Zählen von Zahlkörpern

Gunter Malle

Universität Kaiserslautern

malle@mathematik.uni-kl.de

Zahlkörper

Zahlkörper $\quad = \quad$ endliche Erweiterungen $K/\mathbb{Q}$

Fragen:

- welche Galoisgruppen kommen vor?
  (Umkehrproblem)

- wie häufig kommt geg. Galoisgruppe vor?
  (Asymptotik der Zählfunktion)

- Eigenschaften der Zahlkörper?
  (z.B. Klassengruppe)

Quadratische Zahlkörper

Quadratische Zahlkörper: $\mathbb{Q}(\sqrt{d})$, mit $d \in \mathbb{Q}$.

oBdA: d quadratfreie, ganze Zahl:

$d = \ldots, -6, -5, -3, -2, -1, 2, 3, 5, 6 \ldots$

Frage: Wieviele quadratische Zahlkörper $\mathbb{Q}(\sqrt{d})$ gibt es mit

$$|d| \leq x \qquad \text{für} \qquad x \longrightarrow \infty \text{ ?}$$

Zähle quadratfreie $d \in \mathbb{N}$, $|d| \leq x$.

Bekannt: Anzahl asymptotisch zu $\zeta(2)^{-1}\, x$,

$\zeta(s)$ = Riemannsche ζ-Funktion.

Heuristisches Argument:

Sei $p \in \mathbb{P}$ Primzahl. Jede p^2-te Zahl ist durch p^2 teilbar. Also:
$\prod_{p\in\mathbb{P}}(1-\frac{1}{p^2})$ aller Zahlen quadratfrei.

$$\text{Mit} \qquad \frac{1}{1-\frac{1}{p^2}} = \sum_{k=0}^{\infty} \frac{1}{p^{2k}}$$

folgt

$$\left(\prod_{p\in\mathbb{P}}(1-\frac{1}{p^2})\right)^{-1} = \prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p^2}}$$
$$= \prod_{p\in\mathbb{P}} \sum_{k=0}^{\infty} \frac{1}{p^{2k}}$$
$$= \sum_{n\in\mathbb{N}} \frac{1}{n^2} = \zeta(2).$$

Somit

$$\#\{\text{quadratfreie } d \in \mathbb{N},\ d \le x\} \ \sim \ \frac{1}{\zeta(2)}x.$$

(Hier $f(x) \sim g(x)$ falls $\lim_{x\to\infty}\frac{f(x)}{g(x)} = 1$.)

Galoisgruppen

Nun: allgemeine Zahlkörper $K/\mathbb{Q}$ mit fester Galoisgruppe

$$G = \mathsf{Gal}(K/\mathbb{Q})$$

(als Permutationsgruppe auf den Einbettungen in einen algebraischen Abschluss von $\mathbb{Q}$).

Sei

$$N(\mathbb{Q},G;x) := \\ \#\{K/\mathbb{Q} \mid \mathsf{Gal}(K/\mathbb{Q}) = G,\ |D(K/\mathbb{Q})| \leq x\},$$

wobei $D(K/\mathbb{Q})$ die Körperdiskriminante von $K/\mathbb{Q}$ bezeichnet.

Frage: Asymptotik von $N(\mathbb{Q},G;x)$ für $x \to \infty$?

Falls $[K:\mathbb{Q}] = n \Longrightarrow$
G Permutationsgruppe auf n Symbolen, also $G \leq \mathfrak{S}_n$ (symmetrische Gruppe).

Eine Vermutung

Vermutung: (M. 2002) *Es gibt* $c_G > 0$ *mit*

$$N(\mathbb{Q}, G; x) \sim c_G \; x^{a(G)} \; (\log x)^{b(G)}$$

für gewisse explizit bekannte $a(G)$, $b(G)$.

Definition von $a(G)$:

Für $1 \neq g \in \mathfrak{S}_n$ sei

$\mathrm{ind}(g) := n - \#\text{Bahnen von } g \text{ auf } \{1, \ldots, n\}$,

$$a(G) := \frac{1}{\min\{\mathrm{ind}(g) \mid 1 \neq g \in G\}}.$$

$$b(G) := \ldots$$

(hängt von der Anzahl der Elemente von minimalem Index ab).

Resultate

Satz: (Wright 1989)
Die Vermutung gilt für alle abelschen Gruppen.

Beweis mit Klassenkörpertheorie

Satz: (Klüners 2004)
Die Vermutung gilt für verallgemeinerte Quaternionengruppen

$$Q_{4m} := \langle x, y \mid x^{2m} = 1, y^2 = x^m, x^y = y^{-1} \rangle$$

$m = 2^f$, $f \geq 1$.

Satz: (Klüners–M. 2004)
Abschwächung der Vermutung gilt für alle nilpotenten Gruppen.

Ad hoc Argumente für Gruppen $G \neq \mathfrak{A}_4$ vom Grad $n \leq 4$, sowie für $\mathfrak{S}_5$ (Bhargava, Cohen et al., Davenport-Heilbronn).

Ursprung der Vermutung:

Heuristische Überlegungen und ausgedehnte Computerexperimente (Erstellen von Tabellen von Zahlkörpern mit beschränkter Diskriminante).

Satz: (M. 2006) *Es gibt genau 389 013 654 total reelle primitive Zahlkörper der Diskriminante höchstens* 10^9.

Erzeugung der Zahlkörper durch:

- Klassenkörpertheorie (z.B. relativ-quadratische)
- Satz von Hunter (bei primitiven Gruppen)

Computeralgebrasysteme:

- KANT
- Pari-gp

Total reelle Zahlkörper kleinen Grades

n	G	vollst. bis	Anzahl
3			
	$\mathfrak{A}_3$	10^{16}	15 852 618
	$\mathfrak{S}_3$	10^{7}	592 421
4			
	Z_4	10^{14}	607 589
	V_4	10^{12}	769 284
	D_4	10^{9}	4 903 607
	$\mathfrak{A}_4$	10^{14}	1 232 860
	$\mathfrak{S}_4$	10^{9}	17 895 702
5			
	$\mathfrak{A}_5$	10^{11}	8 121
	$\mathfrak{S}_5$	10^{9}	2 341 055
6			
	$\mathfrak{A}_4$	10^{16}	127 140
	$\mathfrak{S}_4(T_7)$	10^{12}	39 215
	$\mathfrak{S}_4(T_8)$	10^{14}	26 008
	$\mathfrak{A}_5$	10^{11}	720
	$\mathfrak{A}_6$	10^{10}	159
	$\mathfrak{S}_6$	10^{9}	147 553

Cohen-Lenstra-Martinet Heuristik

Cohen und Lenstra (1983) geben eine Heuristik für die Klassengruppen quadratischer Zahlkörper.

Einzige bewiesene Fälle: 3-Rang (Davenport-Heilbronn) und 4-Rang (Fouvry-Klüners).

Cohen und Martinet (1990) erweitern dies auf Zahlkörper beliebigen Grades.

Experimentelle Resultate:
Durchschnittlicher p-Rang der Klassengruppe von Z_3-Körpern mit Diskriminante $\leq D$:

D	$p=2$	$p=5$	$p=7$
10^7	$1,275$	$1,000$	$1,155$
10^9	$1,361$	$1,043$	$1,212$
10^{11}	$1,415$	$1,045$	$1,267$
10^{13}	$1,448$	$1,048$	$1,289$
10^{15}	$1,470$	$1,045$	$1,301$
[C-M]	$1,250$	$1,040$	$1,306$

Zusammenhang zur Asymptotik-Vermutung

$\mathfrak{A}_4$ ist semidirektes Produkt

$$1 \longrightarrow Z_2^2 \longrightarrow \mathfrak{A}_4 \longrightarrow Z_3 \longrightarrow 1$$

$\mathfrak{A}_4$-Erweiterung $N/\mathbb{Q}$ vom Grad 6 ist quadratische Erweiterung eines Z_3-Körpers $L/\mathbb{Q}$.

Elemente der Ordnung 2 in der Klassengruppe von L führen zu unverzweigten $\mathfrak{A}_4$-Erweiterungen von L.

Hat die Klassengruppe von L hohen 2-Rang, so gibt es viele $\mathfrak{A}_4$-Körper über L mit gleicher Diskriminante.

Asymptotik für $\mathfrak{A}_4$ hängt also eng mit C-L-M Heuristik für Z_3-Körper zusammen.