Computing the Hilbert Class Field of Real Quadratic Fields

joint work with H. Cohen

Methods for computing class fields

Genus field theory

M. Ishida, *The Genus Fields of Algebraic Number Fields*, LN in Math. **555**, Springer-Verlag, 1976

Complex multiplication

R. Schertz, *Problèmes de Construction en Multiplication Complexe*, Sém. th. Nombres Bordeaux (1992), 239–262

Kummer theory

C. Fieker, *Computing Class Fields via the Artin Map*, preprint 1997

Stark's conjectures

H. Stark, *Values of L-functions at* $s = 1$. *III. Totally Real Fields and Hilbert's Twelfth Problem*, Advances in Math. **22** (1976), 64–84

H. Cohen, X.-F. Roblot, *Computing the Hilbert Class Field of Real Quadratic Fields* submitted to Math. Comp.

A special case of Stark's conjectures

Assume the Abelian rank one stark conjecture. Then there exists a unit $\varepsilon \in K$ such that:

$$\sigma(\varepsilon) = e^{-2\zeta'(0,\sigma)}$$

for all $\sigma \in G$. Futhermore, if we set $\alpha = \varepsilon + \varepsilon^{-1}$, we have:

$$H_k = k(\alpha) = \mathbb{Q}(\alpha)$$

and for any infinite place w of H_k wich does not divide v:

$$|\alpha|_w \leq 2.$$

Hecke L-functions

Definition

For $s \in \mathbb{C}$ with $Re(s) > 1$:

$$L(s, \chi) = \prod_{\mathfrak{p}} (1 - \chi(\mathfrak{p}) \mathcal{N}\mathfrak{p}^{-s})^{-1}$$

Relation with ζ-functions

For all $\sigma \in G$:

$$\zeta(s, \sigma) = \frac{1}{[K:k]} \sum_{\chi \in \hat{G}} L(s, \chi) \overline{\chi}(\sigma).$$

Functional equation

Define

$$\Lambda(s, \chi) = C^s \Gamma(s/2) \Gamma\left(\frac{s+1}{2}\right) L(s, \chi)$$

where

$$C = \frac{\sqrt{D \mathcal{N} \mathfrak{f}}}{\pi}.$$

Then for all $s \in \mathbb{C}$:

$$\Lambda(s, \chi) = W(\chi) \Lambda(1 - s, \overline{\chi}).$$

A refinement of a theorem of Friedman

For all $n \geq 1$, define:

$$a_n(\chi) = \sum_{\mathcal{N}\mathfrak{a}=n} \chi(\mathfrak{a})$$

and

$$T(\chi) = \sum_{n\geq 1} a_n(\overline{\chi}) \frac{C}{2n} e^{-\frac{2n}{C}}$$

$$S(\chi) = \sum_{n\geq 1} a_n(\chi)\,\mathrm{Ei}(2n/C)$$

where Ei denotes the exponential integral function.

Then we have:

$$L'(0,\chi) = S(\chi) + W(\chi)T(\chi).$$

Computation of the $a_n(\chi)$

Prime power case

1. p is inert, $a_{p^m} = \chi(p)^m$
2. $p\mathcal{O}_k = \mathfrak{p}^2$ is ramified, $a_{p^m} = \chi(\mathfrak{p})^{2m}$
3. $p\mathcal{O}_k = \mathfrak{p}\mathfrak{p}'$ is split,
   (a) if $\chi(\mathfrak{p}) = \chi(\mathfrak{p}')$, $a_{p^m}(\chi) = (m+1)\chi(\mathfrak{p})^m$
   (b) otherwise,

$$a_{p^m}(\chi) = \frac{\chi(\mathfrak{p})^{m+1} - \chi(\mathfrak{p}')^{m+1}}{\chi(\mathfrak{p}) - \chi(\mathfrak{p}')}.$$

General case

Write $n = p_1^{m_1} \dots p_r^{m_r}$ then

$$a_n(\chi) = a_{p_1^{m_1}}(\chi) \dots a_{p_r^{m_r}}(\chi).$$

An example

The ground field

$$\omega = \sqrt{438},\ k = \mathbb{Q}(\omega),\ D = 172,\ Cl_k \simeq C_4$$

The field K

$$\mathfrak{p} = 11\mathcal{O}_k + (-3+\omega)\mathcal{O}_k,\ K = k(\mathfrak{p}v),\ Gal(K/k) \simeq C_8$$

The polynomial

$$\tilde{A}(X) = X^4 - 2009298.2915480506125X^3 + 839444123.5847875937X^2 - 40221955871.31370562X + 23416101 7552.69584759$$

$$A(X) = X^4 + (-48004\omega - 1004649)X^3 + (20055096\omega + 419722059)X^2 + (-960939696\omega - 20110977936)X + (5594323104\omega + 117080508780)$$

Reduced polynomial

$$X^4 + 2X^3 + (\omega - 25)X^2 + (-\omega + 22)X + (-3\omega + 63)$$

$$X^4 - 2X^3 - 5X^2 + 6X + 3$$

Tables

All non principal real quadratic fields of discriminant $\leq 10\,000$: 1761 fields with class numbers from 2 to 27

Implementation in PARI/GP

Computation of Hilbert class field of real quadratic fields: function `quadhilbert`.

Computation of real class fields of totally real number fields: function `bnrstark` (still in development).

Thank you for your attention