung offen und nur in wenigen Fällen von speziellen Kurven, alle ohne rationale Punkte, bekannt. Im Votrag soll ein Überblick über Ergebnisse und offene Fragen im Zusammenhang mit der Schnittvermutung gegeben werden.

**Abstract**: The section conjecture posed in a letter of Grothendieck to Faltings in 1983, asserts that the rational points of a hyperbolic complete over a number field are in bijection with the (conjugacy classes of) sections of the fundamental group exact sequence. The section conjecture is essentially open, and the situation is well understood only in a few special cases. In this talk I will give an overview of old and new results on the section conjecture.

**Stefan Wewers**: *Lifting automorphisms of curves and differential equations in characteristic p*

**Abstract**: In positive characteristic the automorphism group of a curve may violate the Hurwitz bound. Such examples give a negative answer to the general form of the *lifting problem* (for automorphism groups of curves). It is an interesting and difficult problem to characterize exactly the automorphism groups in characteristic p which do lift. In my talk I will discuss one specific aspect of this problem which came up in the proof of the Oort conjecture by Obus, Pop and myself.