Mathematisches Forschungsinstitut
Oberwolfach

Tagungsbericht

Algebraische Zahlentheorie

vom 31.7. - 6.8.1967

Unter der Leitung von Herrn Professor Dr. Hasse (Hamburg) und Herrn Professor Dr. Roquette (Heidelberg) fand in Oberwolfach vom 31.7. bis 6.8. eine Tagung über Algebraische Zahlentheorie statt. Die zahlreichen Teilnehmer kamen aus verschiedenen Ländern, aus Frankreich, Großbritannien, Griechenland, Kanada, Niederlanden, Polen, Schweden, Schweiz, Vereinigten Staaten und Deutschland. Es wurde ein weites Spektrum interessanter Vorträge geboten. Im Mittelpunkt des Interesses standen die Vorträge von Brumer, Holley und Pfister, in denen jeweils klassische, seit längerer Zeit ungelöste wichtige Fragen ihre Beantwortung fanden.

Teilnehmer:

Ayoub, R., Frankfurt
Barner, K., Stuttgart
Behr, H., Göttingen
Benz, H., Hamburg
Brückner, H., Hamburg
Brumer, A., Paris
Cassels, J.W.S., Cambridge
Eichler, M., Basel
Geyer, W.D., Heidelberg
Guthschmidt, N., Berlin
Hooley, Ch., Durham
Kubota, T., Nagoya
Kuipers, L., Delft
Jacobinski, H. Vendelsö
Jehne, W., Köln
Lakkis, K., Athen
Leopoldt, H.W., Karlsruhe
Lutz, Elisabeth, Grenoble
Martinet, J., Grenoble
Maus, E., Hamburg
Menalda, A. Leiden
Merriman, J.R., Oxford
Meyer, C., Köln
Miller, L., Göttingen
Neukirch, J., Bonn
Pfister, A., Göttingen

Ribenboim, P., Kingston
Schinzel, A., Warschau
Sonn, J., Göttingen
Tamme, Hamburg
de Vreugd, C., Leiden
van der Wall, Leiden
Wilson, R., London
Zassenhaus, H.J., Worthington/Ohio
Zimmer, H.G., Tübingen

Kurzfassungen der 19 gehaltenen Vorträge
Reihenfolge, in der sie gehalten wurden.

H. ZASSENHAUS: Über die Äquivalenz ganzzahliger Darstellungen

Sei k ein algebraischer Zahlkörper, A eine zentraleinfache Algebra endlicher Dimension über k, also $A = D^{f \times f}$ mit einem Schiefkörper D. Sei o ein dedekindscher Ring mit Quotientenkörper k, R eine o-Ordnung von A, die in einer Maximalordnung R_1 enthalten sei. Wir betrachten o - torsionfreie, endlich erzeugte R-Moduln M, M'. Sie zerfallen in unzerlegbare R - linksideale, die Anzahl der Summanden heißt der Rang. Wie im kommutativen Fall läßt sich auch hier eine Steinitzklasse (Idealklasse modulo Normen von Hauptidealen) definieren.

Satz 1: Ist $R = R_1$ und $f > 1$ oder Rang $M > 1$, so sind M, M' genau dann äquivalent, wenn sie gleichen Rang und Steinitzklasse haben.

Satz 2: Ist $R_1 M = R_1 M'$ und $f > 1$ oder Rang $M > 1$, so sind M, M' genau dann eigentlich äquivalent, wenn sie in allen Lokalisierungen eigentlich äquivalent sind.

Zum Beweis wird der Approximationssatz für Normeinseinheiten verwendet.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

HOOLEY, Ch.: Artins Vermutung über Primitivwurzeln

In diesem Vortrag wurden Vermutungen von Artin aus dem Jahre 1927 auf die Riemannsche Vermutung für die Dedekindsche Zetafunktion und L-Reihen zurückgeführt.

Die Vermutungen von Artin:

1. Die ganze Zahl a ist für unendlich viele Primzahlen p Primitivwurzel modulo p, falls a kein volles Quadrat und $a \neq 1$ ist.
2. N(x) sei die Anzahl obiger Primzahlen kleiner x, dann gilt asymptotisch $N(x) \sim A(a) \cdot x/\log x$, wobei A(a) eine positive Konstante ist.

2.) impliziert 1.). Es wird 2.) bewiesen, indem man von einer asymptotischen Formel für die Dedekindsche Zetafunktion zu gewissen Kummerkörpern ausgeht. Der Autor verwendet Siebmethoden. Die der Aussage in (2.) entsprechende Summe wird in vier Summen aufgeteilt und die einzelnen Summen nach verschiedenen Methoden abgeschätzt. Der Wert der Konstanten A(a) ergibt sich in Übereinstimmung mit einer Vermutung von Heilbronn.

KUBOTA, T.: Über L-Reihen und Gaußsche Summen

Es werden zu einem Charakter einer diskontinuierlichen Gruppe Eisensteinsche Reihen erklärt. Diese Reihen genügen einer Funktionalgleichung. Weiter werden ihre Fourierentwicklungen untersucht. Diese funktionentheoretischen Ergebnisse werden auf den Fall der Hilbertschen Modulgruppe eines totalimaginären Zahlkörpers angewendet. Dabei wird weiter vorausgesetzt, daß es sich um einen abelschen Charakter handelt, dessen Kern keine Kongruenzuntergruppe ist. Aus den nichtkonstanten Gliedern der Fourierentwicklungen der Eisensteinschen Reihe erhält man dann einen neuen Typ von Zetafunktionen. Die Koeffizienten dieser Zetafunktionen sind Gaußsche Summen. Im allgemeinen haben diese Funktionen keine Produktentwicklung. Zur Bestimmung der Residuen wird das Reziprozitätsgesetz für die n-ten Potenzreste benutzt. Als ein weiteres Ziel der Untersuchung nannte der Vortragende, diese Residuenbestimmung unabhängig vomReziprozitätsgesetz zu gewinnen, um eventuell daraus das Reziprozitätsgesetz abzuleiten.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

BRÜCKNER, H.: Eine explizite Formel für das p^n-te Normrestsymbol

Über einem p-adischen Körper k, der die primitive p^n-te Einheitswurzel ξ enthalte, sei die Algebra $k[u,v]$ mit $u^{p^n} = a, v^{p^n} = b$, $(a, b \in k^x)$, $uv = \xi\, vu$ gegeben. Die Invariante (a,b) dieser Algebra ist in speziellen Fällen von Artin und Hasse (1928), allgemein von Safarevic (1950) angegeben worden. Die vorgetrageneFormel ist expliziter als die von Safarevic und als Analogon zu der (einfachen) Formel von H.L. Schmid - E. Witt für den charakteristikgleichen Fall anzusehen.

BEHR, H.: Endliche Definierbarkeit verallgemeinerter Einheitengruppen

Sei k ein algebraischer Zahlkörper, o der Ring der ganzen Zahlen in k, s eine endliche Menge von Primdivisoren p von k, $o(s) = \{x \in k; x$ p-ganz für $p \in s\}$, k_p die komplette Hülle von k bez. p. Ferner sei G eine algebraische Matrizengruppe über k und für einen Ring R sei $G_R = \{X \in G;$ X und X^{-1} haben Koeffizienten in $R\}$. Es gelten die Sätze

1. G_o ist endlich definierbar, d.h. durch endlich viele Erzeugende mit endlich vielen Rationen.
2. Für reduktives G ist $G_{o(s)}$ endlich definierbar.

Der Beweis von 1. stützt sich auf die Konstruktion von Fundamentalbereichen von Borel - Harish Chandra (Annals 75) und Beweismethoden von Gerstenhaber, Behr (Crelle 211) und Macbeath.

Das Problem 2 wurde von M. Kneser (Crelle 214/15) so reduziert: $G_{o(s)}$ ist genau dann endlich definierbar, wenn G_{k_p} für alle $p \in S$ kompakt definierbar ist. Die kompakte Erzeugbarkeit von G_{k_p} für reduktives G ist ein Ergebnis von Borel-Tits (IHES 27), die kompakte Definierbarkeit kann man aus einer Cartan-Zerlegung von G_{k_p} (Bruhat-Tits, C.R. 293) folgern.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

CASSELS, J.W.S.: Über das Zerfallen von f(x) - g(y)

Lewis, Davenport und Schinzel (Quat.J. 12) fragten, wann das Polynom $f(x) - g(y)$ in $\mathbb{C}[x,y]$ zerfällt. Neben dem trivialen Fall $f = h(f_1(x))$, $g = h(g_1(y))$, in dem $f_1(x) - g_1(y)$ Teiler von $f(x) - g(y)$ ist, entdeckten sie den Fall $f = F_k(x)$, $g = -F_k(y)$, wobei k eine gerade natürliche Zahl ist und

$$2\,F_k(x) = (x + \sqrt{x^2 - 1})^k + (x - \sqrt{x^2 - 1})^k \ .$$

Hier zerfällt $f(x) - g(y)$ in lauter quadratische Faktoren. Der Vortragende zeigt, daß das Problem nur kombinatorischer Natur ist, indem er die betreffenden Riemannschen Flächen betrachtet. Mit Rechenanlagen zeigte M.J.T. Guy so, daß es weitere komplizierte Fälle der Grade 7 und 11 gibt.

KUIPERS, L.: Gleichverteilung mod M von Folgen aus GF(q)[x]

Sei k ein Körper mit $q = p^r$ Elementen, M ein Polynom vom Grad $m \geq 2$ in $k[x]$. Nach J.H. Hodges (1966) heißt eine Polynomfolge $F = (A_i)$ aus $k[x]$ gleichverteilt mod M, wenn für jedes $B \in k[x]$ die Anzahl $F(n, B, M)$ der zu B mod M kongruenten Polynome unter $A_1, \ldots, A_n$ asymptotisch gleich $n\,q^{-m}$ ist. Der Vortragende gibt ein Gleichverteilungskriterium, das L.A. Rubels Definition der Gleichverteilung in lokalkompakten abelschen Gruppen entspricht.

JACOBINSKI, H.: Klassifikation von Gittern über Ordnungen

Sei k ein algebraischer Zahlkörper, A eine halbeinfache Algebra über k, o ein dedekindscher Ring mit Quotientenkörper k, R eine o-Ordnung von A, die in einer Maximalordnung 0 enthalten sei. Ein o-torsionsfreier, endlich erzeugter R-Modul M heißt R-Gitter. Für ein Primideal p in o bezeichne M_p die p-adische Komplettierung von M. Eine Klasse lokalisomorphen Gitter heißt ein Geschlecht.

Voraussetzung: Keine der einfachen Algebren von $E = \mathrm{Hom}_A(kM, kM)$ ist ein total definiter Quaternionenschiefkörper.

Sei F das Führerideal von R, I_F die Gruppe der F-primen Ideale des

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Zentrums C von A, n die reduzierte Norm von E über C, so gilt mit $H = \{(n\ a) \in I_F;\ a \in \mathrm{Hom}_R(M, M)\}$:

Satz: Es gibt eine Bijektion zwischen dem Geschlecht von M und der Gruppe I_F/H.

Ist N im Geschlecht von M mit $N_p = M_p$ für $F_p \neq 0_p$, so wird die bijektive Zuordnung durch $N \to n\ (\mathrm{Hom}_o(0M, 0N))$ mod H.

Spezialfall: Ist R = 0, so besteht H nach Eichler genau aus den Hauptidealen (a), wo a an allen in A verzweigten unendlichen Primstellen positiv ist.

Mit diesem Ergebnis lassen sich die Sätze von Serre und Bass über das Abspalten und Kürzen auf nichtprojektive Gitter verallgemeinern.

BRUMER, A.: Über den $\mathfrak{p}$-adischen Regulator

K sei ein algebraischer Zahlkörper, E_K seine Einheitengruppe und r(K) die Anzahl der Grundeinheiten. $\overline{E}_K$ sei der Abschluß des Bildes von E_K im Produkt $\prod_{\mathfrak{P}, p} U_{\mathfrak{P}}$ der $\mathfrak{P}$-adischen Einheitengruppen (p = feste Primzahl). Weiter sei $r_p(K)$ der Rang von $\overline{E}_K$ über $\mathbb{Z}_p$.

Satz: Sei K abelsch über Q oder über einem imaginärquadratischen Zahlkörper, dann gilt $r_p(K) = r(K)$.

Der Beweis wird dadurch erbracht, daß man das Nichtverschwinden der p-adischen Regulatoren dieser Körper zeigt und so eine Frage von Leopoldt beantwortet. Dies geschieht, indem man ein Resultat von Baker ins p-adische überträgt.

Lemma: Sei Ω Komplettierung eines algebraischen Abschlusses von Q_p. Es seien $\alpha_1, \ldots, \alpha_n$ algebraische Einheiten von Ω. Angenommen die p-adischen Logarithmen $\log \alpha_1, \ldots, \log \alpha_n$ sind über Q linear unabhängig, so sind sie es auch über dem algebraischen Abschluß von Q.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

SCHINZEL, A.: Primitive Primfaktoren von Lehmer-Zahlen

Der Vortragende gibt einen Bericht über seine Arbeiten (Acta Arith. 8) und das folgende neue Resultat:
Seien L, M natürliche teilerfremde Zahlen, $L < 4M$ und $M \neq 1$.
Sind α, b Lösungen der Gleichung $x^2 - \sqrt{L}x + M = 0$ und ist

$$P_n(\alpha, b) = \begin{cases} (\alpha^n - b^n) \cdot (\alpha - b)^{-1} & n \text{ ungerade} \\ (\alpha^n - b^n) \cdot (\alpha^2 - b^2)^{-1} & n \text{ gerade} \end{cases}$$

so hat $P_n(\alpha, b)$ für große n vier oder zwei primitive Primfaktoren (je nachdem, ob gewisse Kongruenzen erfüllt sind oder nicht).

MEYER, C.: Zum Hilbertschen Klassenkörperkonstruktionsproblem für reell-quadratische Grundkörper

Eine allgemeine Konstruktion der Klassenkörper zu reell-quadratischem Grundkörper durch geeignete analytische Funktionen, nach dem Muster der komplexen Multiplikation, ist bislang nicht durchgeführt worden. Man kann versuchen, durch Aufstellung der Kroneckerschen Grenzformel für reell-quadratische Körper die fraglichen Funktionen ausfindig zu machen. Die bisherige, auf Hecke zurückgehende Gestalt dieser Grenzformel ist hierfür jedoch nicht geeignet. Indem man diese Formel mit einem von Szegö stammenden Entwicklungssatz aus der Theorie der orthogonalen Polynome in Zusammenhang bringt, hofft der Vortragende, so eventuell zu einer Lösung des Klassenkörperkonstruktionsproblems zu gelangen.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

MAUS, A.: Über die Verzweigungsgruppenreihe

Es wird eine gruppentheoretische Kennzeichnung der Verzweigungsgruppenreihe gegeben.

Sei k ein lokaler Körper, $\underline{k}$ der endliche Restklassenkörper, Char $\underline{k} = p$. k enthalte keine p-ten Einheitswurzeln $\neq 1$. Sei K eine endliche, galoissche, rein verzweigte Erweiterung von k, $G = \mathrm{Gal}(K/k)$. Die Verzweigungsgruppenreihe von $K|k$ besitzt folgende Eigenschaften:

(1) $G_i \trianglelefteq G$, $G_i = 1$ für hinreichend hohes i

(2) G/G_1 zyklisch von zu p primen Ordnung e_o.

(3) G_i/G_{i+1} elementar abelsche p-Gruppe, $i \geq 1$

(4) G_i/G_{i+1} im Zentrum von G_1/G_{i+1}, $i \geq 1$

(5) als G/G_1-Modul ist G_i/G_{i+1} direkte Summe isomorpher, irreduzibler Teilmoduln.

(2') k enthält die e_o-ten Einheitswurzeln.

(3') $\dim G_i/G_{i+1} \leq \dim \underline{k}$, $i \geq 1$ (Dimension über GF(p))

Umgekehrt:

Ist G eine filtrierte Gruppe: $G = G_o \supset G_1 \supset G_2 \supset \ldots \supset G_r \supset G_{r+1} = 1$ mit den Eigenschaften (1) - (5), so gibt es zu jedem lokalen Körper k_o (mit obigen Einschränkungen) eine endliche Erweiterung k/k_o und eine normale Erweiterung K/k, so daß K/k die G_i als Reihe der verschiedenen Verzweigungsgruppen besitzt.

Im char.-gleichen Fall kann $k = k_o$ gewählt werden, wenn k_o (2'), (3') erfüllt. Im char.-ungleichen Fall kann k/k_o abgeschätzt werden.

Die Ergebnisse können mit anderen Methoden verallgemeinert werden.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

TAMME, G.: Algebraische Funktionenkörper vom Geschlecht 2 mit zerfallender Multiplikatorenalgebra

Sei K/k ein alg. Funktionenkörper vom Geschlecht 2 mit algebraisch abgeschlossenem Konstantenkörper. Es wird die Menge der elliptischen Teilkörper von K untersucht und jedem ellipt. Teilkörper eine komplementärer zugeordnet. Für die Teilmenge der maximalen ellipt. Teilkörper ist diese Zuordnung sogar eineindeutig, involutorisch und läßt den Grad von K über dem Teilkörper invariant. Für die Multiplikatorenalgebra $M = M_Q(K)$ von K über Q gilt dann:

1. Falls es keine ellipt. Teilkörper gibt, ist M Divisionsalgebra.
2. Falls es nur endlich viele max. ellipt. Teilkörper gibt, so sind es nur zwei zueinander nicht isogene, M ist dann direkte Summe der beiden "ellipt." Multiplikatorenalgebren.
3. Falls es unendlich viele gibt, sind sie alle isogen und M ist Matrizenring über der elliptischen Multiplikatorenalgebra.

Zum Beweis wird jedem Multiplikator ein Teilkörper von K zugeordnet, der Koordinatenkörper. Umgekehrt wird jedem Teilkörper von K ein Normmultiplikator zugeordnet. Im Vergleich dieser Zuordnungen wird die Weilsche Metrik auf M benutzt.

MARTINET, J.: Galoissche Erweiterungen von Q mit der Gruppe D_{2p}

Sei K eine galoissche Erweiterung von Q. Lokal existiert eine Ganzheitsnormalbasis genau dann, wenn nur zahme Verzweigung vorliegt. Ist K über Q abelsch, so gilt das auch global (Speiser). Der Vortragende beweist die globale Behauptung für den Fall, daß die Galoisgruppe von K über Q eine Diedergruppe der Ordnung 2 p (p prim) ist.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

AYOUB, R.: Über die Zetafunktion eines imaginär quadratischen Zahlkörpers

Sei K ein quadratischer Zahlkörper mit der Diskriminante - p. Sei

$$Z_K(s) = \sum_{n=1}^{\infty} \frac{F(n)}{n^s} \quad \text{und} \quad H(x) = \sum_{n \leq x} F(n),$$

dann ist $H(x) = \alpha x + R(x, p)$, wobei α das Residuum der Zetafunktion Z_K bei 1 ist. Es gibt eine Beziehung zwischen $R(p, p)$ und den Körpern mit Klassenzahl 1. Folgende Abschätzung wird bewiesen ($\epsilon > 0$ beliebig): $R(x, p) = 0((x\,p)^{\frac{1}{3}} + \epsilon) + 0(p^{\frac{1}{2}+\epsilon})$, wobei die Konstanten in den o's nur von ϵ, nicht von x oder p abhängen.

JEHNE, W.: p. Klassengruppen und verallgemeinerte Γ-Erweiterungen

Eine verallgemeinerte Γ-Erweiterung N eines algebraischen Zahlkörpers K ist eine abelsche Erweiterung mit Galoisgruppe $G \simeq Z_p^m$ (p-Primzahl, m-natürliche Zahl). Es wird gezeigt:

1. Zu festem K existiert eine größte verallgemeinerte Γ-Erweiterung N mit explizit angebbarem $m = m_K$.
2. Dieses N gibt Anlaß zu einer ausgezeichneten Untergruppe C^* der p-Klassengruppe C von K.

Unter der Voraussetzung der p-adischen Unabhängigkeit der globalen Einheiten gilt für eine Automorphismengruppe H von K: Für große η, natürliche Zahl, existiert eine exakte Folge:

$$1 \to E_\eta / E^{p^\eta} \to B_\eta \to C^* \to 1 \qquad (\eta \gg 0)$$

(E_η Einheitengruppe aller Einheiten, die lokal für alle $P \mid p$ p^η-te Potenzen sind), so daß B_η in einem von zyklischen Gruppen induzierten Darstellungsmodul einer bestimmten Form, abhängig

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

von H, enthalten ist.

Schließlich wurden Abschätzungen des Ranges der p-Klassengruppe nach oben und unten angegeben, mit Anwendungen auf das p-Klassenkörperturm-Problem.

BARNER, K.: Quadratsummen in total-reellen algebraischen Zahlkörpern

Satz 1: Sei k ein beliebiger algebraischer Zahlkörper und das Primideal $\mathfrak{l}$ in k ein Teiler von 2 mit der absoluten Verzweigungsordnung e. Dann gilt für die $\mathfrak{l}$-adische Darstellungsdichte der Zahl 1 als Summe von 4m Quadraten ganzer Zahlen aus k

$$d_{\mathfrak{l}}(\mathfrak{l}^{(4m)}, 1) = N(\mathfrak{l})^{[\mathfrak{l}/2]},$$

wobei $[\frac{\mathfrak{l}}{2}]$ den ganzen Teil von $\frac{\mathfrak{l}}{2}$ bezeichnet.

Beweishilfsmittel: Gaußsche Summen, Galois-Theorie.

Satz 2: Die einzigen total-reellen algebraischen Zahlkörper, in denen das Geschlecht der quaternären Einheitsform aus genau einer Klasse besteht, sind der Körper $\mathbb{Q}$ der rationalen Zahlen und die beiden quadratischen Körper $\mathbb{Q}(\sqrt{5})$ und $\mathbb{Q}(\sqrt{2})$.

Beweishilfsmittel: Siegels Hauptsatz aus der analytischen Theorie der quadratischen Formen, eine gute Diskriminantenabschätzung von C.A. Rogers und Satz 1.

MERRIMAN, J. /PFISTER, A.: Darstellung definiter Funktionen als Summe von Quadraten

Im ersten Vortrag gibt Herr Merriman einen historischen Bericht über Hilberts 17-tes Problem: Jede positiv definite rationale Funktion mit reellen Koeffizienten läßt sich als Summe von Quadraten darstellen. E. Artin gab dafür einen Beweis, indem er den Begriff des reell

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

abgeschlossenen Körpers eingeführte (und die Hilbertsche Vermutung gleich für rationale Funktionen über reell abgeschlossenen Körpern bewies). 1967 vermutete J. Ax die Verschärfung, daß die Anzahl der Quadrate höchstens 2^n ist, n = Anzahl der Variablen: Dies ist für n = 1 trivial und wurde für n = 2 von Hilbert mit Hilfe algebraischer Funktionentheorie bewiesen. Weitere Beweise stammen von Witt und Geyer. Ax bewies seine Vermutung für n = 2 und 3 mit kohomologischen Methoden unter Verwendung von Ergebnissen von Serre.

Herr Pfister trug im zweiten Vortrag mit elementaren Methoden einen Beweis für beliebiges n vor. Dabei benutzte er frühere eigene Resultate. Offen bleibt, ob die Schranke 2^n bestmöglich ist und ob ein ähnliches quantitatives Resultat auch für positiv definite Funktionen mit rationalen Koeffizienten gilt.

L. Miller
(Göttingen)

Gefördert durch
DFG Deutsche Forschungsgemeinschaft