MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 33/1973

Algebraische Zahlentheorie

12.8. bis 18.8.1973

Die alle zwei Jahre stattfindende Fachtagung über Algebraische Zahlentheorie stand wieder unter der Leitung von Herrn Professor Dr.H.Hasse und Herrn Professor Dr.P.Roquette. Auch diesmal fand sie großes Interesse, insbesondere nahmen zahlreiche Vertreter aus dem Ausland an dem Kongress teil. Die Vorträge und die anschließenden Diskussionen betrafen u.a. folgende Einzelgebiete:

Funktionenkörper, primitive Divisoren, Einbettungsprobleme, Minimaldiskriminanten, elliptische Modulformen, elliptische Kurven, Strukturen von Moduln, Kohomologie, Quaternionenerweiterungen, Klassenzahlformeln, Einheiten, quadratische Formen.

Der bevorstehende 75. Geburtstag von Herrn Professor Dr. H. Hasse gab Anlaß zu einer kurzen Würdigung seines Werkes durch die Herren Professoren Dr.C.Meyer und Dr.M.Eichler. Prof. Meyer überreichte eine Liste der dem Jubilar gewidmeten Arbeiten, die in einem Festband des Crelleschen Journals erscheinen werden.

Teilnehmer

Armitage, J.V.	Nottingham	Lang, H.	Köln
Becker, E.	Köln	Leicht, B.	Heidelberg
Bertrandias, F.	Grenoble	Leutbecher, A.	München
Brizolis, D.	Pomona	Liang, J.J.	Tampa
Brückner, H.	Hamburg	McCulloh, L.R.	Urbana
Bundschuh, P.	Köln	Madan, M.L.	Columbus
Cassels, J.W.S.	Cambridge	Martinet, J.	Bordeaux
Eichler, M.	Basel	Meyer, C.	Köln
Frei-Imfeld, G.	Quebec	Neukirch, J.	Regensburg
Fröhlich, A.	London	Ochoa, J.	Madrid
Geyer, W.-D.	Erlangen	Peters, M.	Münster
Gordon, B.	Los Angeles	Pfister, A.	Mainz
Halter-Koch, F.	Köln	Pohst, M.	Köln
Harder, G.	Bonn	Popp, H.	Mannheim
Hasse, H.	Hamburg	Roquette, P.	Heidelberg
Hazewinkel, M.	Rotterdam	Scharlau, W.	Münster
Ikeda, M.	Ankara	Schertz, R.	Köln
Jarden, M.	Heidelberg	Schinzel, A.	Warschau
Jehne, W.	Köln	Sonn, J.	Haifa
Kiyek, K.	Paderborn	Stender, H.J.	Köln
Klingen, N.	Köln	Stephens, N.M.	Oxford
Knebusch, M.	Saarbrücken	Ullom, St.V.	Urbana
Lakkis, K.	Thessaloniki	v.d. Waall, R.W.	Nijmegen
Lamprecht, E.	Saarbrücken	Zimmer, H.G.	Karlsruhe

Vortragsauszüge

J.V. ARMITAGE: The " Riemann Hypothesis " for curves and the geometry of numbers

The " Riemann Hypothesis " for curves over finite fields was formulated as a theorem concerning the product of linear forms and a new proof was then given using methods based on the geometry of numbers.

M.L. MADAN: Algebraic Function Fields with Small Class Number

What are the algebraic function fields of nonzero genus which have class number one ? Mac Rae, (Journal of Algebra, 1971), answered this question for the special case of function fields which are quadratic extensions of rational function fields and have a prime of degree one. In collaboration with C.Queen, (Acta Arithmetica, 1972), we solved the problem almost completely. In a joint paper with J.Leitzel and C.Queen, with the above title, it is now shown that there is no function field of genus 4 over GF(2) which has no prime of degree less than 4 and precisely one prime of degree 4. It is also proved that there are two nonisomorphic fields of genus 3 which have class number one. In all, there are 7 nonisomorphic function fields of class number one. Imaginary quadratic extensions of class number 2 (in the sense of Artin) are classified. Necessary and sufficient conditions are given for a function field to have class number 2.
The main tool is the Riemann Hypothesis. An exception is the proof showing the nonexistence of a function field of genus 4 and class number one.

M. EICHLER: Über die Definitionskörper gewisser automorpher Funktionen

Sei k ein total reeller algebraischer Zahlkörper vom Grade n, K/k eine Quaternionen-Algebra, welche an genau n-1 unendlichen Primstellen von k verzweigt ist. Sie läßt sich durch zweireihige Matrizen in k darstellen. Weiter sei $\mathfrak{O}$ eine maximale Ordnung von K und Γ die Gruppe der Einheiten $U \in \mathfrak{O}$, deren Normen $n_{K/k}(U) \gg 0$, d.h. total positiv sind. Diese Einheiten, als zweireihige Matrizen $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ dargestellt, definieren eine diskontinuierliche Gruppe von Abbildungen der oberen Halbebene $\operatorname{Im} z > 0$ auf sich vermöge

$$z \longrightarrow \frac{\alpha z + \beta}{\gamma z + \delta} .$$

Die hierzu gehörigen automorphen Funktionen wurden zuerst von Poincare untersucht (vgl. Fricke-Klein, Vorlesungen autom.

Funktn., S. 586 ff). Shimura zeigte, daß der Körper dieser automorphen Funktionen über dem absoluten Klassenkörper von k definiert werden kann. Der Vortragende gibt hierfür einen neuen Beweis, der auf gewissen Spezialisierungen von Hilbert-Siegelschen Modulfunktionen beruht.

A. SCHINZEL: Primitive divisors of the expressions $A^n - B^n$ in algebraic number fields

Let A, B be non-zero integers of an algebraic number field K of degree d. A prime ideal $\mathfrak{P}$ of K is called a primitive divisor of $A^n - B^n$ if $\mathfrak{P} | A^n - B^n$ but $\mathfrak{P} \nmid A^m - B^m$ for $m < n$. L.P. Postnikova and the lecturer proved in 1967 that if (A,B)=1 and A/B is not a root of unity, primitive divisors exist for all $n > n_0(A,B)$ and raised the question, whether the same is true for $n > n_0(K)$. The aim of the lecture was to outline the proof of the following stronger

Theorem: If (A,B) = 1 and A/B is not a root of unity then $A^n - B^n$ has a primitive divisor for all $n > n_0(d)$, where d is the degree of A/B and $n_0(d)$ is effectively computable.

The theorem is best possible up to the order of the function $n_0(d)$; the proof is based on a recent theorem of Baker on linear forms in logarithms.

M. JARDEN: Elementary statements over large algebraic fields

It was given a survey of the author's dissertation (which appeared in the Trans. of A.M.S. (1972)):
A. If k is a denumerable Hilbertian field then for almost all $(\sigma_1,\ldots,\sigma_n) \in \mathcal{G}(k_s/k)^e$ the fixed field of $\{\sigma_1,\ldots,\sigma_n\}$, $K = k_s(\sigma_1,\ldots,\sigma_n)$, has the following property: For any non-void absolutely irreducible variety V defined over $k_s(\sigma_1,\ldots,\sigma_n)$ the set of points of V rational over K is not empty.
Here " almost all " is used in the sense of the Haar measure defined on $\mathcal{G}(k_s/k)^e$ with respect to its Krull topology.
B. If E is an elementary statement about fields then the measure of the set of $\sigma \in \mathcal{G}(\tilde{Q}/Q)$ for which E holds in $\tilde{Q}(\sigma)$

is equal to the Dirichlet density of the set of primes p for which E holds in the field F_p of p elements.

A. FRÖHLICH: Galois module structure and Artin root numbers

The connections between Galois module structure for absolutely normal and tame extensions, and Artin root numbers were discussed, with explicit examples for all fields with Galois-group generalized quaternion of order $4p^n$, p an odd prime.

J. MARTINET: On the embedding problem for quaternion extensions

Let k be a number field, and $k_1 = k(\sqrt{m})$ a quadratic extension. The generalized quaternion group H_n of order 4n is defined by 2 generators σ and τ, with relations $\sigma^n = \tau^2$, $\tau^4 = 1$, $\tau\sigma\tau^{-1} = \sigma^{-1}$. Is it possible to find a Galois extension N/k, with a Galois group isomorphic to H_n, cyclic over k_1? The problem is clearly impossible if m is not totally positive. Suppose the contrary. Then the problem has always a solution if n is divisible by 8. For a given n, we have necessary and sufficient conditions on m for the problem to have a solution; indeed, the problem is easily reduced to the case when n is a power of 2. (Joint work with P. Damey).

F. BERTRANDIAS: On the integers of cyclic p-extensions of a local field

Let k denote a local field with ring of integers A, and let K be a cyclic p-extension of k with ring of integers B (p is equal to the characteristic of the residue class field $\bar{k}$). Denote by G the Galois group of K/k.
Let O be the order associated to B in $k[G]$, that is $O = \{\lambda \in k[G], \lambda B \subset B\}$. O is an order of A in $k[G]$, containing $A[G]$. B is a finitely generated O-module, isomorphic with an ideal of O.
Denote by t the ramification number of K/k. Let $\frac{t}{p} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 \ddots}}$ $= [a_0, a_1, \ldots, a_n]$ (with $a_n > 1$) the continued fraction of $\frac{t}{p}$.

If t satisfies the inequality $t < \frac{pe}{p-1} - 1$ (where e is the absolute ramification index of k), we obtain the following results:

(i) B is a free O-module if and only if $n \leq 2$;

(ii) the minimal number of generators of the O-module B is:

$$m = \begin{cases} 1 & \text{if } n = 1 \text{ or } 2 \\ 1 + \sum_{1 \leq i \leq [\frac{n}{2}]} a_{2i} & \text{if } n \geq 3. \end{cases}$$

St.V. ULLOM: Locally free modules over orders

Let K be an algebraic number field, R a Dedekind domain with quotient field K, and A an R-order in a semisimple K-algebra B. Let C(A) be the locally free class group of A. The order A is contained in some maximal R-order A' in B; Swan proved the change of rings map $C(A) \longrightarrow C(A')$ is an epimorphism. We obtain an upper bound for the exponent e(A) of the kernel D(A) of this map.

In particular take $A = ZG$, G a p-group of order p^n, then e(ZG) divides p^{n-1}. Moreover, Galovich has proved that $e(ZG) = p^{n-1}$, for G cyclic of order p^n, $p > 3$. If G is the symmetric group S_n, the order of $D(ZG) = C(ZG)$ is prime to p for primes $p > \frac{n}{2}$.

J. NEUKIRCH: Tolerante Zahlkörper

Ist K/k eine galoissche Erweiterung algebraischer Zahlkörper, so stellt sich die Frage, wann sich K in einen größeren galoisschen Körper einbetten läßt, derart, daß die Gruppenerweiterung $G(N/k) \longrightarrow G(K/k) = G$ vom vorgegebenen Typus ist. Für die sogenannten Scholzschen Körper ist es bekannt, daß zu jedem $X \in H^2(G(K/k), Z/n)$ ein Körper N existiert, dessen Galoisgruppe die durch X gegebene Gruppenerweiterung $1 \to Z/n \to E \to G \to 1$ realisiert. Es wird gezeigt, daß das gleiche für eine sich zwangsläufig ergebene größere Klasse von Körpern gilt, die als tolerante Körper bezeichnet werden und in der folgenden Weise definiert sind:

Def.: Eine zahm verzweigte Erweiterung K/k heiße tolerant gegenüber n, wenn ihre Zerlegungsgruppen zyklisch sind und $N(\mathfrak{p}) \equiv 1 \bmod e_{\mathfrak{p}} n_{\mathfrak{p}}$ für jede Primstelle $\mathfrak{p}$ von k gilt, wobei $e_{\mathfrak{p}}$ der Verzweigungsindex und $n_{\mathfrak{p}} = \prod_{p \mid e_{\mathfrak{p}}} p^{v_{\mathfrak{p}}(n)}$ ist.

Die weitere Frage, wann es zu jedem $X \in H^2(G, \mathbb{Z}/_p)$ sogar einen gegenüber $\frac{n}{p}$ toleranten Körper $N \supseteq K \supseteq k$ vom Grade p gibt, führt auf eine Hindernistheorie, die einfacher und weniger streng ist als jene, die von Šafarevič für die Scholzschen Erweiterungen entwickelt wurde.

J. SONN: Localizability of Embedding Problems with Non-solvable Kernels

Given an embedding problem $P = P(K/k, 1 \to N \to E \to G(K/k) \to 1)$ in which k is a number field and N is simple non-abelian, we formulate a hypothesis $\underline{L}$ which postulates the existence of extensions $L \supset K$, Galois over k such that $G(L/K) \cong N$ which localizes at each prime p of a finite set S of primes of k, to a prescribed extension $L_p \supset K_p$, Galois over k_p. Does $\underline{L}$ insure a solution field to P? When $N = A_n$, $n \neq 6$, yes. When $N = PSp(2m,q)$ or $PSL(n,q)$, no in general, in particular the answer is no when K/k is a Scholz extension as are the solvable extensions of Šafarevič. However if one suitably prescribes the decomposition groups of the primes in S in K/k, then the answer is yes when $N = PSp(2m,q)$, $m > 1$.

L. McCULLOH: Corresponding residue systems

Let K_1 and K_2 be algebraic number fields with integers O_{K_1} and O_{K_2}. Let N be a common extension of K_1 and K_2, normal over $F = K_1 \cap K_2$. There is a unique ambiguous ideal $\mathfrak{m} = \mathfrak{m}(K_1, K_2)$ of N/K minimal with respect to the property: $O_{K_1} + \mathfrak{m} = O_{K_2} + \mathfrak{m}$. A prime $\mathfrak{P}$ of N divides $\mathfrak{m} \iff \mathfrak{P}$ is totally ramified in K_1/F and K_2/F. If $\mathfrak{P}^M \| \mathfrak{m}$, M can be determined easily unless $[K_1:F] = [K_2:F] = p^n$ where $\mathfrak{P} \mid p$. To determine M in the exceptional case, we pass to the completion. The problem then be-

comes to determine the minimum distance between primes of K_1 and K_2. This can be done solely in terms of ramification invariants if either $M = 1$ or if the K_i/F are cyclic. In general, ramification invariants give only upper and lower bounds and finer invariants will be needed. E.G., if $F = Q_2(\zeta_{15})$ and $L = K_1K_2$ is an elem. abelian extension arising by local class field theory from the quotient $U^{(1)}/U^{(2)}$ of unit groups, then $M = 7$ or 6 according as $\delta(K_1) = \delta(K_2)$ or not, where $\delta(K_i)$ is an element of the residue field $\bar{F}$, viz., the residue class of $a_2^2/2a_0$ where $x^4 + \ldots a_2x^2 + \ldots + a_0$ is any Eisenstein polynomial defining K_i/F.

J.J. LIANG: On minimum discriminant of algebraic number fields

Inspired by previous results of G.Kaur, Hunter and Mayer a new method of determing the minimum absolute value of the discriminant of totally complex sixth degree algebraic number fields is developed. It is 9747 and is assumed only by the algebraic number field $Q(\theta)$, where $\theta = (\sqrt[3]{w(2w+5)} - 1)/(w-1)$ is a root of the monic irreducible polynomial $x^6 - 3x^5 + 4x^4 - 4x^3 + 4x^2 - 2x + 1$ with discrimiant -9747.

H. BRÜCKNER: Zum 1. Fall der Fermatschen Vermutung

Sei r der l-Rang der Klassengruppe des l-ten Kreiskörpers (l eine ungerade Primzahl). M. Eichler zeigte 1965 (Acta math.11) daß der 1. Fall der F.V. für l richtig ist, falls nur $r < (\sqrt{l} - 2)$. Diese Tatsache läßt sich auch beweisen mit Hilfe der durch

$$\frac{1}{1 - \gamma e^{-t}} = \sum_{i=0}^{\infty} \frac{G^{(i)}}{i!} t^i \qquad (\gamma \in Q, \gamma \neq 1)$$

definierten Zahlenfolge $G^{(i)}$, die ähnliche Eigenschaften wie die Folge der Bernoullischen Zahlen aufweist. Es besteht die Hoffnung, daß durch diesen Ansatz die Schranke $(\sqrt{l} - 2)$ noch verbessert werden kann.

M. PETERS: Quadratsummen in Zahlringen

Sei R ein kommutativer Ring mit 1. Die minimale natürliche Zahl $q = q(R)$, derart daß jede Summe von Quadraten aus R bereits durch eine Summe von q Quadraten dargestellt werden kann, wird als "Quadratstufe" von R bezeichnet. (Falls es kein derartiges q gibt, setzt man $q(R) = \infty$).
1) Für Maximalordnungen M in nicht total reellen Zahlkörpern ist die Quadratstufe $q(M) \leq 4$, für beliebige Ordnungen R in nicht total reellen Zahlkörpern $q(R) \leq 5$. Die Schranken sind scharf, zum Beispiel ist in imaginär-quadratischen Zahlkörpern $q(R) = 5$ genau dann, wenn die Diskriminante von R durch 16 teilbar ist. Bei den Beweisen wird der starke Approximationssatz benutzt.
2) Mit elementaren Methoden zeigt man für Ordnungen R in reell-quadratischen Zahlkörpern: $q(R) \leq 5$, und zwar $= 5$, falls die Diskriminante > 28 ist.
In beiden Fällen werden Charakterisierungen der Gesamtheit der durch Quadratsummen darstellbaren Elemente gegeben.

A. LEUTBECHER: Über die Heckeschen Gruppen $G(\lambda)$

In E.Heckes Arbeit "Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung", Math.Ann.112(1936), treten automorphe Formen zu den durch $z \longmapsto z+\lambda$, $z \longmapsto -1/z$ erzeugten diskreten Untergruppen $G(\lambda)$ von $PSL_2\mathbb{R}$ auf. Darin ist $\lambda = \lambda_q = 2\cos\frac{\pi}{q}$. Bekanntlich sind $G(\lambda_4)$ und $G(\lambda_6)$ kommensurabel mit $G(\lambda_3) = PSL_2\mathbb{Z}$.

Satz 1: Ist $q \neq 3,4,6$, so ist stets $G(\lambda_q)$ das einzige Maximum in seiner Kommensurabilitätsklasse bzgl. $PSL_2\mathbb{R}$.

Satz 2: Ist der Körpergrad $[\mathbb{Q}(\lambda_q^2) : \mathbb{Q}] = 2$, mit anderen Worten ist $q = 5,8,10$ oder 12, so ist die Menge aller Spitzen von $G(\lambda_q)$ genau gleich $\lambda_q\mathbb{Q}(\lambda_q^2) \cup \{\infty\}$.

G. HARDER: Kohomologie arithmetisch definierter Gruppen

Es wurde über einige Untersuchungen über die Kohomologie arithmetisch definierter Gruppen Γ berichtet. Diese Gruppen operieren auf einem symmetrischen Raum X und $H^v(\Gamma,\mathbb{C}) = H^v(\Gamma\backslash X,\mathbb{C})$. Es wurden dabei Fragen angeschnitten, die sich aus der Tatsache ergeben, daß dieser Quotient $\Gamma\backslash X$ nicht kompakt ist und man daher die Methode der Hodge-Theorie nicht anwenden kann. Man interessiert sich daher für das Verhalten von Kohomologieklassen im Unendlichen. Das kann in vielen Fällen mit Hilfe der Eisensteinschen Reihen von Maaß-Selberg-Langlands verstanden werden.

B. GORDON: 2-Potenzen der Koeffizienten elliptischer Modulformen

This is a preliminary report on some joint work of Mr.C. Sudler and the speaker. Let q(n) be the number of partitions of n into distinct parts. Some congruences of the Ramanujan type are obtained for q(n), for example $q(125n+26) \equiv 0 \bmod 5$. If e(n) is defined by $2^{e(n)} \| q(n)$, the values of n for which $e(n) = 0,1,2,3,4,$ or 5 are determined. In particular, $e(n) \leq 5$ if and only if $24n+1$ is of the form x^2+6y^2 . Numerical evidence gleaned from a table for $n \leq 64{,}000$ suggests that similar characterizations exist for all $e(n) \leq 12$. Moreover, e(n) is additive as a function of $24n+1$, i.e. if $(24n_1+1, 24n_2+1) = 1$, and $(24n_1+1)(24n_2+1) = 24n+1$, then $e(n) = e(n_1)+e(n_2)$.

R.W. VAN DER WAALL: Splitting properties of primes by means of Artin conductors

Let p be an odd prime, and let t be a natural number such that $p \nmid t$ and such that t is not the p^{th}-power of another natural number. Consider the field $\mathbb{Q}(\sqrt[p]{t})$. How does $p\mathbb{Z}$ split in $\mathbb{Q}(\sqrt[p]{t})$ Berwick (1927) finds a very complicated

proof of it, as follows :

Let $t^p \equiv t\ (p^j)$, $t^p \not\equiv t\ (p^{j+1})$, $j \geq 2$. Then

(a) If $2 \leq j \leq n$, then

$$p = \mathfrak{p}_1^{\varphi(p^n)} \mathfrak{p}_2^{\varphi(p^{n-1})} \cdots \mathfrak{p}_{j-1}^{\varphi(p^{n-j+2})} \mathfrak{p}_j^{\varphi(p^{n-j+2})/(p-1)} .$$

(b) If $j \geq n+1$, then

$$p = \mathfrak{p}_1^{\varphi(p^n)} \mathfrak{p}_2^{\varphi(p^{n-1})} \cdots \mathfrak{p}_{n-1}^{\varphi(p^2)} \mathfrak{p}_n^{\varphi(p)} \mathfrak{p}_{n+1} .$$

Here $\varphi(n)$ is Euler's totient function.

If $t^p \not\equiv t\ (p^2)$, then $p = \mathfrak{p}^{p^n}$.

In Roma, Italy, april 1973 I gave a rather divert proof of this result in the case $n = 1$.

It is the purpose of this talk to extend the method of the proof from $n = 1$ to the case $n = 2$. For $n \geq 3$ my method is as least as difficult as Berwick's original proof.

I will use only : 1. Führerdiskriminantenproduktformel for the Galois closure of $\mathbb{Q}(\sqrt[p]{t})$,
2. Congruence relations and properties going back to Dedekind ,
3. Elementary algebraic number theory for normal extensions.

J. OCHOA: Ein elementares Modell für die Divisorenklassen eines algebraischen Körpers

Durch die Einführung einer normalen Form für die Matrizen $A = (a_{ij})$, $(i,j = 1,\ldots,n)$ $a_{ij} \in \mathbb{Z}$, ähnlich über $\mathbb{Z}$, studiert man die Verbindung zwischen Divisoren- und Matrizenklassen, bei Latimer und Mac-Duffee hergestellt. Zufolge der erhaltenen Ergebnisse kann man das Modell für die Divisorenklassen des Körpers definieren. Als letztes studiert man die Abbildung der Einheiten des Körpers in dem Modell mit den Algorithmen, mit denen solche Einheiten bestimmt werden.

D. BRIZOLIS: Ideals in rings of integer-valued polynomials

Define $R_Q^o = \{f \in Q[x] : f(\mathbb{Z}) \subseteq \mathbb{Z}\}$, the ring of integer-valued polynomials over Q. R_Q^o has the following property (Th.Skolem) : If $f_1, f_2, \ldots, f_n \in R_Q^o$ satisfy $(f_1(a), \ldots, f_n(a)) = (1)$ for every $a \in \mathbb{Z}$, then $(f_1, \ldots, f_n) = (1)$ (the unit ideal in R_Q^o) . It is worth noting that $\mathbb{Z}[x]$ does not satisfy this property, for example : $f_1(x) = 3$, $f_2(x) = x^2+1$, $(f_1(a), f_2(a)) = (1)$ for all $a \in \mathbb{Z}$ but $(3, x^2+1) \neq (1)$ in $\mathbb{Z}[x]$. We see that $(3, x^2+1) = (1)$ in R_Q^o. In this note we seek other subrings of $Q[x]$ which satisfy this property. Define $R_Q^k = \{f \in Q[x] : f^{(j)} \in R_Q^o , 0 \leq j \leq k\}$ where $k \in \mathbb{Z}^+$ and $R_Q^\infty = \bigcap_{k=0}^{\infty} R_Q^k$. Then R_Q^k satisfies the above property for $k = 0, 1, 2, \ldots$ and $k = \infty$. We next see an alternative characterization of the above property (Skolem property) in terms of the maximal ideals of subrings of $Q[x]$.

Theorem : Let $R \subseteq R_Q^o$. Then R satisfies the Skolem property if and only if every maximal ideal of R is of the form $M = M_{\alpha,p}^R = \{f \in R : |f(\alpha)|_p < 1\}$ where $\alpha \in \mathbb{Z}_p$ and $p \in \mathbb{Z}$ is prime.

We use this property to prove

Theorem : There is no smallest subring of R_Q^o (containing $\mathbb{Z}[x]$) which has the Skolem property.

The above also have generalizations : let A be an integral domain, K its field of fractions. Define $R_K^o = \{f \in K[x] : f(A) \subseteq A\}$. If we place certain conditions on A (i.e. Dedekind domain, $A/\mathfrak{p}$ finite for every prime ideal $\mathfrak{p}$ of A), then R_K^o is a Skolem ring. The converse is unknown at this time. It is worth noting that if K is any finite algebraic extension of Q, then R_K^o is a Skolem ring. This is false if $[K : Q] = \infty$.

E. BECKER: Über Euklidische Körper

Ein Körper heißt Euklidisch, wenn in ihm die Quadrate einen Positivitätsbereich bilden, er heißt Pythagoräisch, wenn er formal-reell ist und jedes total positive Element Quadrat ist. Jeder formal reelle Körper besitzt einen kleinsten Pythagoräischen Erweiterungskörper : die Pythagoräische Hülle. Jeder formal reelle Körper besitzt minimale Euklidische Oberkörper : seine Euklidischen Hüllen. Für die Euklidischen Hüllen eines Körpers gilt eine Analogie zur Artin-Schreier-Theorie der reellen Hüllen. Euklidische Hüllen sind die maximal-reellen Oberkörper in der maximalen 2-Erweiterung und haben in dieser den Index 2. Aus den Sätzen über Euklidische Hüllen lassen sich Charakterisierungen der Pythagoräischen Hülle ableiten, außerdem gewinnt man eine technische Vereinfachung des Scharlauschen Beweises des Satzes von Pfister über die Torsionsuntergruppe des Wittringes.

M. KNEBUSCH: Reziprozitätsgesetz für algebraische Kurven

Bericht über unveröffentlichte Untersuchungen von W.Scharlau und mir. Sei X vollständige glatte Kurve mit endlichem Konstantenkörper k einer Charakteristik $\neq 2$. Als quadratisches Reziprozitätsgesetz $(\partial_\mathfrak{p})$ zu einem Geradenbündel $\mathcal{L}$ über X bezeichnen wir eine Familie $\partial_\mathfrak{p} : W(L) \longmapsto W(k(\mathfrak{p}))$ von 2. Restklassenformen auf der Wittgruppe der symmetrischen bilinearen Formen über k(X) mit Werten in dem Modul L der rationalen Schnitte von X, so daß $\sum_\mathfrak{p} \mathrm{Tr}^*_\mathfrak{p} \circ \partial_\mathfrak{p}(z) = 0$ für alle $z \in W(L)$ ist. Es läßt sich zeigen, daß $\mathcal{L}$ genau dann ein Reziprozitätsgesetz zuläßt, wenn $\mathcal{L}$ in Pic(X) ein Quadrat ist, und dann bis auf evidente Multiplikatoren auch nur eines. In Math.Z.121(1971),346-368, wurde von W.D.Geyer, G.Harder, W.Scharlau und mir ein solches Reziprozitätsgesetz für $\mathcal{L} = \Omega_X$ = Bündel der Differentiale auf X elementar

hergeleitet. Somit ergibt sich ein nicht analytischer Beweis des Satzes von Armitage (Invent.math.2(1967)), daß Ω_X in Pic(X) ein Quadrat ist.

R. SCHERTZ: Die Klassenzahlformel einfach reeller kubischer Zahlkörper

Die Klassenzahlen der Teilkörper von Ringklassenkörpern über imaginär-quadratischen Körpern lassen sich, ausgehend von den in der Monographie von C.Meyer "Die Berechnung der Klassenzahl abelscher Körper über quadratischen Zahlkörpern", Berlin 1957, bewiesenen Klassenzahlformeln, mittels der komplexen Multiplikation untersuchen. So findet man zum Beispiel den

Satz: Sei $\Sigma = \mathbb{Q}(\sqrt{D})$ ein imaginär-quadratischer Zahlkörper der Diskriminante $D < -4$, und es bezeichne für $f_o \in \mathbb{N}$ $\mathfrak{K}_{f_o}$ die Ringklassengruppe modulo f_o in Σ sowie m die Anzahl der durch drei teilbaren Invarianten von $\mathfrak{K}_{f_o}$. f sei eine Primzahl mit $(f, f_o) = 1$, $(\frac{D}{f}) = -1$, $f+1 \equiv \pm 3 \bmod 9$. Ferner gelte: es existiere ein kubischer Zahlkörper der Diskriminante $(f_o f)^2 D$, jedoch existiere für keinen echten Teiler f_o' von f_o ein kubischer Zahlkörper der Diskriminante $(f_o' f)^2 D$. Dann besteht die Implikation

Für alle einfach reellen kubischen Zahlkörper K der Diskriminante $(f_o f)^2 D$ gilt $3^{m+1} | h_K$ $\Longrightarrow$ $3^{m+1} | [\mathfrak{K}_{f_o} : 1]$.

H.J. STENDER: Über die Einheitengruppe der reinen algebraischen Zahlkörper 6. Grades

Es seien $K = \mathbb{Q}(\omega)$, $\omega = \sqrt[6]{a}$ $(a \in \mathbb{N})$ ein reiner Zahlkörper 6. Grades mit der Einheitengruppe E(K), $K_2 = \mathbb{Q}(\omega^3)$ der quadratische Teilkörper von K mit Einheitengruppe $E(K_2)$,

$E(K_2) = \langle \eta_2 \rangle$, $K_3 = \mathbb{Q}(\omega^2)$ der (reine) kubische Teilkörper von K mit Einheitengruppe $E(K_3) = \langle \eta_3 \rangle$. Es sei $\varepsilon_1 \in E(K)$ mit $N_{K/K_2}(\varepsilon_1) = 1$ und $N_{K/K_3}(\varepsilon_1) = \pm 1$ (Relativnormen), ε_1 keine Potenz in K . Es wurde mitgeteilt, wie man ε_1 konstruieren kann, und gezeigt, wie sich aus dem unabhängigen Einheitensystem $\varepsilon_1, \eta_2, \eta_3$ ein Grundeinheitensystem von K explizit ableiten läßt. - Als Anwendung erhält man für spezielle K folgenden

Satz : Sei $a = D^6 \pm d$, $d, D \in \mathbb{N}$, $d \mid D$, a quadratfrei. Dann ist $S_\xi = \{\xi_k : k = 2,3,6\}$ mit $\xi_k = \frac{\omega^k - D^k}{(\omega - D)^k}$ ($\xi_6 = \frac{1}{\omega - D}$ bei $d=1$) ein Grundeinheitensystem von K .

H. LANG: Kongruenzen zwischen Klassenzahlen quadratischer Zahlkörper

Betrachtet man den imaginären biquadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ mit $\operatorname{sgn} d_1 = \operatorname{sgn} d_2 = -1$ als Erweiterung seines reell-quadratischen Teilkörpers $k_0 = \mathbb{Q}(\sqrt{d_1 d_2})$, so gehört zu dieser Erweiterung K/k_0 eine eindeutig bestimmte L-Funktion über k_0. Diese läßt sich als Produkt

$$L(s,\chi) = L_{d_1}(s) L_{d_2}(s)$$

aus den zu den beiden imaginär-quadratischen Zahlkörpern $k_1 = \mathbb{Q}(\sqrt{d_1})$ und $k_2 = \mathbb{Q}(\sqrt{d_2})$ gehörigen rationalen L-Funktionen darstellen. An der Stelle 1 ist bekanntlich L_{d_1} bzw. L_{d_2} im wesentlichen die Klassenzahl von k_1 bzw. k_2 . Andererseits läßt sich $L(s,\chi)$ als Summe

$$L(s,\chi) = \frac{1}{2} \sum_{\mathfrak{A}} \chi(\mathfrak{A}) L(s,\mathfrak{A})$$

von erweiterten Ringklassen-L-Funktionen schreiben. Dabei ist $24 \frac{(2\pi)^2}{\sqrt{d_1 d_2}} L(1,\mathfrak{A})$ eine ganzrationale Zahl. Aus der arithmetischen Struktur dieser ganzrationalen Zahl lassen sich Kongruenzen mod 3 und mod 4 bzw. mod 8 zwischen den Klassenzahlen der quadratischen Zahlkörper k_0, k_1 und k_2 herleiten.

M. IKEDA: Automorphisms of local Galois groups

Let K be a local field, Ω be its separable closure, and G_K be the Galois group of Ω/K . It is shown that there is an isomorphism Λ from the group of all group automorphisms $\mathrm{Aut}(G_K)$ of G_K to a subgroup H of the group of all automorphisms $\mathrm{Aut}(\Omega^*)$ of the multiplicative group Ω^* . The subgroup H consists of all elements $\sigma \in \mathrm{Aut}(\Omega^*)$ satisfying the following conditions :

1) For any finite Galois extension L of K , L^σ $(= (L^*)^\sigma \cup \{0\})$ is a Galois extension of K with $[L^\sigma:K] = [L:K]$,

2) For any two finite Galois extensions $L_1 \supset L_2$ of K , the following diagram is commutative :

$$\begin{array}{ccc} L_1^* & \xrightarrow{\sigma} & (L_1^*)^\sigma \\ {\scriptstyle N_{L_1/L_2}}\downarrow & & \downarrow{\scriptstyle N_{L_1^\sigma/L_2^\sigma}} \\ L_2^* & \xrightarrow{\sigma} & (L_2^*)^\sigma \end{array}$$

Denoting g^{inn} the inner automorphism generated by an element g of G_K , one has $\hat{g}^{inn} = g$. This implies in particular that the centre of G_K is trivial.

H.G. ZIMMER: Ein Analogon des Satzes von Nagell-Lutz über die Torsion einer elliptischen Kurve

Im Satz von Nagell-Lutz werden für eine über einem Körper definierte elliptische Kurve $\mathcal{E}$ mit der Diskriminante D im Falle, daß $K = \mathbb{Q}$ der rationale Zahlkörper ist und die Kurvengleichung ganzrationale Koeffizienten hat, notwendige Bedingungen für Torsionspunkte in der Gruppe $\mathcal{E}_K$ der über K rationalen Punkte von $\mathcal{E}$ gegeben : Ist $P = (x,y)$ ein Punkt endlicher Ordnung aus $\mathcal{E}_{\mathbb{Q}}$, so hat P ganzrationale Koordinaten x,y , und darüber hinaus ist entweder $y = 0$ oder y^2 teilt D . Ein analoger Satz von Nagell-Lutz ist auch für über einem rationalen Funktionenkörper $K = \Omega(t)$ der Charakteristik 0 definierte elliptische Kurven $\mathcal{E}$ bekannt.
Dieses letztere Resultat läßt sich nun zu einem Analogon des

Satzes von Nagell-Lutz für eine elliptische Kurve $\mathfrak{E}$ über einem Funktionenkörper K/Ω vom Transzendenzgrad 1 der Charakteristik $\neq 2$ verallgemeinern: Ist $P=(x,y)$ ein Punkt endlicher Ordnung aus $\mathfrak{E}_K$, so liegen die Koordinaten x,y im Ω-Modul der Vielfachen in K eines durch die Koeffizienten der Kurvengleichung von $\mathfrak{E}$ gegebenen Divisors $\mathfrak{m}$ bzw. $\mathfrak{m}^3$ von K/Ω, und darüber hinaus ist entweder $y=0$ oder y^{-2} liegt im Ω-Modul der Vielfachen in K des Divisors $D^{-1}\mathfrak{m}^3$ von K/Ω. Diese Bedingungen sind im Falle endlicher Charakteristik q von K/Ω für Punkte der Ordnung q^n bzw. $2q^n$ geeignet zu modifizieren.

K. KIYEK: <u>Pseudobetragsfunktionen auf Quotientenkörpern von Dedekindringen</u>

Es sei K ein Körper. Eine nicht negative Funktion φ auf K heißt Pseudobetragsfunktion, falls $\varphi(xy) \leqq \varphi(x)\varphi(y)$, $\varphi(x-y) \leqq \varphi(x)+\varphi(y)$. Eine Betragsfunktion f auf K heißt in φ enthalten, falls aus $\varphi(x) < 1$ folgt $f(x) \leqq 1$.

<u>Satz 1</u>: Ist f in φ enthalten, so gibt es eine reelle Zahl $s > 0$ mit $f^s \leqq \varphi$.

Nun sei K der Quotientenkörper des Dedekindringes R. Für Primideale $\mathfrak{p}$ von R sei $f_{\mathfrak{p}}$ eine zugehörige nicht archimedische Betragsfunktion. Die Pseudobetragsfunktion φ auf K heißt von endlichem Typ (bez. R), falls in φ nur endlich viele archimedische Betragsfunktionen $f_1,\ldots,f_h$ $(h \geqq 0)$ enthalten sind und $\varphi(x) \leqq \gamma \max(f_1(x),\ldots,f_h(x))$, $x \in R$ $(\gamma > 0)$ gilt.

<u>Satz 2</u>: Ist der ganze Abschluß S von R in einer endlichen Erweiterung L von K endlich erzeugter R-Modul, so ist jede Fortsetzung von φ auf L von endlichem Typ (bez. S).

<u>Satz 3</u>: Ist φ von endlichem Typ, so gibt es endlich viele nicht archimedische Betragsfunktionen $f_{\mathfrak{p}_1},\ldots,f_{\mathfrak{p}_t}$, so daß φ zu $\max(f_1,\ldots,f_h,f_{\mathfrak{p}_1},\ldots,f_{\mathfrak{p}_t})$ äquivalent ist.

Da jede Pseudobetragsfunktion auf $\mathbb{Q}$ von endlichem Typ (bez. $\mathbb{Z}$) ist, erhält man die Resultate von Mahler wieder.

*) W.A. DEMJANENKO: Über die Hypothese von C.L.Siegel und die Hypothese von L.J.Mordell

Let K be a field of algebraic numbers of degree n over the rational field, let G be the algebraic curve of genus > 1, defined over this field.

Theorem 1: If the rank of the curve $u^4+au^2+b = Av^2$ over the field K does not exceed r, then the equation $x^4+ax^2y^2+by^4 = A$ does not have more than $c(r,K)$ integer solutions.

Theorem 2: If the rank of the curve $u^3+au^2v+buv^2+cv^3 = A$ over the field K does not exceed r, then, provided $(x,y) = 1$, the equation $x^3+ax^2y+bxy^2+cy^3 = A$ does not have more than $c(r,K)$ integer solutions.

Proved also the hypothesis by L.J. Mordell for more broad class of algebraic curves than in the paper " Rational points of a class of algebraic curves " (W.A.Demjanenko, Izv.AN UdSSR, ser.mat., 30 (1966), 1373-1396).

*) Dieser Vortragsauszug wurde den Tagungsteilnehmern in einer Kopie übergeben, da Herr Demjanenko nicht - wie vorgesehen - an der Tagung teilnehmen konnte.

M.Pohst (Köln)
H.J.Stender (Köln)