The Mathematical Work of Helmut Koch

Kay Wingberg, Berlin October 2012

Talk on the occasion of Helmut Koch's 80th birthday

Local Algebraic Number Theory

- Primitive representations of the Galois group of a local field (Henniart, Koch, E.-W. Zink)
- Local Langlands conjecture, representations of the multiplicative group of divisions algebras (Henniart, Koch, E.-W. Zink)

Local Algebraic Number Theory

- Primitive representations of the Galois group of a local field (Henniart, Koch, E.-W. Zink)
- Local Langlands conjecture, representations of the multiplicative group of divisions algebras (Henniart, Koch, E.-W. Zink)
- Meta-abelian local class field theory (de Shalit, Koch, Kukkuk, Labute)

Local Algebraic Number Theory

- Primitive representations of the Galois group of a local field (Henniart, Koch, E.-W. Zink)
- Local Langlands conjecture, representations of the multiplicative group of divisions algebras (Henniart, Koch, E.-W. Zink)
- Meta-abelian local class field theory (de Shalit, Koch, Kukkuk, Labute)
- Structure of the absolute Galois group of $\mathfrak{p}$-adic fields (Koch)

Local Algebraic Number Theory

- Primitive representations of the Galois group of a local field (Henniart, Koch, E.-W. Zink)
- Local Langlands conjecture, representations of the multiplicative group of divisions algebras (Henniart, Koch, E.-W. Zink)
- Meta-abelian local class field theory (de Shalit, Koch, Kukkuk, Labute)
- Structure of the absolute Galois group of $\mathfrak{p}$-adic fields (Koch)

Über Galoissche Gruppen von $\mathfrak{p}$-adischen Zahlkörpern
Math. Nachr. 29 (1965) 77-111

The Galois Group of a p-closed extension of a local field
Dolk. Akad. Nauk SSSR 238 (1978) 10-13

Global Theory: Class Field Towers

k a number field, p a prime number,

$$H_\infty(p) = \bigcup_n H_n(p)$$

is the p-class field tower of k, where $H_{n+1}(p)$ is the maximal unramified abelian p-extension of $H_n(p)$, $H_0(p) = k$.
Question: Is the pro-p group

$$G_\varnothing(k)(p) = Gal(H_\infty(p)|k)$$

finite or infinite? Answered 1964 by E.S.Golod and I.R.Šafarevič by a purely group-theoretical result. This result was improved by W.Gaschütz and E.B.Vinberg:

Theorem (Ga/V 1965): *Let G be a finite p-group,*

$$\begin{array}{lll} h_1(G) & \textit{the minimal generator rank of } G & = \dim_{\mathbb{F}_p} H^1(G, \mathbb{Z}/p\mathbb{Z})\,, \\ h_2(G) & \textit{the minimal relation rank of } G & = \dim_{\mathbb{F}_p} H^2(G, \mathbb{Z}/p\mathbb{Z})\,, \end{array}$$

then we have the inequality

$$h_2(G) > \frac{h_1(G)^2}{4}\,.$$

Result is sharp: there exists a family of finite p-groups such that the quotient of the right side by the left side of the inequality converges to 1 (A.J.Kostrikin (1964), H.Koch (1975), J. Wisliceny (1979)).

Refinement by Koch: Let G_n be the Zassenhaus filtration of a pro-p group G.

Theorem (Koch 1969): *Let*

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

be a minimal representation of the finite p-group G by a free pro-p group F with "relations" R such that $R \subseteq F_m$. Then

$$h_2(G) > \frac{h_1(G)^m}{m^m}(m-1)^{m-1} .$$

This means: the complicated the relations are the more have to exist if the group is finite.

1. Application in Number Theory: Unramified extensions.

Theorem: *Let $k|\mathbb{Q}$ be a quadratic field such that at least*

8 prime numbers are ramified, if k is real, or
6 prime numbers are ramified, if k is imaginary,

then $G_\varnothing(k)(2)$ is infinite.

This follows by the (Ga/V)-inequality. The refinement of Koch gives much more:

Theorem (Koch/Venkov 1975): *Let p be odd and $k|\mathbb{Q}$ a quadratic field such that the p-rank of the class group $Cl(k)$ is at least 3,*

$$h_1(G_\varnothing(k)(p)) = \dim_{\mathbb{F}_p} Cl(k)/p \geq 3\,,$$

then $G_\varnothing(k)(p)$ is infinite.

2. The Geometric Class Field Tower Problem.

Serre (1966) and Koch (1969) realized that the Golod/Šafarevič inequality and Koch's refinement also hold for finitely generated p-adic analytic pro-p groups G, i.e.

$$G \hookrightarrow Gl_n(\mathbb{Q}_p)\,.$$

Therefore the Galois group $G_\varnothing(k)(p)$ is i. g. infinite but not p-adic analytic. A consequence of the **Fontaine-Mazur Conjecture**, which postulates a very general geometric principle, is the following conjecture:

Geometric class field tower conjecture: *Let $K|k$ be a tamely ramified Galois p-extension such that $Gal(K|k)$ is a p-adic analytic group, then $K|k$ is finite.*

Global Theory: Restricted Ramification, Wild Case

We consider the Galois group

$$G_S(k)(p) = Gal(k_S(p)|k),$$

where $k_S(p)$ is the maximal p-extension of k which is unramified outside the finite set of primes S. The case where the set S_p of primes above p is contained in S is called the “wild” case.

For an arbitrary finite set of primes S Šafarevič and Koch showed:

Theorem: *For the generator- and relation-rank the following holds:*

$$h_1(G_S(k)(p)) = \sum_{\mathfrak{p}\in S\setminus S_{\mathbb{C}}} \delta_{\mathfrak{p}} - \delta + 1 + \dim_{\mathbb{F}_p} Б_S(k) + \sum_{\mathfrak{p}\in S\cap S_p} n_{\mathfrak{p}} - r\,,$$

$$h_2(G_S(k)(p)) \leq \sum_{\mathfrak{p}\in S\setminus S_{\mathbb{C}}} \delta_{\mathfrak{p}} - \delta + \dim_{\mathbb{F}_p} Б_S(k) + \theta\,,$$

where $n_{\mathfrak{p}} = [k_{\mathfrak{p}} : \mathbb{Q}_{\mathfrak{p}}]$ *is the local degree with respect to* $\mathfrak{p}$ *and* $r = r_1 + r_2$ *the number of archimedean primes,* $\theta \in \{0, 1\}$, $Б_S(k)$ *is a finite obstruction group and*

$$\delta = \begin{cases} 1, & \mu_p \subseteq k, \\ 0, & \mu_p \not\subseteq k, \end{cases} \qquad \text{and} \qquad \delta_{\mathfrak{p}} = \begin{cases} 1, & \mu_p \subseteq k_{\mathfrak{p}}, \\ 0, & \mu_p \not\subseteq k_{\mathfrak{p}}. \end{cases}$$

Here μ_p *is the group of the p-th roots of unity.*

If $S_p \cup S_\infty \subseteq S$ (and k totally imaginary, if $p = 2$), then we have for the cohomological dimension

$$\mathrm{cd}_p\, G_S(k)(p) \leq 2.$$

In Koch's book "Galois Theory of p-Extensions" is a section with the title: "The Structure of $G_S(p)$ in Special Cases". Here one can find a description of the so-called "degenerated case" for the structure of the group $G_S(p)$. Later it was shown that in the "generic case" $G_S(p)$ is a **duality group**.

Theorem: *Let $S_p \cup S_\infty \subseteq S$ (and $p \neq 2$, $\mu_p \subseteq k$). Then $G_S(k)(p)$ has one of the following forms:*

(i) *If the obstruction groups $Б^S_{\{v\}} \neq 0$ for all finite primes $v \in S$, then $G_S(k)(p)$ is a duality group of dimension 2 ("generic case"), i.e. for all $i \in \mathbb{Z}$ and all finite $G_S(p)$-modules A there are canonical isomorphisms*

$$H^i(G_S(p), \mathrm{Hom}(A, I)) \cong H^{2-i}(G_S(p), A)^*.$$

Here I is dualizing module of $G_S(p)$.

(ii) *If $Б^S_{\{v_0\}} = 0$ for a finite prime $v_0 \in S$, then $G_S(k)(p)$ is a free pro-p product of decomposition groups $\mathcal{G}_v$ and a free pro-p group F ("degenerated case"):*

$$\mathop{\ast}_{v \in S \setminus \{v_0\}} \mathcal{G}_v \ast F \xrightarrow{\sim} G_S(k)(p).$$

Global Theory: Restricted Ramification, Tame Case

Again we consider the pro-p group $G_S(k)(p) = Gal(k_S(p)|k)$, where now

$$S \cap S_p = \varnothing.$$

By the theorem of Golod/Šafarevič and the refinement of Koch we get the following result for $k = \mathbb{Q}$ (there are similar results for arbitrary number fields k):

Theorem (Šafarevič 1964, Koch 1969): *Let $p \neq 2$.*

Then the group $G_S(\mathbb{Q})(p)$ is infinite, if $\#S \geq 4$.

If $\#S \leq 3$, then $G_S(\mathbb{Q})(p)$ can be infinite or finite.

Nothing was known concerning the cohomological dimension of $G_S(k)(p)$ (if it is infinite) for a long time. But 2006 John Labute introduced:

$$\textbf{mild} \quad \text{pro-}p \text{ groups,}$$

i.e. groups having a suitable representation by generators and relations. These groups have cohomological dimension 2 ("mildness" was first introduced by D.Anick for discrete groups). A special case are pro-p groups G, which Labute called *groups of Koch-Typ*, with additional properties:
G has a minimal representation by generators $x_1, \dots, x_d$ and relations $w_1, \dots, w_r$ such that $r \le d$ and the relations are of the form

$$w_i \equiv x_i^{p\,a_i} \prod_{i \neq j} [x_i, x_j]^{a_{ij}} \mod F_3$$

where $a_i, a_{ij} \in \mathbb{Z}$ (the "linking numbers").

If $k = \mathbb{Q}$, then $G(\mathbb{Q}_S(p)|\mathbb{Q})$, $S \cap S_p = \varnothing$, is of Koch-Typ (Koch 1970). More general: Arithmetically Koch-groups are Galois groups having only local relations.

The additional properties are condition for the so-called "linking diagram" of the "linking numbers".
Alexander Schmidt generalized Labute's results:

Theorem (Schmidt 2010): *Let p be odd and S a finite set of primes of the number field k. Then there exists a finite set of primes S_0 disjoint to $S \cup S_p$, such that $G_{S \cup S_0}(k)(p)$ has cohomological dimension 2.*

Important for the proof is the following

Theorem (Labute/Minac, Schmidt 2007): *Let p be odd and G a finitely generated pro-p group with $H^2(G, \mathbb{Z}/p\mathbb{Z}) \neq 0$. Assume that there is a decomposition of $H^1(G, \mathbb{Z}/p\mathbb{Z})$ of the form*

$$H^1(G, \mathbb{Z}/p\mathbb{Z}) = U \oplus V$$

as $\mathbb{F}_p$-vector space such:

(i) The cupproduct $V \otimes V \xrightarrow{\cup} H^2(G, \mathbb{Z}/p\mathbb{Z})$ is trivial.

(ii) The cupproduct $U \otimes V \xrightarrow{\cup} H^2(G, \mathbb{Z}/p\mathbb{Z})$ is surjective.

Then $\mathrm{cd}_p G = 2$.

The situation became more complicated if the cupproduct

$$H^1(G,\mathbb{Z}/p\mathbb{Z}) \otimes H^1(G,\mathbb{Z}/p\mathbb{Z}) \xrightarrow{\cup} H^2(G,\mathbb{Z}/p\mathbb{Z})$$

is trivial, i.e. the relations of G "started with 3-commutators or higher" (besides the p-powers). Therefore one has to consider

higher Massey products

(as Koch already mentioned 1978 (or earlier ?)). Morishita (2004), Vogel (2004) and Gärtner(2011) proved analogous results as above.

Theorem (Gärtner 2011): *Let p be odd and G a finitely generated pro-p group with $H^2(G,\mathbb{Z}/p\mathbb{Z}) \neq 0$,*

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

a minimal representation of G by a free pro-p group F with relations R such that $R \subseteq F_h$ and $R \nsubseteq F_{h+1}$, , $h < \infty$ (G has "Zassenhaus invariant" h).
Assume that there is a decomposition of $H^1(G,\mathbb{Z}/p\mathbb{Z})$ of the form

$$H^1(G,\mathbb{Z}/p\mathbb{Z}) = U \oplus V$$

such that for some $1 \leq e \leq h-1$:

(i) The Massey-product $<\xi_1,\dots,\xi_h>= 0$ if at least $h-e+1$ of the ξ_i's lie in V.

(ii) The Massey-product $U^{\otimes e} \otimes V^{\otimes h-e} \xrightarrow{\cup} H^2(G,\mathbb{Z}/p\mathbb{Z})$ is surjective.

Then G is mild and so $\mathrm{cd}_p G = 2$ (if $h = 2$, then this is the result of Labute/Minac-Schmidt).

In particular, there exist mild pro-p groups of the form $G_S(k)(p)$ having trivial cupproduct: for $p = 2$ Massey products can be related to Rédei-symbols (Rédei 1938), which can be calculated.

History of Mathematics, Books on Number Theory

Historical works: Euler, Dirichlet

Books on number theory:

Galois Theory of p-Extensions (1970)

Introduction to Classical Mathematics I (1986)
(where are II, III,... ?)

Number Theory (Encyclopaedia of Math. Sciences) (1991)

Number Theory (1997)

Waiting for the 90-th birthday