MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

TAGUNGSBERICHT 33/1977

ALGEBRAISCHE ZAHLENTHEORIE

14.8. BIS 20.8.1977

Die in zweijährigem Turnus stattfindende Tagung über Algebraische Zahlentheorie stand wieder unter der Leitung von Herrn Professor Dr. H. Hasse und Herrn Professor Dr. P. Roquette. Professor Hasse konnte in seiner Einführung 62 Teilnehmer, darunter viele Kollegen aus dem westlichen und östlichen Ausland begrüßen. In dem reichhaltigen Tagungsprogramm wurden neue Ergebnisse aus der klassischen Zahlentheorie wie Einheiten- und Klassenzahlberechnung mitgeteilt, aber auch unter anderem über die moderneren Methoden (Nonstandard-, Kohomologie- und Modelltheorie in der Algebraischen Zahlentheorie) vorgetragen und diskutiert.

Teilnehmer

S. Agou, Lyon
H.-J. Bartels, Göttingen
S.A. Basarab, Bukarest
E. Becker, Köln
P. Bâyer, Barcelona
H. Benz, Köln
C.J. Bushnell, London
D.G. Cantor, Los Angeles
H. Cohn, New York
R.W. Davis, San Diego
P. Draxl, Bielefeld
G. Frey, Saarbrücken
A. Fröhlich, London
W.-D. Geyer, Erlangen
B. Gordon, Los Angeles
F. Halter-Koch, Essen
H. Hasse, Hamburg
H. Hazewinkel, Rotterdam
F.-P. Heider, Köln
W. Henn, Karlsruhe
G.M. Ikeda, Ankara
M. Jarden, Tel-Aviv
W. Jehne, Köln
E. Kani, Heidelberg
H.I. Karakas, Heidelberg
K. Kiyek, Paderborn

Gefördert durch DFG Deutsche Forschungsgemeinschaft

N. Klingen, Köln
S.V. Kotov, Minsk
K. Lakkis, Thessaloniki
H. Lang, Münster
H.W. Lenstra, Amsterdam
A. Leutbecher, München
P.A. Loeb, Urbana
F. Lorenz, Münster
M.L. Madan, Columbus
G. Martens, Erlangen
B.H. Matzat, Karlsruhe
E. Maus, Göttingen
C. Meyer, Köln
M. Neubrand, Bonn
J. Neukirch, Regensburg
Ch.J. Parry, Blacksburg
R. Perlis, Bonn
M. Pohst, Köln
G. Poitou, Orsay
A. Prestel, Konstanz
J. Ritter, Berlin
P. Roquette, Heidelberg
W. Scharlau, Münster
R. Schertz, Köln
A. Schinzel, Warschau
V. Schulze, Berlin
V. Sprindzuk, Minsk
H.-J. Stender, Köln
R.J. Stroeker, Rotterdam
H. Stützer, Köln
O. Taussky-Todd, Pasadena
W. Trinks, Karlsruhe
R.W. van der Waall, Nymegen
C.D. Walter, Dublin
G. Wicke, Münster
H.G. Zimmer, Saarbrücken

Vortragsauszüge

A. FRÖHLICH: Some new results on the Galois module structure of algebraic integers

N/K is a normal finite extension of number fields with $\Gamma = \mathrm{Gal}(N/K)$. The ring of integers of N is O_N. On assumes N/K to be tame. Thus O_N is locally free over the group ring $\mathbb{Z}[\Gamma]$ and defines an element $U_{N/K} = (O_N)$ in the class group $\mathrm{Cl}(\mathbb{Z}[\Gamma])$ of $\mathbb{Z}[\Gamma]$. The study of $U_{N/K}$ arose in the search for "approximate" normal integral basis theorems. A first main result on Galois module structure is that $U_{N/K}$ lies in the "kernel group" $D(\mathbb{Z}[\Gamma]) \subset \mathrm{Cl}(\mathbb{Z}[\Gamma])$. Let $W(N/K,\chi)$ denote the constant in the functional equation of the Artin L-functions, R_Γ the additive group of virtual characters. Define $W_{N/K}: R_\Gamma \to \{\pm 1\}$ by additivity and for irreducible χ by $W_{N/K}(\chi) = \begin{cases} W(N/K,\chi) & \text{if } \chi \text{ symplectic} \\ 1 & \text{otherwise} \end{cases}$. Write $V_{N/K} = (tW_{N/K})^{-1} U_{N/K}$ (t so that

$tW_{N/K} \in Cl(\mathbf{Z}[\Gamma]))$. Then: (A) Main conjecture: $V_{N/K} = 1$. Consequences of (A) are (B) $U^2_{N/K} = 1$; $U_{N/K} = 1$ if Γ has no irreducible symplectic characters. (C) $U_{N/K}\bar{U}_{N/K} = 1$; i.e. O_N is a stable self dual $\mathbf{Z}[\Gamma]$-Module (where $\bar{\ }$ is the involutory automorphism of $Cl(\mathbf{Z}[\Gamma])$ induced by complex conjugation).

Work by A.Fröhlich, Cassou-Noguès and M.Taylor has led to results of type:

(i) $U_{N/K}$ is in some canonical small subgroup;

(ii) (A), (B) have been proved for Abelian groups and for many other groups.

H. COHN: Rational Compositum-Genus for a Pure Cubic field

In nonabelian fields, to which genus theory does not ordinarily apply, many of the diophantine by-products could still be available. For instance, in pure cubic fields the representability of primes as norms is interrelated for all four subfields of the compositum $\mathbf{Q}(\sqrt[3]{m_\infty}, \sqrt[3]{m_o})$ particularly if only one prime $(=3t+1)$ divides $m_o m_\infty$. This is a generalisation of classic results on quadratic forms.

C. MEYER: Abzählung von Gitterpunkten in Tetraedern

Verschiedene Probleme der Zahlentheorie und der Differentialtopologie erfordern zu ihrer Behandlung explizite Formeln für die Anzahl der Gitterpunkte in dem Tetraeder T_n: $O < \frac{x_1}{a_1} + .. + \frac{x_n}{a_n} < 1$, $O \leq x_1, \dots, O \leq x_n$ des $\mathbf{R}^n$, wobei die a_i paarweise teilerfremde natürliche Zahlen sind. Der passende analytische Ansatz geschieht mittels des Dirichletschen diskontinuierlichen Faktors

$$\frac{1}{2\pi i} \int_L e^{\alpha s} \frac{ds}{s} = \begin{cases} 1 & \text{für } \alpha > O \\ 1/2 & \text{für } \alpha = O \\ O & \text{für } \alpha < O \end{cases}, \quad L \text{ Vertikale durch } \sigma_o > O.$$

Die genaue Ausführung liefert eine Darstellung der fraglichen Gitterpunktzahl durch ein Integral über einen unendlichen geschlossenen Weg. Dieses Integral ist dann nach dem Residuenkalkül berechenbar. Dabei spielen die Nörlundschen Polynome ein ausschlaggebende Rolle. In der Endformel treten als relevante Bestandteile neuartige Dedekindsche Summen des folgenden Typs auf:

$$S^{(n)}_{\nu;\sigma_1,\ldots,\sigma_n}(a_1,\ldots,a_n) := \sum_{\mu_1 \bmod a_1} \sum_{\mu_n \bmod a_n} P_\nu\left(\frac{\mu_1}{a_1}+\ldots+\frac{\mu_n}{a_n}\right) P_{\sigma_1}\left(\frac{\mu_1}{a_1}\right)\cdots P_{\sigma_n}\left(\frac{\mu_n}{a_n}\right),$$

wobei allgemein $P_k(x)$ die (periodische) k-te Bernoullische Funktion ist.

M. JARDEN: <u>Fields of finite corank</u>

Let K be a Hilbertian field. Denote by K_1 and $\tilde{K}$ the separable and the algebraic closure of K respectively, by G(K) the absolute Galois group of K. For every $(\underline{\sigma}) = (\sigma_1,\ldots,\sigma_e) \in G(K)^e$ we denote by $K_1(\underline{\sigma})$ the fixed field of $(\sigma_1,\ldots,\sigma_e)$ in K_1, by $\tilde{K}(\underline{\sigma})$ the maximal purely inseparable extension of $K_1(\underline{\sigma})$. There was given a survey on the properties of the fields $K_1(\underline{\sigma})$ and $\tilde{K}(\underline{\sigma})$ which hold for almost all $(\underline{\sigma})$ (in the sense of the Haar measure μ of G(K) with respect to the Krull topology), for example:

(I) Model theory: If K is finitely generated, then the theory of all elementary statements with coefficients in K that are true in $\tilde{K}(\underline{\sigma})$ is decidable.

(II) Density questions: If K is a countable Hilbertian field with an absolute value v, if w is an extension of v to $\tilde{K}$ and if V is an absolutely irreducible variety defined over $K_1(\underline{\sigma})$, then $V(K_1(\underline{\sigma}))$ is w-dense in $V(\tilde{K})$.

(III) Algebraic groups: If K is finitely generated and E is an elliptic curve over $\tilde{K}(\underline{\sigma})$, then $|E_{tor}(\tilde{K}(\underline{\sigma}))| \begin{cases} = \infty & \text{for } e = 1 \\ < \infty & \text{for } e > 1 \end{cases}$

(IV) Structure of the Galois group: Let K be Hilbertian. Then $\langle\underline{\sigma}\rangle = \hat{F}_e$. If $K \subseteq E \subset K_1(\underline{\sigma})$, then rank $G(E) > e$.

W.-D. GEYER: <u>Die Galoisgruppe von Durchschnitten lokaler Körper</u>

Ist $G = Gal(\bar{Q}/Q)$ und sind $G_1,\ldots,G_n$ Zerlegungsgruppen von Absolutbeträgen auf $\bar{Q}$, so ist die von $G_1,\ldots,G_n$ erzeugte Untergruppe in G nicht unbedingt ein freies Produkt. Für fast alle (im Sinne des Haarmaßes auf G) $(\underline{\sigma}) \in G^n$ gilt aber

$$\langle G_1^{\sigma_1},\ldots,G_n^{\sigma_n}\rangle = \coprod_{i=1}^{n} G_i^{\sigma_i} .$$

Das Ergebnis gilt für beliebige Hilbertsche Körper, sofern die

G_i separabel (im topologischen Sinne) sind.
Die Beweise benutzen eine Verträglichkeit des Hilbertschen Irreduzibilitätssatzes mit Approximationsforderungen, Lemmata von Sturm und Krasner sowie Jardens Methoden über den Umgang mit dem Haarschen Maß bei Galoisgruppen.

N. KLINGEN: Zahlkörper mit gleicher Primzerlegung

Es werden Zahlkörper K, K' untersucht, die in ihrem Primzerlegungsverhalten in bezug auf einen festen Grundkörper k übereinstimmen. Dabei unterscheidet man zwei Grade der Übereinstimmung: schwach: Kronecker-Äquivalenz; stark: arithmetische Äquivalenz. Es wurden einige Resultate berichtet:
(a) Bei beiden Äquivalenzbegriffen darf das Zerlegungsverhalten der Primideale für eine Menge der Dirichletdichte Null differieren. Es wird gezeigt, daß diese Ausnahmemenge leer ist.
(b) Es gibt Türme Kronecker-äquivalenter Körper von beliebig großer endlicher, aber keine von unendlicher Höhe.
(c) Für reine Erweiterungen und Erweiterungen von Primzahlgrad stimmen beide Äquivalenzbegriffe überein.

P.A. LOEB: Nonstandard measure spaces

A. SCHINZEL: Diophantine equations with parameters

A proof of the following theorem obtained jointly with D.J. Lewis is outlined:
Theorem: Let $F(x,y,t_1,\dots,t_r)$ be a polynomial with rational coefficients, quadratic with respect to x,y and $c(t_1,\dots,t_r)$ a non-zero polynomial. If for all integers $t_1,\dots,t_r$ such that $c(t_1,\dots,t_r) \neq 0$ the equation $F(x,y,t_1,\dots,t_r) = 0$ is soluble in rational integers x,y, then there exist rational functions $x(t_1,\dots,t_r)$, $y(t_1,\dots,t_r)$ such that $F(x(t_1..,t_r),y(t_1,..,t_r),t_1,..,t_r) = 0$ identically.
Some related conditional results are discussed.

O. TAUSSKY-TODD: Norms from quadratic fields and their relations to non commutating 2x2 matrices

Two facts concerning norms from quadratic fields arising from non commutating 2x2 rational matrices were observed:
(1) Let A be a rational 2x2 matrix with irrational eigen values α, α'. Let its transpose A' be obtained as $S^{-1}AS = A'$, S a rational 2x2 matrix. Then -det S is a norm from $\mathbf{Q}(\alpha)$.
(2) Let A be as above and B any rational 2x2 matrix $\neq 0$. Then -det(AB-BA) is a norm from $\mathbf{Q}(\alpha)$.
A number of further investigations linked to these facts have been obtained.

H.-J. STENDER: Ein formales Verfahren zur Herstellung parameterabhängiger Scharen von Grundeinheiten

Es wurde an eine kleine Arbeit von L. Bernstein und H. Hasse angeknüpft, in der aus einer lösbaren diophantischen Gleichung $u^k - mv^k = 1$, $k \geq 3$, Grundeinheiten quadratischer Ordnungen konstruiert werden. Es wurde gezeigt, daß sich dieses Verfahren einem allgemeinen unterordnet, nämlich aus lösbaren Gleichungen der Form $ax^n - by^n = c$ Einheitensysteme für reine Zahlkörper $K = \mathbf{Q}(\sqrt[n]{\frac{a}{b}})$ zu konstruieren.
Für n = 2,3,4,6 wurden hieraus explizit Basen der Einheiten- und Relativeinheitengruppen von K hergeleitet. Die Beweise hierzu stützen sich auf Arbeiten von Delaunay, Nagell, Ljunggren und Tartakowski. Eine Reihe früherer Ergebnisse lassen sich hier einordnen.

M. NEUBRAND: Über Einheitenberechnung in algebraischen Zahlkörpern mittels Betrachtung algebraischer Funktionen über $\mathbf{C}$

"z-Einheiten" eines algebraischen Funktionenkörpers $\mathbf{C}(z,w)$ sind die Einheiten des ganzalgebraischen Abschlußes von $\mathbf{C}[z]$ in $\mathbf{C}(z,w)$. Mittels Spezialisierung $z \to N \in \mathbf{Z}$ sollen Einheiten in Klassen algebraischer Zahlkörper gewonnen werden. Hierzu sind die Problemkreise (a) Existenz von z-Einheiten, (b) Möglichkeit der Spezialisierung zu untersuchen. Untersucht wurde dies an Funktionenkörpern mit definierender Gleichung $H(z,w) - bz^1 = 0$ mit $H(z,w)$ homogenes Polynom vom Grad $n > 1$. Ein Ergebnis ist, daß es in den Zahlkörpern des Typs $\mathbb{Q}(\sqrt[n]{D^n+d})$, $d \mid D^{n-1}$, außer den durch Bernstein und Stender bekannten Einheiten keine weiteren in geschlossener Form angebbaren gibt.

J. NEUKIRCH: Zetafunktionen und Etalkohomologie algebraischer Zahlkörper

Sei O_K der Ring der ganzen Zahlen eines total reellen Zahlkörpers K, $2 \neq \ell$ eine Primzahl, S die Menge der über ℓ liegenden Primideale von O_K und $X = \mathrm{Spec}(O_K)\setminus S$. Für eine étale Garbe F auf X werde die Kohomologie "mit kompaktem Träger" durch $H_c^q(X,F) = H_{et}^q(\mathrm{Spec}(O_K), j_!F)$ definiert, wobei $j_!F$ die Fortsetzung von F auf $\mathrm{Spec}(O_K)$ durch Null ist. Man betrachte die im Sinne von Tate n-fach getwisteten Garben $\mathbb{Z}/\ell^\nu(n)$, $n \in \mathbb{Z}$, und setze $H_c^q(X,\mathbb{Z}_\ell(n)) = \varprojlim_\nu H_c^q(X,\mathbb{Z}/\ell^\nu(n))$.
Die Werte der Dedekindschen Zetafunktion $\zeta_K(s)$ von K sind nach einem Satz von Siegel für $-s \in \mathbb{N}$ rationale Zahlen. Über ihre ℓ-Teile hat S. Lichtenbaum die Vermutung ausgesprochen, daß sie die étalkohomologischen Eulercharakteristiken des Schemas X sind. In einer etwas modifizierten Fassung lautet die Vermutung

$$(*) \qquad |\zeta_K(-n)|_\ell = \prod_{q=0}^{3} \# H_c^q(X,\mathbb{Z}_\ell(-n))^{(-1)^{q+1}} \quad \text{für } n \in \mathbb{N} \text{ und } \zeta_K(-n) \neq 0.$$

In diesem Vortrag wurde gezeigt, wie man diese Vermutung für alle ganzen rationalen Zahlen $n \equiv 1 \bmod [K(\mu_\ell):K]$, μ_ℓ ℓ-te Einheitswurzel, beweisen kann, wenn man die Zetafunktion $\zeta_K(s)$ durch eine Funktion $\zeta_I(s)$ ersetzt, von der vermutet wird, daß sie mit der Leopoldtschen ℓ-adischen Zetafunktion übereinstimmt.

P. BÁYER: Étal Euler characteristics of henselian rings

Let X be the spectrum of a henselian valution ring with residue field k of $q = p^d$ elements. Let $x = \mathrm{Spec}(k)$ be the closed point of X. Given a constructible locally free $\mathbb{Q}_\ell$-sheaf F over X_{et}, one defines the zeta function of X with respect to F by the formula

$$\zeta_F(s) = \frac{1}{\det(1-\varphi_{\bar{x}}^{-1}q^{-s};\ F_{\bar{x}})},$$

where $F_{\bar{x}}$ notes the fibre of F in a geometric point $\bar{x}$ over x, and $\varphi_{\bar{x}}:F_{\bar{x}} \to F_{\bar{x}}$ is the Frobenius automorphism. If $\ell \neq p$ and if n, n+1 are not eigenvalues of $\varphi_{\bar{x}}$, then the analogy of the Lichtenbaum conjecture (*) (see preceding abstract) is true.

B. H. MATZAT: Zur Konstruktion von Funktionen- und Zahlkörpern mit vorgegebener Galoisgruppe

Es wurde eine obere Schranke für den Grad des Definitionskörpers $k/\mathbb{Q}$ eines Funktionenkörpers K/R, $R:= \mathbb{C}(t)$, angegeben, in die nur Eigenschaften der Galoisgruppe Gal(K/R) und der Verzweigungspunkte von K/R eingehen.
Diese Schranke gestattet in gewissen Fällen (S_n; A_n; PGL(2,p) und PSL(2,p) für $p \not\equiv \pm 1 \bmod 24$; $P\Gamma L(2,q)$ für $q = 8,9,16$; PGL(2,9); PSL(3,3);...) Funktionenkörper und damit auch Zahlkörper mit den entsprechenden Galoisgruppen über $\mathbb{Q}(t)$ bzw. $\mathbb{Q}$ nachzuweisen, in anderen Fällen erhält man unter Verwendung dieser Gradabschätzung den genauen Definitionskörper (z.B. $\mathbb{Q}(\sqrt{-11})$ für die beiden M_{11}-Körper über R mit minimalem Geschlecht g = 631). Gleichungen für diese Körper können (im Prinzip) berechnet werden. Beispiele hierfür wurden angegeben.

S. AGOU: Polynômes Hyponormaux sur un corps fini

Un polynôme $u(x) \in \mathbb{F}_q[x]$ est dit hyponormal sur $\mathbb{F}_q$, s'il existe une racine x_o de u(x) telle que pour toute racine x de u(x) on ait $\mathbb{F}_q(x_o) \subseteq \mathbb{F}_q(x)$.
L'exposé montrait comment cette notion permet d'étudier les polynômes $f(x^{p^r}-ax)$ sur un corps fini $\mathbb{F}_{q^s}$, où f(x) est irréductible dans $\mathbb{F}_{p^s}[x]$.
Comme conséquence, on en déduit des conditions explicites pour l'irréductibilité des polynômes $f(x^{p^r}-ax)$ sur $\mathbb{F}_{p^s}$.

V.G. SPRINDZUK: Diophantine equations and class numbers

According a well known conjecture of Gauss there is an infinite sequence of real quadratic fields with class number 1. There were given theorems which go in the opposite to Gauss' conjecture.

Theorem: Let $2 \leq k \in \mathbb{N}$, D_m and h_m the dicriminant and class number of $\mathbb{Q}(\sqrt{m^{2k}-1})$ with $2 \leq m \in \mathbb{N}$, then

$$D_m > c_2 (\log m)^{\frac{\tau(2k)}{12} - \delta(k) - \varepsilon} \quad , \quad h_m > c_3 \cdot D_m^{\frac{1}{2} - \frac{12}{\tau(2k) - \delta_1(k)} - \varepsilon} \, ,$$

where τ= number of all divisors, $\delta_1(k) = 12\delta(k)$, $c_i = c_i(k,\varepsilon) > 0$, $\varepsilon > 0$, $\delta(k) = \frac{1}{6}$ if $2 \nmid k, 3 \nmid k$; $= \frac{3}{16}$ if $2 | k, 3 \nmid k$; $= \frac{7}{24}$ if $2 | k, 3 | k$; $= \frac{5}{24}$ if $2 \nmid k, 3 | k$.

The same holds for the sequence of the fields $\mathbb{Q}(\sqrt[t]{m^{tk}-1})$ with $t = 3,4,6$. An analogue is true for the fields of Ankeny-Brauer-Chowla.

G. POITOU: <u>Neue Diskriminantenabschätzungen</u>

Es wurde eine Ungleichung bewiesen für total imaginäre Zahlkörper:

$$\frac{1}{n} \cdot \log|d| \geq \max_{y>0} \{\gamma + \log 4\pi - \frac{12\pi}{n\sqrt{y}} - L_1(y)\} \, ,$$

mit n = Körpergrad, d = Diskriminante, γ = Eulersche Konstante, $L_1(y) = L(y) + \frac{1}{3} \cdot L(\frac{y}{3^2}) + \frac{1}{5} \cdot L(\frac{y}{5^2}) + \ldots$. $L(y)$ ist eine elementare Funktion, deren Reihenentwicklung für $|y| \leq \frac{1}{4}$ konvergiert.
Aus dieser Ungleichung lassen sich leicht Tafeln berechnen.
Ein Beispiel: $n=8$, $y=1{,}7242$, $L_1(y)=0{,}657172\ldots$, $\sqrt[8]{|d|} \geq 5{,}659\ldots$
Herr Lenstra hat bemerkt, daß ein Körper mit der Diskriminante $2^8 17^3$ existiert, also mit $\sqrt[8]{|d|} = 5{,}786\ldots$.

M. POHST: <u>Regulatorabschätzungen für total reelle algebraische Zahlkörper</u>

Ist n der Körpergrad, so bildet man eine geeignete (n-1)-äre positiv definite quadratische Form Q, deren Determinante gerade das n-fache des Quadrats des Regulators R ist. Aus der Geometrie der Zahlen folgt dann: $\operatorname{Min} Q \leq \gamma_{n-1} (\det Q)^{1/(n-1)}$, γ_{n-1} Hermitesche Konstante. Es genügt daher, das Minimum von Q nach unten abzuschätzen, um eine untere Schranke für den Regulator R zu erhalten. Dieses Problem läßt sich als Extremalproblem mit Nebenbedingungen aufbauen und lösen. Die Nebenbedingungen ergeben sich dabei aus den Eigenschaften der Einheiten des zugrunde liegenden Körpers. Beispiele zeigen die Vorteile dieses Verfahrens gegenüber bekannten

Methoden. Als Spezialfall erhält man u.a. die Abschätzung

$$R \geq \left(\frac{1}{n}\left(\frac{\log^2 \frac{1+\sqrt{5}}{2}\, n}{\gamma_{n-1}}\right)^{n-1}\right)^{1/2} .$$

Im übrigen lassen sich auf dem gleichen Weg auch Abschätzungen für komplexe Körper gewinnen, deren Qualität allerdings schlechter ist. Sie ist jedoch immer noch besser als die bisher bekannten unteren Schranken für R.

H.-J. BARTELS: Definite arithmetische Gruppen

$G \subset GL_n$ bezeichne eine über $\mathbb{Q}$ definierte Untergruppe der allgemeinen linearen Gruppe, $K/\mathbb{Q}$ sei totalreell mit Maximalordnung O_K. G sei definit über K in dem folgenden Sinn: $\prod_{v \in S_\infty(K)} G(K_v)$ ist kompakt.

Problem: Wann gilt (*) $G(O_K) = G(\mathbb{Z})$?

(*) ist z.B. richtig für beliebige totalreelle abelsche Erweiterungen $K/\mathbb{Q}$. Die Gleichheit (*) hat dann Konsequenzen:

1. für die Galoiskohomologie der definiten arithmetischen Gruppe $G(O_K)$ und
2. für das Verhalten definiter quadratischer $\mathbb{Z}$-Gitter bei totalreellen Skalarerweiterungen.

Hier besteht ein Zusammenhang mit neueren Resultaten von Y. Kitaoka.

S.V. KOTOV: Über die arithmetische Struktur der rationalen Punkte auf den elliptischen Kurven

Sei F(x,y) ein absolut irreduzibles Polynom vom Grad $n \geq 3$ mit ganzen rationalen Koeffizienten und die Kurve F(x,y) = 0 vom Geschlechte Eins. Wir betrachten auf der Kurve F(x,y) = 0 rationale Punkte der Form

$$(*) \qquad x = \frac{\tilde{x}}{p_1^{z_1} \cdots p_s^{z_s}}, \quad y = \frac{\tilde{y}}{p_1^{z_1'} \cdots p_s^{z_s'}},$$

wobei $\tilde{x},\tilde{y} \in \mathbb{Z}$ und $p_1,\ldots,p_s$ Primzahlen sind mit $ggT(\tilde{x},\tilde{y},p_1 \cdots p_s) = 1$.

Satz: Sei F(x,y) wie oben, habe (x,y) auf der Kurve F(x,y) = 0 die Form (*) und sei $P = \max_i\{p_i\}$, $1 \leq i \leq s$, dann gilt

W. HENN: Über die Automorphismengruppe von Funktionenkörpern einer Variablen

K/Ω sei algebraischer Funktionenkörper vom Geschlechte $g > 1$, algebraisch abgeschlossen mit $\mathrm{char}(\Omega) = p$. Weiter sei $G = \mathrm{Aut}(K/\Omega)$. Für $\Omega = \mathbb{C}$ beweist Hurwitz 1893 die Abschätzung $|G| \leq 84(g-1)$, für beliebiges Ω zeigt H.L.Schmid 1939, daß G endlich ist.

Satz: Es gilt

$$(*) \qquad |G| \leq 3\cdot(2g)^{5/2}$$

bis auf 4 Ausnahmeserien. Die Serie mit relativ zu g maximalem $|G|$ $(>16g^4)$ bilden die unitären Fermatkörper (Leopoldt 1970) $K = \Omega(x,y)$, $x^n+y^n+1 = 0$, $n-1=p^s$ mit $G \cong PGU(3,p^{2s})$.
Zum Beweis studiert man den Verzweigungstyp von K/K^G und die Stuktur der Verzweigungsgruppen und erhält mit der Hilfe der Relativgeschlechtsformel die Abschätzung (*) bis auf einen "kritischen Fall", in dem aber die dann noch möglichen Gruppentypen klassifiziert sind. Der Versuch, ein Modell zu diesen Gruppen zu konstruieren, führt dann zu den vier Ausnahmeserien.

S.A. BASARAB: Some model theory for henselian valued field

Some problems concerning the completeness and the model-completeness of the first order theories of some classes of henselian valued fields having a finite absolute ramification index $e \geq 1$, as well as other connected problems, e.g. the model-companions and the model-completions of the theories of some classes of valued fields are considered.
In the last section some applications in arithmetic and approximation theory are given.

R. PERLIS: Class numbers of arithmetically equivalent fields

Let K and K' be two algebraic number fields with the same zeta functions $\zeta_K(s) = \zeta_{K'}(s)$. The following theorems were discussed, with exemples:

1. A natural number ν is defined whose prime divisors lie among the divisors of the degree $[N:K]$, where N is the normal closure of K. For $p \nmid \nu$ we have for the p-Sylow-group of the class group

$$P > c \cdot \ln \ln X ,$$

wobei $X = \max\{|\tilde{x}|, |\tilde{y}|\}$, $c > 0$ nur von $F(x,y)$ abhängt und effektiv bestimmt ist.

G. FREY: Torsionspunkte elliptischer Kurven

Mit Hilfe der Reduktionstheorie von Néron und der Theorie der Tate-Kurven wurden notwendige Bedingungen für die Existenz von Torsionspunkten elliptischer Kurven E/K, die rational über K sind, hergeleitet, falls K eine nichtarchimedische Rang-Eins-Bewertung besitzt. Diese lokalen Ergebnisse lassen sich global anwenden, um z.B. über $\mathbb{Q}$ alle elliptischen Kurven mit ganzer j-Invariante und mit rationalen Torsionspunkten zu bestimmen und um für globale Körper zu beweisen:

Satz: Zu $0 \neq j \in K$ gibt es nur endlich viele elliptische Kurven E mit $j(E)=j$ und $P \in E(K)$ der Ordnung > 2.

Weiter sieht man, daß, falls die Ordnung von P "groß genug" ist, E in allen Stellen semistabile Reduktion haben muß. Für $K = \mathbb{Q}$ sind diese Betrachtungen eine Vorarbeit, um das Theorem von Mazur zu beweisen: $|E(\mathbb{Q})_{tor}| \leq 12$.

H.G. ZIMMER: Quasifunktionen auf elliptischen Kurven über bewerteten Körpern

Die Néron-Tate-Höhe auf der rationalen Punktgruppe einer elliptischen Kurve über einem globalen Körper ist eine quadratische Form, die sich als Limes der Weil-Höhe schreiben läßt. Bei dieser Konstruktion spielt die Produktformel eine wichtige Rolle. Problem: Läßt sich eine Néron-Tate-Höhe, die "fast" eine quadratische Form ist, für einen nicht notwendig der Produktformel genügenden Körper definieren? Hierzu kann man sich auf eine elliptische Kurve über einem beliebigen bewerteten Körper beschränken. Tate hat Existenz und Eindeutigkeit einer solchen Höhe, die nach Néron Quasifunktion heißt, angekündigt und in Spezialfällen explizit angegeben. Es zeigt sich, daß die Néron-Tate-Höhe auch in der "lokalen" Situation als Limes einer Funktion darstellbar ist.

$$Cl_K^{(p)} \cong Cl_{K'}^{(p)} .$$

2. Let $n = [K:Q]$ and $r=r_1+r_2-1$ the unit rank of K. Then is valid for the class numbers

$$h_K/h_{K'} \leq (n\cdot[\tfrac{n+1}{2}])^r .$$

J. RITTER: Lokale Körper mit isomorphen absoluten Galoisgruppen

Sei K endliche Erweiterung von Q_p mit absoluter Galoisgruppe G_K. Durch das Studium der maximal abelschen Erweiterungen von K zu geeigneten Exponenten gewinnt man aus G_K die Kenntnis folgender Daten: $m = [K:Q_p]$, f=Restklassengrad, $r=\max\{i \mid \zeta_{p^i} \in K\}$, $\tilde{r}=\max\{j \mid \zeta_{p^j} \in K_{tr}$ = max. zahm verzweigte Erweiterung von K$\}$. Ist noch $r\geq 1$, so kann man mit Hilfe von Ergebnissen von Uchida die Zahl s, definiert durch $\zeta_{p^{\tilde{r}}}^{\sigma} = \zeta_{p^{\tilde{r}}}^{s}$ (σ ein Frobeniusautomorphismus), abgelesen werden. Nun läßt sich ein Kriterium für Körper L angeben, wann $G_K = G_L$ ist; hierbei gehen Resultate von Jakovlev über die Struktur von G_K ein:
<u>Satz:</u> Sei $r\geq 1$, $\tilde{r}-r=i$. Dann existiert genau ein über Q_p abelscher Körper $B\subseteq K$ mit $[B:A] = p^i$ mit U=unverzweigte Teilerweiterung von K, $A = U(\zeta_{p^r})$. Genau dann gilt $G_K \cong G_L$, wenn <u>1</u>. L rein verzweigt über B vom Grad $[K:B]$ ist und <u>2</u>. $p \nmid [L\cap Q_p^{ab}:B]$.

B. GORDON: Division rings with prescibed maximal subfields

Suppose $K \subset L$ are algebraic number fields. We say that L is K-adequate if L is a maximal subfield of a finite dimensional division algebra D with center K. A finite group is called K-admissible if G is the Galois group of a normal K-adequate extension L/K. Among other things, the following were shown:

1. S_n is Q-admissible $\Longleftrightarrow$ $n\leq 5$; A_n is not Q-admissible if $n\geq 8$;
2. A_2, A_3, A_4 are K-admissible for every number field K;
3. A_5 is K-admissible, if $\sqrt{-1} \notin K$ or if $\exists$ prime ideals $\mathfrak{z}_1 \neq \mathfrak{z}_2$ of K lying over (2), whose residue degrees are even;
4. If G is admissible for every K, then the Sylow groups of G are abelian and generated by ≤ 2 elements;
5. any metacyclic nilpotent group is Q-admissible.

M. HAZEWINKEL: <u>Twisted Lubin-Tate formal group laws, ramified Witt vectors and Artin-Hasse exponential mappings</u>

For any ring R let $\Lambda(R)$ denote the multiplicative group of power series of the form $1+a_1t+\ldots$ with coefficients in R. The Artin-Hasse exponential mappings are homomorphisms $W_{p^\infty}(k) \to \Lambda(W_{p^\infty}(k))$ which satisfy certain additional properties. There was given a generalisation with $W_{p^\infty}(k)$ replaced by rings of Witt vectors associated to a (global) twisted Lubin-Tate formal group law and Λ replaced by the curve functor of that global formal group law. The Witt-vector-like A-algebra functor $W^F_{q^\infty}(-)$ associated to the twisted formal A-module F satisfies $W^F_{q^\infty}(\ell) \simeq B$ if B is an unramified extension of A with residue field ℓ. Here A is the ring of integers of a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$. Whence the name "ramified-Witt-vectors" for $W^F_q(-)$.

R. SCHERTZ: <u>Erzeugung von Ringklassenkörpern über imaginär-quadratischen Körpern durch singuläre Werte der Δ-Funktion</u>

Sei Σ ein imaginär-quadratischer Zahlkörper. Für $f\in\mathbb{N}$ sei Ω_f der Ringklassenkörper mod f über Σ. Untersucht man Klassenzahl und Einheitengruppe der Teilkörper von Ω_f mit den Methoden der komplexen Multiplikation, so spielen dabei vielfach Quotienten der Form $\Delta(\mathfrak{a})/\Delta(\mathfrak{b})$ eine Rolle, wobei $\mathfrak{a}$ und $\mathfrak{b}$ zur Ordnung mit dem Führer f in Σ gehörige Ideale sind und Δ die Diskriminante aus der Theorie der Modulfunktionen bedeutet. Diese Quotienten liegen bekanntlich in Ω_f, jedoch ist bisher noch nicht geklärt, ob sie Ω_f über Σ erzeugen. Durch Betrachtung von L-Funktionen zu Ringklassenkörpern in Σ kann man diese Frage positiv beantworten.

C.D. WALTER: <u>A class number relation in Frobenius extensions of number fields</u>

Let K/k be a normal extension of number fields whose Galois group is a metacyclic Frobenius group G with kernel N and complement F. For exemple this situation occurs for the extension $k(\sqrt[p]{a},\sqrt[p]{1})/k$ for an odd prime p, $[k(\sqrt[p]{a}):k] = p$, $\sqrt[p]{1}\notin k$.

Let $h(H)$ be the class number of the field fixed by the subgroup H, and $\mathfrak{b}(H)$ that part of its class group consisting of classes with orders prime to $n = |N|$. Then for $f = |F|$

$$\mathfrak{b}(1)/\mathfrak{b}(N) \cong \bigoplus_{i=1}^{f} \mathfrak{b}(F)/\mathfrak{b}(G) \qquad \text{and}$$

$$h(1)/h(N) = (h(F)/h(G))^{f} Qn^{-A}$$

for an explicit number A depending on the rank of the unit groups and Q a certain unit index.

C.J. BUSHNELL: Distribution in Galois orbits

Fröhlich has shown that, for many finite groups Γ, if $F/\mathbf{Q}$ is tame and Galois with $\Gamma = \mathrm{Gal}(F/\mathbf{Q})$, then $F/\mathbf{Q}$ has a normal integral basis: there is an $a \in O_F$ such that $a \cdot \mathbf{Z}[\Gamma] = O_F$. The set of all $a \in F$ with this property constitute an orbit of the action of the group $\mathbf{Z}[\Gamma]^{\times}$ on F. One knows very little about the numbers a. So one seeks theorems about the growth of the norms $N_{F/\mathbf{Q}}(b)$ for $b \in a \cdot \mathbf{Z}[\Gamma]^{\times}$, for example of the type $|\{x \in \mathbf{Z}[\Gamma]^{\times} \mid |N_{F/\mathbf{Q}}(a \cdot x)| < M\}| < \infty$.
One can show that, when $x \mapsto |N_{F/\mathbf{Q}}(a \cdot x)|$, $x \in \mathbf{Q}[\Gamma]$, is extended to a function on $\mathbf{R}[\Gamma]$, and then averaged over a maximal compact subgroup of $\mathbf{R}[\Gamma]^{\times}$, it "usually" (in some sense) grows at the rate one would expect.

H. LANG: Über die Klassenzahl der Ringklassenkörper mit einem reell-quadratischen Grundkörper

K sei imaginärer Ringklassenkörper über dem reell-quadratischen Grundkörper k und K_o sein größter reeller Teilkörper. Für den Quotienten $h(K)/h(K_o)$ der Klassenzahlen besteht eine Formel, in der als wesentliche Bestandteile Werte $L(1,\mathfrak{k})$ von erweiterten Ringklassen-L-Funktionen auftreten. Mit $d(k)$ = Diskriminante von k hat man: $\psi(\mathfrak{k}) = 6f\sqrt{d(k)}\,\pi^{-2}L(1,\mathfrak{k}) \in \mathbf{Z}$. Genaue Kenntnis dieser Zahlen $\psi(\mathfrak{k})$ führt zu Aussagen der Form:
Sei der maximale absolut-abelsche Teilkörper L von K auch imaginär und L_o der größte reelle Teilkörper von L. Wenn $d(k)$ kein Produkt aus positiven Primdiskriminanten ist, gilt für die Klassenzahlen

$$\frac{h(K)\cdot h(L_o)}{h(K_o)\cdot h(L)} \in \mathbf{N}\ .$$

E. KANI: The Theorem of Mordell-Weil via Nonstandard Methods

Let F be a function field of one variable with constant field a number field K. The Theorem of Mordell-Weil states that the group $C_o(F/K)$ is a finitely generated group.
One of the main ingredients of the proof is the construction of a quadratic form (called the Tate Height) on $C_o(F/K)$ with certain properties. This is usually done by the methods of algebraic geometry. It is possible to use the methods of "Nonstandard Algebra" (cf. e.g. A.Robinson-P.Roquette: The Finiteness Theorem of Siegel-Mahler, J.N.Th.7(1975)) to construct such a form with the same properties. This is done by suitably generalizing Weil's quadratic form σ defined on the ring of correspondences on an algebraic curve as well as the Theorem of Castelnuovo-Severi.

H.W. LENSTRA: The algebraic closure of two

J.H. Conway proved (in "On numbers and games") that the class of ordinal numbers is turned into an algebraically closed field of characteristic 2 by following inductive definitions of "+" and "$\cdot$": $a+b$ is the least ordinal number distinct from all $a'+b$, $a+b'$; $a\cdot b$ is the least ordinal distinct from all $(a'b+ab')+a'b'$, where, in each case, a',b' range over all ordinals $<a$ and $<b$, respectively. It is easy to compute sums, but for products this problem has been solved only for a certain beginning segment of the ordinal numbers. Thus, it is possible to calculate with ordinals smaller than $\omega^{\omega^{\omega}}$, which forms an algebraic closure of the prime subfield $2=\{0,1\}$; here we identify each ordinal with the set of previous ones. The result can be extended to $\lim_{n} \underbrace{\omega^{\omega^{\cdot^{\cdot^{\omega}}}}}_{n}$, which turns out to be a field isomorphic to the quadratic closure of the field of rational functions in one varialbe over $\omega^{\omega^{\omega}}$.

W. TRINKS: Der Satz von Euler und Lagrange über die Periodizität von Kettenbrüchen

Sei K endlich-algebraischer Zahlkörper, Σ endliche Menge von Primstellen von K, worin die unendlichen enthalten sind, $\mathbf{A} := \prod_{p\in\Sigma} K_p$ (Komplettierungen), $\mathcal{W} := \{\alpha\in K \mid \forall p\notin\Sigma : |\alpha|_p \leq 1\}$, K sei diagonal in $\mathbf{A}$ eingebettet

und A als K-Algebra aufgefaßt. Ferner sei $\|\xi\| := \max_{p\in\Sigma} |\xi|_p$ für $\xi\in A$. Dann gilt: Ist $\mathcal{W}$ Hauptidealring, so ist folgender Algorithmus ($\xi_o := \xi$, $\xi_{n+1} := \xi_n'$) periodisch für genau solche $\xi\in A$, für die $L=K(\xi)$ eine quadratische Erweiterung ist. Algorithmus:
$0<\varepsilon<1$ sei gegeben, $C_1, C_2, \ldots$ eine Aufzählung der Elemente $C\in\mathcal{W}$. $D_i\in\mathcal{W}$ werde so gewählt, daß $\|C_i\xi+D_i\|$ minimal ist. (C_*, D_*) sei dasjenige Paar (C_i, D_i) mit minimalem i, das erfüllt: $[\|C_i\xi+D_i\|\leq\varepsilon$ und $ggT(C_i,D_i)=1]$, ein solches Paar existiert immer. Dazu wähle man $A_*, B_*\in\mathcal{W}$ so, daß $A_*D_*-B_*C_*$ eine 1-Wurzel ist; $\|A_*\|$ minimal unter allen solchen (A_*, B_*).
Dann sei $\xi' := \dfrac{A_*\xi+B_*}{C_*\xi+D_*}$. Ergebnis: Aus den Perioden erhält man ein System von L/K-Relativ-Σ-Einheiten maximalen Ranges. Ein passendes Σ erhält man für alle relativ-reellquadratischen L/K, wo L nicht im Hilbertschen Klassenkörper von K liegt.

C.J. PARRY: Real quadratic fields with class numbers divisible by 5

Conditions were given for a real quadratic field to have class number divisible by five. If 5 does not divide m then a necessary condition for 5 to divide the class number of the real quadratic field with conductor m or 5m is that 5 divide the class number of a certain cyclic biquadratic field with conductor 5m. Conversely, if 5 divides the class number of the cyclic field then either one of the quadratic fields has class number divisible by 5 or one of their fundamental units satisfies a certain congruence condition modulo 25.

E. BECKER: Summen n-ter Potenzen in Körpern

Im folgenden sei K ein Körper der Charakteristik Null.
Satz: Zu $r,n,m \in \mathbb{N}$, n gerade, gibt es $s = s(n,m,r)\in\mathbb{N}$ mit

$$\bigwedge_{K}\ \bigwedge_{x_1,\ldots,x_r\in K}\ \bigvee_{y_1,\ldots,y_s\in K}\ \left(\sum_{i=1}^{r} x_i^n\right)^m = \sum_{j=1}^{s} y_j^{nm}.$$

Korollar: Es gibt $F_1,\ldots,F_s \in \mathbb{Q}(X_1,\ldots,X_r)$ mit

$$(X_1^n+\ldots+X_r^n)^m = \sum_{j=1}^{s} F_j(X_1,\ldots,X_r)^{nm}.$$

Der Fall n=2 ist von Hilbert (1909) behandelt worden, hierbei sind die F_i als Linearformen wählbar. Für $n \geq 4$ sind nicht alle F_i Polynome.
Der Beweis verwendet Harrison-Primstellen, Bewertungstheorie, Kompaktheitssatz der Modelltheorie. Letzterer Satz ergibt die Unabhängigkeit der oberen Schranke s von K, $x_1,\dots,x_r$.
Als weitere Konsequenzen der Methode wurden erwähnt:
1. $-1 = \sum x_i^2$, so auch $-1 = \sum y_j^n$ für n gerade.
2. K algebraischer Zahlkörper. Dann gilt $\{\sum x_i^2\} = \{\sum y_j^n\}$, n gerade.

R.W. VAN DER WAALL: The conductor of the quadratic residue symbol revised

A short talk was given about the pages 106-110 of Hasse's "Vorlesungen über Zahlentheorie", explicitly on the notions of Erklärungsmodul and conductor. The pages are in fact the first occasions where they are defined. Some inaccuracies were repared.

W. Henn, Karlsruhe