MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 34/1990

Algebraische Zahlentheorie

12.08. bis 18.08.1990

Die Tagung fand statt unter der Leitung von Herrn Prof. W. Jehne (Köln), Herrn Prof. H.-W. Leopoldt (Karlsruhe) und Herrn Prof. P. Roquette (Heidelberg).
Die Vorträge gaben Auskunft über den Stand der Forschung zu einer Reihe von klassischen zahlentheoretischen Problemen. Außerdem wurde über neuere Entwicklungen in Verbindung mit der arithmetischen Geometrie, der konstruktiven Zahlentheorie und der Modelltheorie berichtet.
Zwei Vorträge waren besonderen Aspekten der Geschichte der algebraischen Zahlentheorie gewidmet.

Vortragsauszüge

H. Koch (Berlin-Ost)

Even unimodular, positive-definite lattices of rank $p+1$, whose group of isometries contains an element of order p and the relative class number h^- of the p-th cyclotomic field

Let p be a prime. By J. Thompson a lattice L with the properties above, in particular with the isometry Π of order p is determind by its sublattices L^{Π} and its orthogonal complement L^-. L^{Π} is of rank two and discriminant p, L^- is of rank $p-1$ and discriminant p and is isometric to the lattice $L(\mathfrak{a},\gamma)$, where $\mathfrak{a}$ is an ideal in $k = \mathbb{Q}(\zeta)$, $\zeta = e^{2\pi i/p}$ such that the norm $N\mathfrak{a}$ of k to its maximal real subfield k_0 is a principal ideal of k_0 generated by the totally positive number $\gamma \in k_0$. The bilinear form of $L(\mathfrak{a},\gamma)$ is given by $(\alpha,\beta) = \mathrm{Tr}_{k/\mathbb{Q}}\, \alpha\delta\beta^{\iota}$, $\alpha, \beta \in \mathfrak{a}$, where ι denotes complex conjugation and $\delta = \gamma\,(N\lambda)^{(p-3)/2}$, $\lambda = 1-\zeta$. In the talk it is shown that the isometry classes of lattices of type $L(\mathfrak{a},\gamma)$ are in one to one correspondence to the $\mathrm{Gal}(k/\mathbb{Q})$-orbits of $\mathrm{Cl}(k)/\mathrm{Cl}(k_0)$.

S. Böge (Heidelberg)

Witt-Invariante und ein gewisses Einbettungsproblem

Es wird der folgende Satz bewiesen:
Sei $L/\mathbb{Q}$ eine galoissche Erweiterung mit Galoisgruppe $\mathrm{PSL}(2,\ell)$, wobei ℓ eine Primzahl $\equiv 3$ oder $5 \bmod 8$ ist. Genau dann läßt sich L in eine Erweiterung mit Galoisgruppe $\mathrm{SL}(2,\ell)$ über $\mathbb{Q}$ einbetten, wenn

1. L total reell ist und
2. für jede ungerade Primzahl p mit gerader Verzweigungsordnung gilt: p hat ungeraden Restklassengrad genau dann, wenn $p \equiv 1 \bmod 4$.

[für $\ell = 3$ besagt dies dasselbe wie ein Satz von Kolvenbach.] Der Beweis beruht auf

(1) dem Kriterium von Serre
(2) expliziter Berechnung der Witt-Invarianten von Spurformen nicht dyadischer Körper und
(3) genauer Betrachtung der Möglichkeiten für Verzweigungsgruppen, wenn $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{PSL}(2,\ell)$.

K. Miyake (Nagoya)

On the capitulation problem

Recently the mathematican H. Suzuki succeeded in giving a proof to the following theorem:

Theorem. Let k be an algebraic number field of finite degree and K be an unramified abelian extension of k . Then at least [K:k] ideal classes of k become principal in K .
In case that K/k is cyclic of prime degree, we have Hilbert's theorem 94 in his celebrated Zahlbericht. We also have the principal ideal theorem when K is Hilbert's class field of k . The content of the present theorem has been confirmed in various cases namely, in case that K/k is cyclic in general and also in those cases which Terada's principal ideal theorem is capable to cover; however it has also been aware of, by group theoretic examples, that all cases can not be covered by these known cases.
It should also be noted that Suzuki's proof of the theorem consists of careful analysis of group rings of finite abelian groups; we may say that it is elementary.

O. Neumann (Jena)

Über die Frühgeschichte der Theorie der "idealen Zahlen"

Erst in den letzten 15-20 Jahren wurde man darauf aufmerksam, daß es in verschiedenen Archiven (insbesondere im Zentralen Archiv der Berliner Akademie der Wissenschaften) Primärquellen gibt, die eine revidierte Darstellung der Frühgeschichte der Theorie der "idealen Zahlen" erfordern. Im Vortrag wurde die These begründet, daß der Hauptanstoß zu Kummers Schöpfung der "idealen Zahlen" im Ausbau der Kreisteilungstheorie (Gauß-Jacobi-Summen), in der Suche nach den höheren Reziprozitätsgesetzen und insbesondere in der Theorie der Zerlegung der Primzahlen $p \equiv 1 \pmod{\lambda}$, wobei λ eine feste ungerade Primzahl ist; im Ring $\mathbb{Z}[\sqrt[\lambda]{1}]$ zu suchen ist. Eine herausgehobene Rolle der Fermat-Vermutung läßt sich nicht überzeugend belegen. - Der Vortragende teilte mit, daß es im Deutschen Museum in München 53 Briefe von E.E. Kummer (1810- 1893) an den Stuttgarter Gymnasialprofessor C.G. Reuschle (1812-1875) und 8 Briefe von Reuschle an Kummer gibt.

R. Schertz (Augsburg)

Galoismodulstruktur und elliptische Funktionen

Sei K ein imaginär-quadratischer Zahlkörper. Ist f ein ganzes Ideal in K, so bezeichnet K(f) den Strahlklassenkörper modulo f über K . Betrachtet man Erweiterungen vom Typ N/M , $N = K(\mathfrak{l}\mathfrak{g})$, $M = K(\mathfrak{l}\mathfrak{g}^*)$, $\mathfrak{g}^* | \mathfrak{g} | \mathfrak{g}^{*2}$, $\mathfrak{l} \in \mathbb{N}$, mit einem ganzen zu $\mathfrak{l}$ teilerfremden Ideal $\mathfrak{g}$, so kann man unter geeigneten Voraussetzungen zeigen, daß die Hauptordnung von N ein freier Modul vom Rang 1 über der zur Erweiterung N/M assoziierten Ordnung $\mathcal{A}_{N/M}$ im Gruppenring von Gal(N/M) über M ist:

(1) $$\mathcal{O}_N = \Theta \mathcal{A}_{N/M} .$$

Das galoiserzeugende Element Θ und $\mathcal{A}_{N/M}$ werden dabei mit Hilfe elliptischer Funktionen konstruiert. Eine Erzeugung der Form (1) hat man zum Beispiel

stets, wenn ℓ eine in K zerlegte Primzahl ist. Auch im Fall $\ell = 1$ ist (1) gültig, wenn man über g noch zusätzliche Voraussetzungen macht.

H. Opolka (Braunschweig)

Teilungspunkte elliptischer Kurven und Galoisdarstellungen

Der Vortrag beschäftigt sich mit der Charakterisierung von Zahlkörpererweiterungen, die durch Adjunktion von Teilungspunkten rationaler Punkte elliptischer Kurven entstehen, durch holomorphe oder cuspidale Galoisdarstellungen. Genauer: Sei k ein Zahlkörper, dessen cyclotomische Erweiterungen die Leopoldt-Vermutung für alle Primzahlen erfüllen. Sei X eine über k definierte elliptische Kurve, so daß alle Elemente von $\partial = \mathrm{End}(X)$ über k definiert sind, sei $\Gamma \leq X(k)$ ein freier ∂ - Modul vom Rang r und sei ℓ eine Primzahl, so daß das Paar (Γ,ℓ) zulässig ist. (Die Definition des Begriffes "zulässig" ist kompliziert, aber die Eigenschaft "zulässig" ist für "hinreichend großes ℓ " stets erfüllt.) Dann definiert (Γ,ℓ) zusammen mit einer eigentlichen Lösung Φ einer Folge von zentralen Einbettungsproblemen, die durch die Weil-Paarung definiert sind, eine Folge von irreduziblen komplexen Darstellungen $R = R(\Gamma,\ell,\Phi) = (R_1,R_2,\ldots)$ mit den folgenden Eigenschaften:

(a) Alle R_n sind außerhalb aller über ℓ und ∞ liegenden Stellen von k und aller schlechten Reduktionsstellen von k unverzweigt.

(b) $\mathrm{Grad}(R_n) = \ell^{(r+1)n-1}(\ell - 1)$.

(c) $R_n = \mathrm{Ind}_{k(\mu_{\ell^n})}^{k}(D_n)$ eine irreduzible Darstellung von $G_{k(\mu_{\ell^n})}$ mit projektiver Kernkörpererweiterung $\overline{k}^{\mathrm{Ker}(\overline{D}_n)}/k = k(\frac{1}{\ell^n}\Gamma)/k(\mu_{\ell^n})$ ist.

(d) Wenn n gerade ist, dann ist R_n monomial, also holomorph.

(e) Die R_n mit dem ungeraden Index n sind i.a. nicht monomial.

(f) R_n ist durch R_{n+1} eindeutig bestimmt.

(g) Die R_n mit geradem Index n sind für $\ell = 3$ oder in dem Fall, daß X komplexe Multiplikation besitzt, cuspidal.

Beispiel: $X/\mathbb{Q} : y^2 + y = x^3 - x$, $P := (0,0) \in X(\mathbb{Q})$, $\Gamma = \langle P \rangle$, $\ell = 3$.

T. Metsänkylä (Turku)

Computation of the zeros of p - adic L - functions

In a joint work with R. Ernwall T. Metsänkylä has computed the zeroes of the Leopoldt-Kubota p - adic L - functions $L_p(s,\chi)$ for some small primes p and for a number of Dirichlet characters χ . The zeros of the corresponding Iwasawa

power series $f_\Theta(T)$ were also computed. The characters χ (associated to quadratic extensions of the p - th cyclotomic field) were chosen so as to cover as many different splitting types of the $f_\Theta(T)$ as possible. The λ - invariant of this power series, equal to its number of zeros, assumed values up to 8 . - The talk was a report on these computations and their results.

B.W. Matzat (Heidelberg)

Frattini-Einbettungsprobleme über Hilbertkörpern

Jedes Einbettungsproblem über einem Hilbertkörper kann zerlegt werden in ein Frattini-Einbettungsproblem gefolgt von einem zerfallenden Einbettungsproblem. In dem Vortrag wurde eine leicht nachprüfbare hinreichende Bedingung für die Lösbarkeit regulärer Frattini-Einbettungsprobleme vorgestellt. Der resultierende Satz enthält Einbettungssätze von Feit und Völklein als Spezialfälle. Anwendungsbeispiele sind u.a. Realisierungen über $Q(t)$ von z.B. $2 \cdot A_n$ (Mestre/Völklein), $3 \cdot G$ für G ($\neq J_3$) sporadisch (Feit), $3 \cdot PSL_3(p)$ für $p \equiv 5 \bmod 12$ (Malle), $2^2 \cdot PSL_3(4)$ ...

G. Malle (Heidelberg)

Disconnected groups of Lie type as Galois groups

Two years ago G. Malle gave a talk at Oberwolfach about the realization of exceptional groups of Lie type as Galois groups over abelian number fields. The constructions relied on the Rationality Criterion of Matzat and Thompson. One of the cases which could not be handled were the groups $E_6(q)$, $q \equiv 1 \pmod 3$. Here he shows that the right approach for those groups is to consider the extenion $E_6(q)_{sc}.2$ by the graph automorphism. To verify the rationality criterion, some information on character values in the disconnected groups $E_6(q)_{sc}.2$ is needed. This can be obtained by studying the Hecke algebra of the permutation character on the Borel subgroup, generalizing well known results in the connected case. In particular, the Howlett-Lehrer comparison theorem for multiplicities in induced characters can be shown to hold in that case as well. Combining this with some more calculations, using Ree's theorem, it can be proved that $E_6(q)_{sc}.2$, $E_6(q)_{sc}$, $E_6(q).2$ and $E_6(q)$ for $q = p^n$, $p \neq 2$, are Galois groups over Q^{ab}. For all $q = p$ that are primitive roots mod 19, the above groups even occur as Galois groups over Q .

M. Jarden (Tel Aviv)

Intersection of local fields

Consider a countable Hilbertian field K . Denote its absolute Galois group by G(K) . Let E_i be a local algebraic extension of K , where "local" means that E_i is Henselian or real closed, i = 1 ,..., m . Let e be a nonnegative integer und equip $G(K)^{m+e}$ with the Haar measure.

Free product theorem: For almost all $(\sigma,\tau) \in G(K)^{m+e}$

$$\langle G(E_1)^{\sigma_1}, \dots, G(E_m)^{\sigma_1}, \tau_1, \dots, \tau_e \rangle \cong \prod_{i=1}^{m} G(E_i) * \langle \tau_1, \dots, \tau_e \rangle .$$

Here $*$ denotes the free product in the category of profinite groups.

The case $K = \mathbb{Q}$, $m = 0$, $e = 1$ is due to Ax (Annals of Math. 1968).

The case $m = 0$ is due to Jarden (Israel J. 1974).

The case $e = 0$ and E_i is Henselization of K with respect to a valuation of rank 1, or a real closed field with an archimedean ordering, is due to Geyer (Israel J. 1978). Let v_i be a valuation (resp. ordering) of K induced by E_i. Then

a) $v_i = v_j$ in which case E_i is conjugate to E_j; or v_i is independent of v_j where we can use the weak approximation theorem.

b) K is v_i - dense in E_i.

Geyer constructs polynomials $f_i \in E_i[X]$, $i = 1, \dots, m$ and approximate them simultaneously by polynomials in $K[X]$. In the general case (a) and (b) above do not hold, and therefore the approximation is impossible. The main new idea in the proof of the general free product theorem is to construct f_i such that they are all equal to a polynomial $f \in K[X]$. Then it is possible to use an "approximation of zero" theorem for Hilbert sets over K, and approximate f simultaneouesly with respect to $v_1, \dots, v_m$ without any restrictions on them.

D. Haran (Tel Aviv)

On virtually projective fields

A profinite group G is (real) projective if it is a closed subgroup of (a free product of copies of $\mathbb{Z}/2\mathbb{Z}$ with) a free profinite group.

Main result. Let K be a field such that its absolute Galois group G has an open projective subgroup G'. Then G is real projective.

In case that G is torsion free, G is projective (and hence real projective). This is the content of Serre's theorem (Topology 3 (1965) 413-42). The proof of this theorem is based on Galois cohomology.

Haran's main result seems to be of similar nature. To obtain an appropriate analogue of the proof, he first introduces a new cohomology theory for the pairs $G = (G, \mathrm{Inv}(G))$. It has the property: $\mathrm{cd}_p G \leq 1$ for all primes p if and only if G is real projective. Incidentally, if K is an algebraic extension of rationals then $\mathrm{cd}_p G \leq 2$ for all primes p.

He then shows that $\mathrm{cd}_p G' < \infty$ implies that $\mathrm{cd}_p G < \infty$. From this the main result follows easily, since the new cohomology theory has properties analogous to the Galois cohomology.

E.W. Zink (Berlin)

Darstellungstheorie lokaler Divisionsalgebren

Sei $F/\mathbb{Q}_p$ ein p - adischer Zahlkörper und D/F eine zentrale Divisionsalgebra vom Index n . Beschrieben werden die irreduziblen komplexen Darstellungen der multiplikativen Gruppe D^* . Der Formalismus der Darstellungsfilter, angewendet auf die Normalteilerreihe $D^* \supset U \supset U^1 \supset U^2 \supset \ldots$ der Einheiten und Einseinheiten in D , reduziert das Problem auf die Bestimmung von "zulässigen Paaren" (J,π) , bestehend aus einer Untergruppe $J \subset D^*$ und einer irreduziblen Darstellung $\pi \in \hat{J}$. Die zulässigen Paare sind kanonische Objekte. Durch Induktion erhält man aus ihnen sämtliche irreduziblen Darstellungen von D^* , und zwei Paare führen auf dieselbe Darstellung genau dann, wenn sie konjugiert sind. Die Gruppen J, welche in den Paaren auftreten, erhält man in der Form $J = J_\beta$ mit $\beta \in D/O$, wobei O der Bewertungsring in D ist, d.h. man hat ein kanonisches Verfahren, um zu jeder Restklasse β eine Gruppe J_β und darüber hinaus eine Untergruppe $H^1_\beta \subset J^1_\beta := J_\beta \cap U^1$ zu definieren, Zu bestimmen sind dann noch die in den zulässigen Paaren auftretenden Darstellungen π , und das läßt sich auf die Konstruktion geeigneter Charaktere $\Theta_\beta : H^1_\beta \to \mathbb{C}^*$ zu jedem $\beta \in D/O$ reduzieren. Im Gegensatz zu H^1_β ist es nicht möglich, der Restklasse β das Θ_β kanonisch zuzuordnen, Kanonisch (nämlich über die Selbstdualität von D^+) gehört zu β ein additiver Charakter ψ_β des Primideals $\mathfrak{P}$ von D , und jede Wahl von $\beta \mapsto \Theta_\beta$ mit der Eigenschaft

$$\beta' \equiv \beta \bmod \mathfrak{P}^{-r} \ (r \geq 1) \quad \text{impliziert} \quad (\Theta_{\beta'} \cdot \Theta_\beta^{-1})(1+y) = \psi_{\beta'-\beta}(y)$$

$$\text{für} \quad 1 + y \in H^1_\beta \cap U^{[r/2]+1} = H^1_{\beta'} \cap U^{[r/2]+1}$$

leistet das Verlangte.

E. Kani (Kingston)

Kurven vom Geschlecht 2 mit elliptischen Differentialen

Es wurden diejenigen Funktionenkörper F|K (algebraisch abgeschlossen) vom Geschlecht 2 konstruiert bzw. klassifiziert, die einen maximal elliptischen Teilkörper (m.e.T.) $F_1 \subset F$ vom Index $N = [F:F_1]$ mit $\mathrm{char}(K) \nmid N$ enthalten. Diese Konstruktion wurde in einer gemeinsamen Arbeit mit G. Frey benutzt, um die Höhenvermutung für elliptische Kurven zu untersuchen; (siehe den nächsten Vortrag).

Hier wurden hauptsächlich Modulprobleme solcher Kurven studiert. Sei dazu $\mathfrak{M}_2^{ell}(N) = \{$ Isomorphieklassen solcher Paare $(F,F_1)\}$. Dann gilt:

Satz 1. $\mathfrak{M}_2^{ell}(N)$ ist durch eine affine, normale, irreduzible Fläche $M_2^{ell}(N)$ repräsentierbar. Genauer ist $M_2^{ell}(N)$ eine offene Untervarietät von $B_{1,1} := (X(N) \times X(N)) / \Gamma_N$, wobei X(N) die affine Modulkurve (der Stufe - N - Struktur) und $\Gamma_N = \{(g, wgw^{-1}) : g \in G\} \subset G \times G$,mit $G = Sl_2(\mathbb{Z}/N\mathbb{Z}) / (\pm 1)$, $w = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ bezeichnet.

Satz 2. Die Vergißabbildung $\mathfrak{M}_2^{ell}(N) \to \mathfrak{M}_2$ (= Isokl. von Fkp. vom Geschlecht 2) wird durch einen endlichen Morphismus $f_N : M_2^{ell}(N) \to M_2$ repräsentiert, der über die kanonische Involution τ_N auf $M_2^{ell}(N)$ (und $B_{1,1}(N)$) faktorisiert. Ferner ist die induzierte Abbildung

$$\bar{f}_N : \bar{M}_2^{ell}(N) := M_2^{ell}(N)/\tau_N \to \bar{M}_2^{ell}(N)^* := f_N(M_2^{ell}(N)) \subset M_2$$

birational, und daher ist $\bar{f}_N$ die Normalisierung von $\bar{M}_2^{ell}(N)^*$.

Satz 1 besagt, daß jedes Paar (F,F_1) wie oben durch ein Tripel (E_1, E_2, ψ) beschrieben wird, wobei E_1, E_2 elliptische Kurven sind und $\psi : E_1[N] \xrightarrow{\sim} E_2[N]$ eine Anti-Isometrie ist; wir nennen dann (E_1, E_2, N) den Typ von (F,F_1). Sei nun zu vorgegebenen (E_1, E_2, ψ):

$$n(E_1, E_2, N) := \#\{(F,F_1) : (F,F_1) \text{ besitzt Typ } (E_1, E_2, N)\}$$

(mit Vielfachheiten gezählt). Es gilt dann der folgende Existenzsatz:

Satz 3. Man hat $\frac{1}{2} N^3 > n(E_1, E_2, N) > \frac{1}{20} N^3$, außer wenn E_1 und E_2 supersingulär sind und $j(E_1), j(E_2) \in \{0, 1728\}$. Es gibt daher, bis auf diese Ausnahmefälle, stets Kurven mit elliptischen Differentialen von vorgegebenem Typ.

Dagegen gibt es auch den folgenden Nichtexistenzsatz:

Satz 4. Sei char(k) = 2 oder 3 und E_1 und E_2 supersingulär. Dann ist $n(E_1, E_2, N) = 0$ für alle Primzahlen N ($\neq$ char(K)).

G. Frey (Essen)

Über Kurven vom Geschlecht 2, die elliptischen Kurven überlagern, und eine arithmetische Anwendung

Sei C eine reguläre minimale arithmetische Fläche über einem Zahlkörper K. Die Fasern von C seien semistabil, das Geschlecht der allgemeinen Faser sei g und der Führer von C sei N_C. Dann wird für die Selbstschnittzahl der relativen dualisierenden Garbe ω_C vermutet: $\omega_C^2 \leq c \deg N_C + d$, wobei c nur von g abhängt und d linear von $\log|s_k|$ und polynomial von [K:Q] und g abhängt. Durch Verwendung der im letzten Vortrag beschriebenen Konstruktion wird gezeigt, daß die Richtigkeit dieser Vermutung für C mit g = 2 die Höhenvermutung für elliptische Kurven impliziert: Sei E|K eine semistablie elliptische Kurve mit Führer N_E. Dann ist ihre Faltingshöhe $h_K(E) \leq c_1 \deg N_E + d_1$ mit nur von K abhängigen Zahlen c_1 und d_1.
Wir hoffen, daß wir mit ähnlichen Überlegungen auch folgende Vermutung angreifen können: Sei E|K eine elliptische Kurve. Dann gibt es nur endlich viele natürliche Zahlen n und elliptische Kurven $E^{(n)}|K$, so daß die n - Torsionspunkte von E und $E^{(n)}$ Galois-isomorph sind.

F. Pop (Heidelberg)

Isomorphisms of stratified absolute Galois groups

To state the main result, one needs the following definition:

Definition. Let K be an infinite field, finitely generated and of transcendence degree $r \geq 0$ over its prime field F.

I. A geometrical stratification on K consists of a tower $\mathcal{K} = (K_k)_{1 \leq k \leq r}$ of subfields of K satisfying: $K_0 = F$ and $K_k \mid K_{k-1}$ is a rational function field of one variable for all k.
If $r = 0$ then any geometrical stratification is empty by definition.

II. A Galois stratification on G_K is the sequence of normal subgroups of G_K $\mathcal{G} = (\mathcal{G}_{K_k})_{1 \leq k \leq r}$ which is defined by a geometrical stratification $\mathcal{K} = (K_k)_k$ of K by setting $\mathcal{G}_{K_k} = G_{KK_k^{sep}}$, viewed as subgroup of G_K.
If $r = 0$ then any Galois stratification is empty by definition.

Theorem. Let K and L be finitely generated infinite fields and suppose that

$$\Phi : G_K \longrightarrow G_L$$

is an isomorphism of their absolute Galois groups which maps a given Galois stratification $(\mathcal{G}_{K_k})_k$ of G_K isomorphically onto a Galois stratification $(\mathcal{G}_{L_\ell})_\ell$ of G_L. Then there exists a unique isomorphism ($\tilde{}$ denotes the algebraic closure)

$$\tilde{\Phi} : \tilde{L} \longrightarrow \tilde{K}$$

such that $\Phi(g) = \tilde{\Phi}^{-1} g \tilde{\Phi}$ for all $g \in G_K$. In particular, $\tilde{\Phi}$ maps the perfect closure L_m^1 of each L_m isomorphically onto the perfect closure K_m^1 on K_m for all m.

H.W. Lenstra, jr. (Berkeley)

Factoring integers with algebraic number fields

In this lecture a new integer factoring method is described, the number field sieve, which depends on the use of algebraic number fields. It was invented by J.M. Pollard (England) in 1988, and further developed jointly with A.K. Lenstra (Bellcone, New Jersey) and M. Manasse (DEC, Palo Alto). It was recently used to factor the 148-digit number $F_9/2424833 = (2^{2^9}+1)/2424833$ into the product of two primes of 49 and 99 digits, the smaller one being

7455602 8256478 8420833 7395736 2004549 1878336 6342657 .
Currently the method is only practically possible for special numbers n, but one conjectures that even for general n it should, for $n \longrightarrow \infty$, be faster than any other known method.

R.W.K. Odoni (Glasgow)

New results on free quotients of $SL(2,O_K)$

Let $\mathcal{D} = \{ d \in \mathbb{N} \mid -d$ is a quadratic field discriminant $\}$. Let $d \in \mathcal{D}$. $K = \mathbb{Q}(\sqrt{-d})$ and for $m \in \mathbb{N}$ let $R_d(m)$ be the unique $\mathbb{Z}$-order in K with $(O_K : R_d(m)) = m$. The group $B = B(d,m) = SL(2,R_d(m))$ is called a Bianchi group.
Zimmert (1971) and Grunewald/Schwermer (1980) showed, that there is an epimorhism

$$B(d,m) \longrightarrow\!\!\!\!\!\rightarrow \mathcal{F}_z$$

where $\mathcal{F}_z$ is the free group on z generators and $z = z_d(n) = \# Z_d(n)$. Here $Z_d(n)$ an finite subset of $\mathbb{N}$, which has an expicit description.
By applying methods of analytic number theory asymptotic formulas for the value $Z_d(1)$ (observe $R_d(1) = O_K$) were obtained.
This makes it possible to find all Bianchi groups, which lack a non-abelian quotient. Computer programmes have been written to do this.

R. Schoof (Utrecht)

On the work of Kolyvagin on class groups of abelian number fields

Recently Kolyvagin gave a description of the class groups of abelian number fields. The description of the minus parts involves "generalized" Bernoulli numbers, while cyclotomic units are used to describe the plus parts. For the minus-part the result was as follows:
Let $p \neq 2$ be a prime and let $\chi : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \bar{\mathbb{Q}}_p^*$ be a character of order prime to p. Let f denote the conductor of χ and let $Cl(\chi)$ denote the χ-eigenspace of the p-part of the classgroup of $K = \bar{\mathbb{Q}}^{Ker\,\chi}$.
Let p^M be a large power of p. Let S be the following set of integer

$$S = \{ n = \text{square-free product of primes } \ell \equiv 1 \pmod{p^M},\ \chi(\ell) = 1 \}$$

Definition. For $n \in S$ $B_\chi(n) = \sum_{x \in (\mathbb{Z}/n\mathbb{Z})^*} \left\langle \frac{x}{n} \right\rangle \chi^{-1}(x) \prod_{\ell \mid n} \mathrm{ind}_\ell x \in R_\chi / p^M R_\chi$

where: for $\alpha \in \mathbb{R}$ $\langle \alpha \rangle \in [0,1)$ satisfies $\alpha \equiv \langle \alpha \rangle \bmod \mathbb{Z}$
: $\mathrm{ind}_\ell : (\mathbb{Z}/\ell\mathbb{Z})^* \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}/p^M\mathbb{Z}$ a homomorphism.

Definition. $I_\chi^{(k)}$ = the ideal in $R_\chi / p^M R_\chi$ generated by $B_\chi(n)$ for $n \in S$ having at most k prime divisors.

Note that $B_\chi(1)$ is the usual Bernoulli number $B_{1,\chi^{-1}}$ while $I_\chi^{(0)}$ is the usual Stickelberger ideal.

Theorem. For all $k \geq 0$

$$I_\chi^{(k)} = F\,it_{R_\chi}^{(k)}(Cl(\chi)) \pmod{p^M}.$$

Here R_χ is the χ - part of the groupring $\mathbb{Z}_p[\Delta]$ where $\Delta = Gal(K/\mathbb{Q})$. Since the sequence of higher Fitting ideals determine the structure of $Cl(\chi)$ as an R_χ - module, one obtains from the theorem a description of the structure of $Cl(\chi)$ in terms of the numbers $B_\chi(n)$.

J. Ritter (Augsburg)

Über die Ganzzahligkeit von Gruppendarstellungen

Im Vortrag wird über gemeinsame Untersuchungen mit A. Weiss aus Edmonton zu zwei Fragen aus obigem Themenkreis berichtet. 1. Gibt es zu vorgegebener irreduzibler komplexer Darstellung T einen minimalen Zerfällungskörper F, so daß T ganzzahlig über F realisierbar ist; falls dem so ist, gilt dasselbe dann auch schon für jeden minimalen Zerfällungskörper? Dies ist eine alte Frage in der Darstellungstheorie, die bei ungeraden nilpotenten Gruppen von Roquette positiv beantwortet wurde. 2. Falls, wie oben, T über einem Zerfällungskörper F realisierbar ist, läßt sich dann T^γ für jeden Automorphismus γ von F über dem Sphärenkörper $\mathbb{Q}(tr\,T)$ ganzzahlig in T konjugieren? Diese Frage wurde von Fröhlich im Zusammenhang mit Untersuchungen zur multiplikativen Galoismodulstruktur gestellt. Zu 1. wird mit $G = \langle x, y : x^{19} = 1 = y^9,\ x^9 = x^7 \rangle$ ein Gegenbeispiel zur ersten Teilfrage und mit der achtelementigen Quaternionengruppe eines zur zweiten Teilfrage (mit $F = \mathbb{Q}(i)$ und $= \mathbb{Q}(\sqrt{-35})$) gegeben. Frage 2. wird positiv beantwortet, falls F eine Einheitswurzel der Ordnung $|G|$ enthält.

B.W. Green (Heidelberg)

Stable reductions of algebraic curves

Let F/K be a function field in 1 variable over an algebraically closed field K and V a finite set of valuations of F such that the residue field Fv is a function field in 1 variable over the corresponding residue field Kv. $f \in F$ is defined to be V - regular for F/K if f is residually transcendental for each $v \in V$ and $\deg f = \sum_{v \in V} \deg f_v$.

One can associate to each V - regular function $f \in F$ a residue curve $C_f w$ having Fw as ring of fractions. ($Fw = \mathcal{O}_w / \mathcal{M}_w$, $\mathcal{O}_w \{ x \in F \mid v(x) \geq 0 \ \forall v \in V \}$, $\mathcal{M}_w = \{ x \in F \mid v(x) > 0 \ \forall v \in V \}$.)

Theorem 1. Let f and g be V - regular functions for F | K. Then the curves in reduction $C_f w$ and $C_g w$ are isomorphic (notation Cw).

Theorem 2. Let (K,v_K) be a valued field and suppose that K is algebraically closed. Let $F \mid K$ be any function field in 1 variable, with $g_F \geq 2$. Then there exists a unique set of constant reductions $V = \{ v_i : 1 \leq i \leq s \}$, $v_i \mid_K = v_K$, such that the curve Cw is stable, ie. Cw is reduced and connected, has only ordinary double points as singularities and each non-singular rational component of Cw meets the other components in at least 3 points.

J. Neukirch (Regensburg)

Was ist ein Motiv?

Mit dem Ziel, einer größeren Allgemeinheit auf diese geheimnisvolle Frage eine Auskunft zu geben, die von allen technischen Komplikationen frei einem direkten Verständnis zugänglich sein sollte, wurde die Geschichte des Begriffs "Motiv" erzählt, wurde geschildert, welcher Gedanke seinen Erfinder Alexander Grothendieck bestimmte, seine erste Definition zu geben, wie Pierre Deligne mit seinen "absoluten Hodge-Zyklen" eine neue Theorie der Motive aufbaute. Weiter wurde die elegante Theorie von Uwe Jannsen dargestellt, die gemischten Motive vorgestellt und die motivische Galoisgruppe definiert. Es wurde der tiefliegende Zusammenhang mit der K - Theorie erwähnt und die Anwendungen auf die motivischen L - Reihen hervorgehoben, wie sie in der Deligne-Vermutung und der Beilinson-Vermutung zum Ausdruck kommen.

C. Deninger (Münster)

Lokale Faktoren der Hasse-Weil L - Funktionen

Sei $X/\mathbb{Q}$ eine glatte, projektive Varietät. Für $0 \leq \omega \leq \dim X$ betrachtet man die L - Funktion:

$$L(H^\omega(X),s) = \prod_p \det_{\mathbb{Q}_\ell} (1 - Fr_p^* p^{-s} \mid H^\omega(X_{\overline{\mathbb{Q}}},\mathbb{Q}_\ell)^{I_p})^{-1}, \quad \ell \neq p$$

mit den üblichen Bezeichnungen. Diese hat man zur Gewinnung einer Funktionalgleichung mit einem Γ - Faktor $L_\infty(H^\omega(X),s)$ zu vervollständigen, der nach einer Vorschrift von Serre aus der Hodge Struktur über $\mathbb{R}$ gewonnen wird. Dann vermutet man für $\Lambda(H^\omega(X),s) = L(H^\omega(X),s)\, L_\infty(H^\omega(X),s)$ meromorphe Fortsetzbarkeit nach $\mathbb{C}$ und eine Funktionalgleichung. Im Vortrag wurden mit Hilfe einfacher "Barsotti-Tate"-Ringe $\mathbb{C}$ - Vektorräume $\mathcal{F}_p$ für $p \leq \infty$ mit Endomorphismen Θ_p konstruiert. Für p, so daß $H^\omega(X)$ gute Reduktion hat, ist $\mathcal{F}_p = H_p^\omega(X)$ mit einer Cohomologietheorie H_p^ω auf reinen absoluten Hodge Motiven M für die $H^\omega(M)$ gute Reduktion hat. Entscheidend sind nun die Formeln:

$$L_p(H^\omega(X),s) = \det_\infty\Big(\tfrac{\log p}{2\pi i} (s - \Theta_p) \,\Big|\, H_p^\omega(X) \Big)^{-1} \quad \text{für} \quad p \leq \infty .$$ [Für $p < \infty$ falls Fr_p^* halbeinfach auf $H_{et}^\omega(X)^{I_p}$ operiert.] Hierbei ist $\det_\infty$ eine geeignet regularisierte Determinante und $\log \infty := i$. Diese einheitliche Formel für die lokalen L - Faktoren an den endlichen und unendlichen Stellen läßt hoffen, daß

sich das Grothendiecksche Programm zur Behandlung der L - Funktionen vom Funktionenkörper- auf den Zahlkörperfall übertragen läßt. Man hat hierzu einen Topos über $\overline{\mathrm{Spec}\,\mathbb{Z}} = \mathrm{Spec}\,\mathbb{Z} \cup \{\infty\}$ zu finden. Für den $\mathcal{F}_p = (j_* R^\omega \pi_* \mathcal{O}_X^{\mathrm{Topos}})_p$ für $p \in \overline{\mathrm{Spec}\,\mathbb{Z}}$ ist. Hierbei: $X \xrightarrow{\pi} \mathrm{Spec}\,Q \to \mathrm{Spec}\,\mathbb{Z}$.

W. Bauer (Wuppertal)

Zur Vermutung von Birch und Swinnerton-Dyer für abelsche Varietäten über Funktionenkörpern der Charakteristik p

Sei p eine ungerade Primzahl. $S/\mathbb{F}_p$ eine glatte, projektive, integre Kurve mit Funktionenkörper K. Ferner sei A/S eine abelsches Schema und $A_K := A \times_S \mathrm{Spec}\,K$.
Mit Resultaten von Katz-Messing und Etesse leiten wir aus der ℓ-adischen Darstellung der Hasse-Weil L - Funktion A_K/K eine explizite rationale Darstellung von $L(s)$ in p^{-s} ab: $L(s) = \dfrac{P_1(p^{-s})}{P_0(p^{-s}) \cdot P_2(p^{-s})}$, wobei $P_i(t)$ das charakteristische Polynom des Frobenius auf der i-ten kristallinen Kohomologie von S mit Koeffizienten im Dieudonné-Modul von A/S nach Berthelot-Breen-Messing ist. Hieraus erhalten wir eine Darstellung von $L(s)$ mittels syntomischer Kohomologie. Mit der fundamentalen exakten Sequenz

$$0 \longrightarrow \mu_{p^n} \longrightarrow I_n \xrightarrow{1-p^{-1}F} \mathcal{O}_n^{\mathrm{cris}} \longrightarrow 0,$$

die man aus Fontaine-Messing's Resultaten gewinnt, zeigen wir:

Satz. Sei ρ die Ordnung der Nullstelle von $L(s)$ bei $s = 1$. Dann gilt:
$\rho = \mathrm{rg}_{\mathbb{Z}} A_K(K) \iff Ш(A_K/K)(p)$ ist endlich, und in diesem Fall ist:

$$\left| \lim_{s \to 1} L(s)\,(s-1)^{-\rho} \right|_p^{-1} = \frac{\#\,Ш(A_K/K)(p) \cdot |\det h|_p^{-1}}{\#\,A_K(K)(p) \cdot \#\,\hat{A}_K(K)(p)} \cdot q^{-\deg e^* \Omega^1_{A/S} + d(1-g)}.$$

Dabei ist h die Neron-Tate Höhenpaarung, $e : S \longrightarrow A$ der Einsschnitt, $d = \dim A_K$ und g das Geschlecht von K.

Mit dem entsprechenden Satz von P. Schneider für $\ell \neq p$ erhält man unter der Voraussetzung, daß $Ш(A_K/K)(\ell)$ endlich ist für eine Primzahl ℓ, die Vermutung von Birch und Swinnerton-Dyer, wie von Tate formuliert.

U. Jannsen (Bonn)

Hasse Prinzip und quadratische Formen über höher-dimensionalen Körpern

Ist K ein algebraischer Zahlkörper, so ist nach dem Satz von Hasse-Brauer-Noether die von den Restriktionen induzierte Abbildung

$$\mathrm{Br}(K) \longrightarrow \bigoplus_v \mathrm{Br}(K_v)$$

injektiv, wobei v die Stellen von K durchläuft und K_v die Komplettierung

von K bezüglich v ist. Kato zeigte, daß sich dies in folgender Weise auf einen Funktionenkörper F in einer Variablen über K verallgemeinert: hier ist die Abbildung

$$H^3(F,\mathbb{Q}/\mathbb{Z}(2)) \longrightarrow \bigoplus_v H^3(FK_v,\mathbb{Q}/\mathbb{Z}(2))$$

injektiv. Beide Sätze haben als Konsequenz Hasse-Prinzipien für (gewisse) quadratische Formen und Abschätzungen für Pythagoraszahlen (minimale Anzahl von Quadraten für die Darstellung einer Summe von Quadraten).
Es wurde ein neuer Beweis von Katos Satz skizziert, der sich auf den nächst höherdimensionalen Fall verallgemeinern läßt:

Satz. Sei F ein Funktionenkörper in zwei Variablen über K. Dann ist die Restriktionsabbildung

$$H^4(F,\mathbb{Q}/\mathbb{Z}(3)) \longrightarrow \bigoplus_v H^4(FK_v,\mathbb{Q}/\mathbb{Z}(3))$$

injektiv.

Wieder ergeben sich Anwendungen auf quadratische Formen: nach einer Bemerkung von Colliot-Thélène folgt aus dem Satz zusammen mit Ergebnissen von Merkuriev, Suslin, Rost und Jacob ein Hasse-Prinzip für Pfisterformen der Dimension 8 und daraus wiederum, daß in F jede Quadratsumme Summe von 8 Quadraten ist.
Allgemein sollte für einen Funktionenkörper von Transzendenzgrad d über K ein entsprechendes Lokal-Globalprinzip für $H^{d+2}(\,.\,,\mathbb{Q}/\mathbb{Z}(d+1))$ gelten. Man beachte, daß $H^2(K,\mu_\infty) = H^2(K,\mathbb{Q}/\mathbb{Z}(1)) \xrightarrow{\sim} Br(K) = H^2(K,\overline{K}^*)$ ist.

K. Wingberg (Heidelberg)

Galoisgruppen algebraischer Zahlkörper und Selmergruppen elliptischer Kurven

Sei E eine elliptische Kurve mit CM durch den Ring der ganzen Zahlen eines imaginär-quadratischen Zahlkörpers K mit guter ordinärer Reduktion bei $p \neq 2, 3$, also $p = \mathfrak{p}\overline{\mathfrak{p}}$ in K. Sei $F = K(E_p)$ und F_∞ die zyklotonische $\mathbb{Z}_p$-Erweiterung von F.

Theorem. Es existiert eine natürliche Galoiserweiterung $\tilde{F}$ von F, derart, daß $G(\tilde{F}/F_\infty)$ eine Demuskingruppe ist; genauer gibt es $2\tilde{g}$ Erzeugende $x_1, y_1, \ldots, x_{\tilde{g}}, y_{\tilde{g}}$ von $G(\tilde{F}/F_\infty)$, wobei $\tilde{g}$ die Summe gewisser Iwasawa-λ-Invarianten ist, mit einer definierenden Relation

$$\prod_{i=1}^{\tilde{g}} [x_i,y_i] = 1 .$$

Ferner identifiziert sich die nicht-ausgeartete Paarung

$$H^1(G(\tilde{F}/K_\infty),T_p(E)) \times H^1(G(\tilde{F}/K_\infty),T_p(E)) \xrightarrow{\cup} H^2(G(\tilde{F}/K_\infty),T_p(G_m)) \xrightarrow{\sim} \mathbb{Z}_p$$

mit der algebraischen p-adischen Höhenpaarung von E/K_∞, falls p nicht

anormal für E ist.
Allgemeiner kann gezeigt werden, daß $H^1(G(\tilde{F}/Q_\infty), Sym^n(E(p))(k))$ sich für kritisches $k \in \mathbb{Z}$ mit der von R. Greenberg definierten Selmergruppe $S(n,k)$ identifiziert, wobei $Sym^n(E(p))$ die n-te symmetrische Potenz der Galoisdarstellung $G_Q \longrightarrow Aut(E_{p^m})$, $m \geq 1$, bezeichnet. Somit ergibt sich eine kanonische Quasi-Isomorphie

$$S(n,k)^* \approx \overline{S(n,1-n-k)}^* \qquad (\cdot \text{ inverse } G(F_\infty/F)\text{-Op.})$$

C. Schmidt (Karlsruhe)

Kongruenzeigenschaften spezieller L - Funktionswerte Siegelscher Modulformen

Der Vortrag berichtet über eine Arbeit zusammen mit S. Böcherer (Freiburg). Es werden Siegelsche Modulformen $F: \mathbb{H}_n \longrightarrow \mathbb{C}$ vom Grad n und Gewicht k betrachtet, welche Eigenformen unter der Hecke-Algebra sind. Eine wichtige Invariante solcher Modulformen ist die zugehörige Standard- L -Funktion $D(F,s)$. Es wurden die sogenannten kritischen Werte aller getwisteten L - Funktionen $D(F,\chi,s)$ untersucht hinsichtlich:
Algebraizität, Nennerabschätzung und p - adischer Interpolierbarkeit.
Das Hauptresultat ist die Existenz einer p - adischen L - Funktion $L_p(F,s)$, vorausgesetzt F genügt einer gewissen p - Regularitätsbedingung. Die so gefundenen L - Funktionen enthalten als Spezialfall für $n=1$ die von Coates und dem Vortragenden konstruierten p - adischen L - Funktionen zum symmetrischen Quadrat einer modularen elliptischen Kurve E/Q.

E. Nart (Bellaterra, Barcelona)

Gute Reduktion elliptischer Kurven über Zahlkörpern

Es werden einige Ergebnisse von S. Comalada vorgestellt:
Sei K ein Zahlkörper; für jede endliche Stelle v von K betrachte man die Menge: $J(v) = \{ j \in K \mid$ es existiert eine elliptische Kurve $/K_v$ mit guter Reduktion bei v und j - Invariante $j \}$. Es gilt:

$v \nmid 6 \Rightarrow \quad J(v) = \{ j \in \mathcal{O}_v : v(\Delta_j) \equiv 0 \pmod 6 \}$, wobei $\Delta_j = 6^{12} \frac{j^2}{(j-1728)^3}$

$v \mid 3 \Rightarrow \quad J(v) = \{ j \in \mathcal{O}_v : v(\Delta_j) \equiv 0 \pmod 6$ und $f_j(X)$ hat eine Wurzel modulo $\mathfrak{p}_v^{v(\Delta_j)/2} \}$, $f_j(X) = X^3 - 27 \frac{j}{j-1728} X - 54 \frac{j}{j-1728}$ und $\mathfrak{p}_v$ ist das Primideal von $\mathcal{O}_v :=$ v - ganzzahlige Elemente von K.

$v \mid 2 \Rightarrow \quad J(v) = \{ j \in \mathcal{O}_v : v(\Delta_j) \equiv 0 \pmod 6$ und $q_j(X)$ hat eine Wurzel modulo $\mathfrak{p}_v^{2v(\Delta_j)/3} \}$, $q_j(X) = 3X^4 - 6 \cdot 27 \frac{j}{j-1728} X^2 - 12 \cdot 54 \frac{j}{j-1728} X - \left(\frac{27j}{j-1728} \right)^2$

Sei $J = \{ j \in K :$ es existiert eine elliptische Kurve $/K$ mit überall guter Reduktion und j - Invariante $j \}$.

Das Hauptergebnis ist: $J = \{ j \in K : j \in J(v)$ für alle v und $\prod_v (d_v, u) = 1$ $\forall u \in U_K^+ / U_K^2 \}$, wobei U_K^+ die total-positiven Einheiten und $(d_v)_v$ explizit gegebene Elemente von K_v^* / K_v^{*2} sind.

A. Pfister (Mainz)

Systeme quadratischer Formen

Ein Satz von D. Leep über die System- n -Invariante eines nichtreellen Körpers F wird auf reelle Körper F übertragen. Sei $Q = (Q_1, \ldots, Q_r) : V \longrightarrow F^r$ eine quadratische Abbildung und $2Q = Q \oplus Q = V \oplus V \longrightarrow F^r$. Man schreibt $2Q \sim O$, wenn $2Q$ auf einem Teilraum $T \subset V \oplus V$ mit $\dim T \geq \dim V$ verschwindet. Die (modifizierte) System-Invariante wird definiert duch

$$u_r'(F) = \operatorname{Max} \{ \dim V \mid \exists Q : V \longrightarrow F^r, \ Q \text{ ansisotop}, \ 2Q \sim O \}.$$

Sei ferner $w(F) := u'(F(\sqrt{-1})) < \infty$. Dann ist auch $u_r'(F)$ endlich für alle $r \in \mathbb{N}$, und man hat eine Abschätzung

$$(*) \qquad u_1' \leq 2(w-1), \quad u_r' \leq \frac{9}{16} w^3 r^6 \text{ für } r \geq 2.$$

Es wurden viele Beispiele gegeben, in denen man u_1' und w genau kennt oder obere Abschätzungen hat. Für Zahlkörper und Funktionenkörper über endlichen Körpern oder reell-abgeschlossenen Körpern läßt sich (*) verbessern. Falls F nichtreell (d.h. -1 Quadratsumme in F) ist, gilt nach Leep die bessere Abschätzung

$$u_r' \leq u_1' \cdot r(r-1).$$

E. Bayer Flueckiger (Besançon)

Trace forms in Galois extensions

Let K be a field, $\operatorname{char}(K) \neq 2$, and let $T : L \times L \longrightarrow K$ be the trace form:

$$T(x,y) = \operatorname{Tr}_{L/K}(xy).$$

Problem. Which Galois extensions have a self-dual normal basis?

Theorem 1 (E.B.-H. Lenstra). Every Galois extension of odd degree has a self-dual normal basis.

On the other hand, it is easy to see that if G has a quotient of order 2, then L/K has no self-dual normal basis.

This talk gave some results about the existence of such bases in extensions

with group of even order, but without quotient of order 2 . These results were obtained in common with J.-P. Serre.
For instance one has:
Let $G = J_1$ be the first Jankogroup and L/K an extension with group J_1 . One has $H^3(J_1,\mathbb{Z}/2\mathbb{Z}) = \{1, c\}$. Let $c(L/K)$ be the image of c under $H^3(J_1,\mathbb{Z}/2\mathbb{Z}) \longrightarrow H^3(K,\mathbb{Z}/2\mathbb{Z})$. Then

Theorem 2 (E.-B. - J.-P. Serre). L/K has a self-dual normal basis if and only if $c(L/K) = 0$.

R. Kucera (Brno)

On the bases of the Stickelberger ideal and the group of circular units of a cyclotomic field

In his talk the referent gave the following generalization of Kubert's ordinary distribution: Let $T_1, \dots, T_n$ be any finite abelian groups with elements $j_i \in T_i$ of order 2 . One can construct abelian semigroups $T_i^* = T_i \cup \{g_i^*\}$ by inserting a new element g_i^* and defining $a \cdot g_i^* = g_i^*$ for any $a \in T_i^*$. One considers the group $G = \prod_{i=1}^{n} T_i$ and the semigroup $G^* = \prod_{i=1}^{n} T_i^*$. Let us fix any $\lambda_1, \dots, \lambda_n \in G$. A distribution is any mapping $\varphi : G^* \longrightarrow A$, where A is an abelian group, satisfying the relation $\sum_{\beta \in T_i} \varphi(\beta\alpha) = \varphi(g_i^*\alpha) - \varphi(g_i^*\lambda_i\alpha)$ for any $i \in \{1, \dots, n\}$ and for any $\alpha \in G^*$, $\alpha g_i^* \neq \alpha$. We can consider a universal distribution $\varphi_U : G^* \longrightarrow U$ (in the sence of category theory) and take U as G-module. Let $j = (j_1, \dots, j_n) \in G$.

Theorem. $\{(1+j)\varphi(\alpha);\ \alpha \in M_+\}$ is a basis of $(1+j)U$ and $\{(1-j)\varphi(\alpha);\ \alpha \in M_-\}$ is a basis of $(1-j)U$ (considered as $\mathbb{Z}$-module), where

$$M_\pm = \prod_{i=1}^{n} \left(T_i^* \setminus \{j_i\} \right) \Big\backslash \left(N_\pm \cup \bigcup_{k=1}^{n} \left(\prod_{i=1}^{k-1} T_i^* \right) \cdot T_K' \cdot \left(\prod_{i=k+1}^{n} \{1, g_i^*\} \right) \right)$$

$T_K' \subset T_K$ is such that $1 \in T_K'$, $T_K' \cup j_K T_K' = T_K$, $T_K' \cap j_K T_K' = \emptyset$ and

$$N_\pm = \left\{ (k_1, \dots, k_n) \in \prod_{i=1}^{n} \{1, g_i^*\};\ (-1)^{\operatorname{card}\{i; k_i = 1\}} = \mp 1 \right\} .$$

This theorem can be used for the explicit construction of bases of the Stickelberger ideal and of the group of circular units in any cyclotomic field. By means of these bases elementary proofs of Sinnott's class number formulas can be obtained by computing a determinant of a transition matrix.

G. Frei-Imfeld (Quebec)

Zur Vorgeschichte des Artinschen Reziprozitätsgesetzes

Anhand der Geschichte der Dichtigkeitssätze bei Dirichlet, Kronecker, Frobenius und Čebotarev wird gezeigt, daß daraus nicht nur die Beweisidee für das Artinsche Reziprozitätsgesetz hervorgegangen ist, sondern auch die Schaffung der Klassenkörpertheorie durch Weber. Wichtige Etappen waren die Erforschung der Kreisteilungskörper und die Sätze von Kronecker über den von den singulären Werten erzeugten absoluten Klassenkörper über einem imaginär-quadratischen Zahlkörper sowie die von Dedekind und Frobenius unabhängig eingeführte Frobeniussubstitution.

F. Halter-Koch (Graz)

Ein quantitatives Resultat über nicht-eindeutige Faktorisierungen

Für einen noeth. Integritätsbereich R, $\alpha \in R$, $\alpha \neq 0$, $\alpha \notin R^*$ sei $F_R(\alpha)$ die Anzahl der wesentlich verschiedenen Faktorisierungen $\alpha = u_1 \cdot \ldots \cdot u_r$ in irreduzible Elemente $u_i \in R$.

Satz. K sei globaler Körper, S endliche Menge von Stellen von K, $S \supset S_\infty(K)$ im ZK-Fall, $S \neq \emptyset$ im FK-Fall, $R = \bigcap_{v \notin S} \mathcal{O}_{K,v}$ der Holomorphiering. $\overline{K}/K$ endlich separabel, $\overline{S}$ endliche Menge von Stellen von $\overline{K}$, die alle Fortsetzungen von Stellen in S enthält, $\overline{R} = \bigcap_{\overline{v} \notin \overline{S}} \mathcal{O}_{\overline{K},\overline{v}} \supset R$. Dann ist für $f_0 \lhd R$, $\alpha_0 \in R$:

$$\#\left\{ (\alpha) \lhd R \mid \alpha \equiv \alpha_0 \bmod f,\ F_{\overline{R}}(\alpha) \le k,\ (R:\alpha R) \le x \right\} =$$

$$Cx(\log x)^{-1+\frac{1}{k}} \cdot \left[\sum_{\nu=0}^{N} \frac{P_\nu(\log\log x)}{(\log x)^\nu} + O\left(\frac{(\log\log x)^j}{(\log x)^{N+1}} \right) \right]$$

für jedes $N \ge 1$. Dabei ist $P_\nu \in \mathbb{Z}[X]$, $\deg P_0 = \bar{a}_k \ge 2$, $j \in \mathbb{N}$. $\bar{a}_k$ hängt von der duch die Primideale $\mathfrak{p}$ von R auf $Cl(\overline{R})$ definierten Orbitstruktur, nicht von α_0 oder f ab. Weiter ist $\bar{h} = \left[K^{S,f} \cdot \widetilde{H(\overline{K})} : K \right]$, wobei $\widetilde{H(\overline{K})}$ = normale Hülle $/K$ des Hilbertschen Klassenkörpers von $\overline{K}$; $K^{S,f}$ = (f,S)-Strahlklassenkörper ist.
Im Funktionenkörperfall sei $q = \#(\text{Konst}(K))$; dann gilt die Asymptotik nur für $x = q^n \longrightarrow \infty$ (gem. Arbeit mit W. Müller).

J. Brinkhuis (Rotterdam)

On ambiguous classes

A rather general method to get an explicit grip on the G-invariant classes in the class group of an order (where G is a finite group acting on the order) will be presented. The motivating test case is the problem of determining the

structure of the ring of integers in $Q(\mu_p)$ as a Galois module over an intermediate field K with [N:K] prime. The method leads for example to the result that the element in the appropriate class group which describes this structure has order [K:Q]. Over the maximal orders this becomes either [K:Q] or $\frac{1}{2}$[K:Q].
A byproduct of the method is a trivial way to determine the prime factorisation of Gauss sums.

A. Leutbecher (München)

Einheitengraphen in Zahlringen

Diese Einheitengraphen wurden 1980 von K. György eingeführt und stecken implizit in H.W. Lenstras Konstruktion euklidischer Zahlkörper von 1977. Ein kommutativer Ring R mit ausgezeichneter Untergruppe U von R^* (für die $-1 \in U$ ist) definiert wie folgt einen Graphen $\Gamma(R,U)$: Die Eckenmenge von $\Gamma(R,U)$ ist R selbst und die Kanten sind die Paare $(a,b) \in R^2$ mit $a - b \in U$. Diese Struktur $\Gamma(R,U)$ ist mit Ringmorphismen verträglich, und daraus resultieren z.B. im Zahlkörperfall Abschätzungen für verallgemeinerte Cliquenzahlen $M_k(R,U)$, $k \in \mathbb{N}$, $M_\infty(R,U) = \lim_{k\to\infty} M_k(R,U)/k$. Der Referent berichtet über neuere Ergebnisse von G. Niklasch. Darunter ist einerseits die Einbettung des "affinen" Graphen in einen "projektiven" Graphen $\Gamma P(R,U)$, dessen Struktur wichtige Invarianten des Ringes wiederspiegelt, und andererseits die explizite Bestimmung der Limescliquenzahl M_∞ für eine Serie von Ordnungen algebraischer Zahlkörper.

G. Everest (Norwich)

The traces of algebraic units and the Leopoldt conjecture

Two asymptotic formulas will be compared. One counts the traces of units in a totally real extension of Q; the other counts the p-primary parts of those traces. In connection with the Leopoldt conjecture the comparison shows the presence of an "Euler-factor" and, in the most interesting case, the size of this factor is measured by the inverse of the (Leopoldt) p-adic regulator. The referent gives an indication of how these results are obtained.
Also these formulas will be extended to a "3-term" formula and a brief indication of the proof will be given, refering back to the fundamental work of Hardy and Littlewood for this type of problem.

E. Kleinert (Hamburg)

Gruppenordnungen und Faserprodukte

Jeder Ordnung Λ über einem Dedekindring R ist eine Ordnung $\tilde{\Lambda}$ kanonisch zugeordnet, die sich charakterisieren läßt als die eindeutig bestimmte kleinste

Oberordnung von Λ, die als mehrfaches Faserprodukt geschrieben werden kann. Die Grundeigenschaften der Zuordnung $\Lambda \longrightarrow \tilde{\Lambda}$ werden beschrieben; die Frage wird untersucht, wann $\Lambda = \tilde{\Lambda}$ ist. Für $\Lambda = \mathbb{Z}_p G$, G endlich mit normaler p-Sylowgruppe, wird ein notwendiges und hinreichendes Kriterium für $\Lambda = \tilde{\Lambda}$ in Termen von G angegeben.

Berichterstatter: K.Künnemann (Münster)

Tagungsteilnehmer

Prof.Dr. Jannis A. Antoniadis
Dept. of Mathematics
University of Crete
P. O. Box 407

Iraklion Crete
GREECE

Dr. Werner Bauer
Fachbereich 7: Mathematik
Universität/Gesamthochschule
Wuppertal, Gaußstr. 20
Postfach 10 01 27

5600 Wuppertal 1

Dr. Eva Bayer-Flueckiger
Lab. de Mathematiques
Universite de Franche-Comte
Route de Gray

F-25030 Besancon

Prof.Dr. Sigrid Böge
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288/294

6900 Heidelberg 1

Dr. Jan Brinkhuis
Econometrisch Instituut
Erasmus Universiteit
Postbus 1738

NL-3000 DR Rotterdam

Prof.Dr. Christopher Deninger
Mathematisches Institut
Universität Münster
Einsteinstr. 62

4400 Münster

Dr. Graham Everest
School of Mathematics
University of East Anglia
University Plain

GB- Norwich, Norfolk , NR4 7TJ

Prof.Dr. G. Frei-Imfeld
Dept. de Mathematiques,
Statistiques et Act.
Universite Laval
Cite Universitaire

Quebec , PQ G1K 7P4
CANADA

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

4300 Essen 12

Prof.Dr. Albrecht Fröhlich
Dept. of Mathematics
Imperial College of Science
and Technology
Queen's Gate, Huxley Building

GB- London , SW7 2BZ

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

8520 Erlangen

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

Tel Aviv , 69978
ISRAEL

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

6900 Heidelberg 1

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

5000 Köln 41

Prof.Dr. Franz Halter-Koch
Institut für Mathematik
Universität Graz
Halbärthgasse 1/I

A-8010 Graz

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

DK-2100 Kobenhavn

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

Tel Aviv , 69978
ISRAEL

Dr. Ernst Kani
Department of Mathematics and
Statistics
Queen's University

Kingston, Ontario K7L 3N6
CANADA

Dr. Uwe Jannsen
Max-Planck-Institut für Mathematik
Gottfried-Claren-Str. 26

5300 Bonn 3

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

8400 Regensburg

Dr. Ernst Kleinert
Mathematisches Seminar
Universität Hamburg
Bundesstr. 55

2000 Hamburg 13

Prof.Dr. Johann B. Leicht
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288/294

6900 Heidelberg 1

Prof.Dr. Helmut Koch
Akademie der Wissenschaften
Karl-Weierstraß-Institut für
Mathematik
Mohrenstr. 39/Postfach 1304

DDR-1086 Berlin

Prof.Dr. H.W. Lenstra jr.
Dept. of Mathematics
University of California

Berkeley , CA 94720
USA

Dr. Radan Kucera
Dept. of Mathematics
University
Janackovo namesti 2a

662 95 Brno
CZECHOSLOVAKIA

Prof.Dr. Heinrich-Wolfg. Leopoldt
Mathematisches Institut II
Universität Karlsruhe
Kaiserstr. 12

7500 Karlsruhe 1

Klaus Künnemann
Mathematisches Institut
Universität Münster
Einsteinstr. 62

4400 Münster

Prof.Dr. Armin Leutbecher
Mathematisches Institut
TU München
PF 20 24 20, Arcisstr. 21

8000 München 2

Prof.Dr. Erich Lamprecht
Fachbereich 9 - Mathematik
Universität des Saarlandes
Bau 27

6600 Saarbrücken

Prof.Dr. Falko Lorenz
Mathematisches Institut
Universität Münster
Einsteinstr. 62

4400 Münster

Prof.Dr. Manohar L. Madan
Dept. of Mathematics
100 Mathematics Building
The Ohio State University
231 W. 18th Ave.

Columbus , OH 43210-1174
USA

Prof.Dr. Katsuya Miyake
Dept. of Mathematics
College of General Education
Nagoya University
Chikusa-Ku

Nagoya 464-01
JAPAN

Dr. Gunter Martin Malle
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368

6900 Heidelberg 1

Enric Nart
Dept. Matematiques
Universidad Autonoma de Barcelona

E-08193 Bellaterra, Barcelona Catalunya

Prof.Dr. B.Heinrich Matzat
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368

6900 Heidelberg 1

Prof.Dr. Jürgen Neukirch
Fakultät für Mathematik
Universität Regensburg
Universitätsstr. 31
Postfach 397

8400 Regensburg

Prof.Dr. Leon McCulloh
Department of Mathematics
University of Illinois
Altgeld Hall
1409, West Green Street

Urbana , IL 61801
USA

Dr. Olaf Neumann
Sektion Mathematik
Friedrich-Schiller-Universität
Jena
Universitätshochhaus, 17. OG.

DDR-6900 Jena

Prof.Dr. Tauno Metsänkylä
Institute of Mathematical Sciences
University of Turku

SF-20500 Turku

Prof.Dr. Robert W. K. Odoni
Dept. of Mathematics
University of Glasgow
University Gardens

GB- Glasgow G12 8QW

Prof.Dr. Hans Opolka
Institut für Algebra und
Zahlentheorie
TU Braunschweig
Pockelsstr. 14

3300 Braunschweig

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

8900 Augsburg

Prof.Dr. Albrecht Pfister
Fachbereich Mathematik
Universität Mainz
Postfach 3980
Saarstr. 21

6500 Mainz

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

6900 Heidelberg 1

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

6900 Heidelberg 1

Prof.Dr. Reinhard Schertz
Institut für Mathematik
Universität Augsburg
Universitätsstr. 8

8900 Augsburg

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

7750 Konstanz 1

Prof.Dr. Claus-Günther Schmidt
Mathematisches Institut II
Universität Karlsruhe
Kaiserstr. 12

7500 Karlsruhe 1

Dr. Hans-Peter Rehm
Mathematisches Institut II
Universität Karlsruhe
Kaiserstr. 12

7500 Karlsruhe 1

Prof.Dr. Rene Schoof
Mathematisch Instituut
Rijksuniversiteit te Utrecht
P. O. Box 80.010

NL-3508 TA Utrecht

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

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

8400 Regensburg

Prof.Dr. Kay Wingberg
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288/294

6900 Heidelberg 1

Peter Stevenhagen
Fakulteit Wiskunde en Informatica
Universiteit van Amsterdam
Plantage Muidergracht 24

NL-1018 TV Amsterdam

Prof.Dr. Zdzislaw Wojtkowiak
Max-Planck-Institut für Mathematik
Gottfried-Claren-Str. 26

5300 Bonn 3

Jörg Wildeshaus
Mathematisches Institut
Universität Münster
Einsteinstr. 62

4400 Münster

Prof.Dr. Ernst-Wilhelm Zink
Akademie der Wissenschaften
Karl-Weierstraß-Institut für
Mathematik
Mohrenstr. 39/Postfach 1304

DDR-1086 Berlin