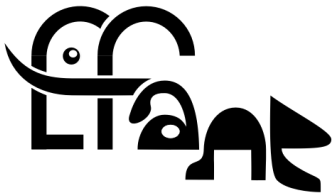
Shimura class groups with GP

Andreas Enge

LFANT project-team
INRIA Bordeaux–Sud-Ouest
andreas.enge@inria.fr
http://www.math.u-bordeaux1.fr/~enge

Atelier Pari/GP, Besançon, 09/01/2014
(with Emmanuel Thomé)



Quartic CM fields and CM types

- CM field: imaginary-quadratic extension of a totally real number field

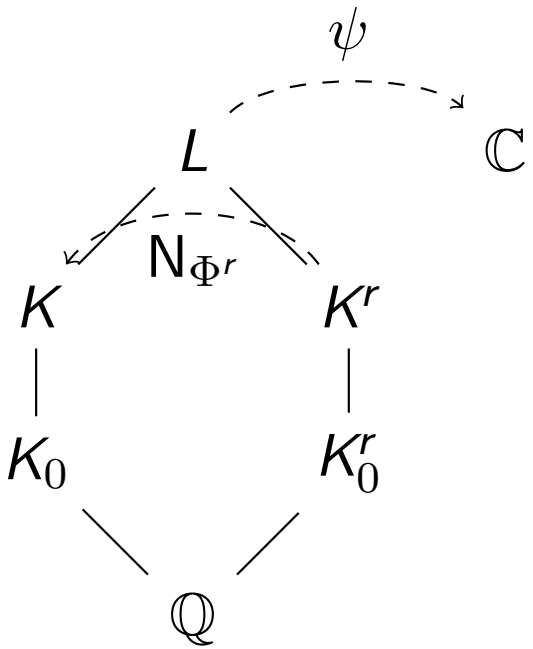
$$K = K_0\left(\pm\sqrt{\tfrac{-A\pm\sqrt{D}}{2}}\right) = \mathbb{Q}[Y]/(Y^4 + AY^2 + B)$$
$$\Big|$$
$$K_0 = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}[Z]/(Z^2 + AZ + B)$$
$$\Big|$$
$$\mathbb{Q}$$

  $D = A^2 - 4B > 0$

- CM type $\Phi = (\varphi_1, \varphi_2)$ embeddings of K into $\mathbb{C}$, $\overline{\varphi}_2 \neq \varphi_1$
- Reflex field

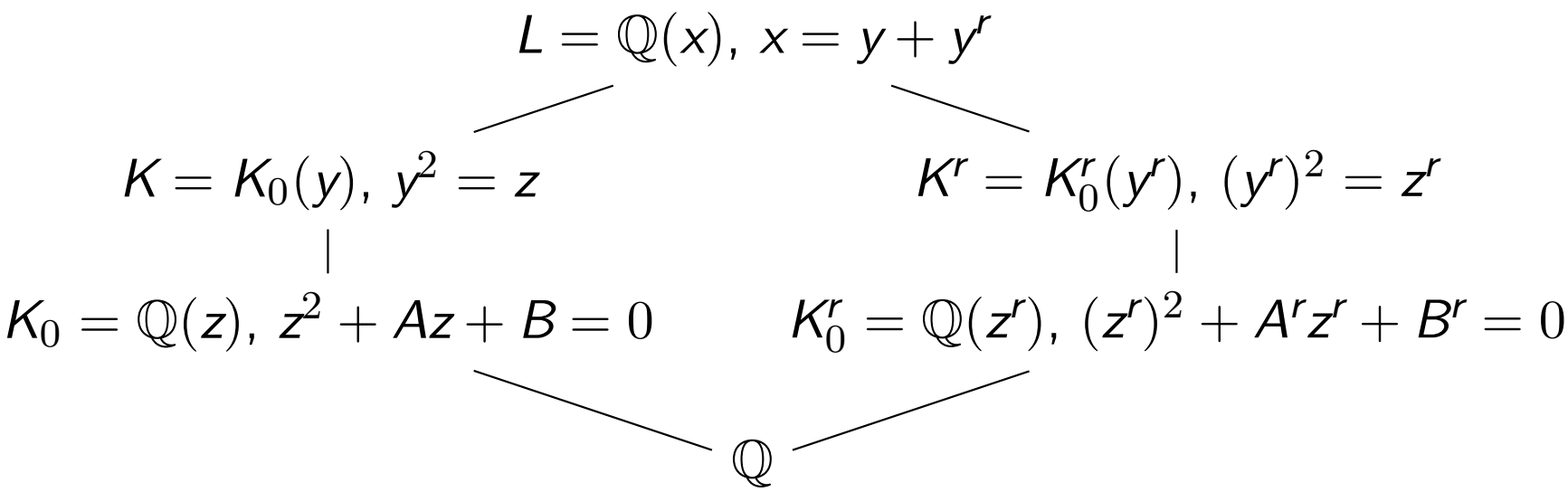
$$\begin{aligned} K^r &= K(\{\varphi_1(x) + \varphi_2(x) : x \in K\}) \\ &= \mathbb{Q}[Y^r]/((Y^r)^4 + A^r(Y^r)^2 + B^r),\ A^r = 2A,\ B^r = A^2 - AB \end{aligned}$$

Fields and maps (typical case)



$$\mathsf{N}_{\Phi^r}(\mathfrak{b}) = \mathsf{N}_{L/K}(\mathfrak{b}\mathcal{O}_L)$$

Explicit fields (typical case)




```
init_cmfield_basic
complex_conjugate_element
complex_norm
complex_conjugate_ideal
type_norm
```

Do we need more on number field diagrams?

CM points and class polynomials

- Admissible pair (modulo principality)
  $(\mathfrak{a}, \xi)$ s.t. $(\mathfrak{a}\bar{\mathfrak{a}}\mathcal{D}_{K/\mathbb{Q}})^{-1} = (\xi)$, $\varphi_1(\xi), \varphi_2(\xi) \in i\mathbb{R}_{>0}$
- Polarisation $E_{\Phi,\xi} : \Phi(K)^2 \to \mathbb{C}, (\Phi(x), \Phi(y)) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(\xi\bar{x}y)$
  symplectic form $\mathbb{C}^2 \to \mathbb{R}$
- Period matrix
  $(\mathfrak{a}, \xi) \rightsquigarrow \tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix}$ with $\Im(\tau)$ positive definite

$$\tau \in (K^r)^{2\times 2}$$

- Igusa class polynomial

$$\prod_{\Phi,\mathfrak{a},\xi} (X - i_1(\tau)) \in \mathbb{Q}[X]$$

$$\prod_{\mathfrak{a},\xi} (X - i_1(\tau)) \in K_0^r[X]$$

Shimura class group and typenorm subgroup

- Shimura class group

$$\mathfrak{C}(K) = \{(\mathfrak{c}, u) : \mathfrak{c}\bar{\mathfrak{c}} = u\mathcal{O}_K, u \gg 0\} / \mathcal{P}(K)$$

  acts regularly on admissible triples for given Φ

- Reflex type norm subgroup, image of

$$\begin{aligned} \mathrm{N}_{\Phi^r} : \mathrm{Cl}_{K^r} &\to \mathfrak{C}, \\ \mathfrak{b} &\mapsto \left(\mathrm{N}_{\Phi^r}(\mathfrak{b}), \mathrm{N}(\mathfrak{b})\right), \end{aligned}$$

  gives irreducible factor of Igusa class polynomial

`shimura_subgroup` in `shimura-naive.gp`

Shimura class group from abstract groups

$$1 \longrightarrow \mathcal{O}_{K_0}^+ / N_{K/K_0}(\mathcal{O}_K^*) \xrightarrow{u \mapsto (\mathcal{O}_K, u)} \mathfrak{C} \xrightarrow{(\mathfrak{a},\alpha)\mapsto\mathfrak{a}} \mathrm{Cl}_K \xrightarrow{N_{K/K_0}} \mathrm{Cl}_{K_0}^+ \longrightarrow 1$$

1. Compute a matrix M for $\mathrm{N}_{K/K_0} : \mathrm{Cl}_K \to \mathrm{Cl}_{K_0}^+$.
2. Compute generators $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ of the kernel of M.
3. Compute a basis for the lattice L_0 of relations such that the subgroup of Cl_K generated by $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ is isomorphic to $\mathbb{Z}^r/L_0$.
4. Lift $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ to $\mathfrak{C}$: Pick arbitrary totally positive $\alpha_i \in K_0$ such that $\mathfrak{a}_i\bar{\mathfrak{a}}_i = \alpha_i\mathcal{O}_{K_0}$.
5. If $\mathcal{O}_{K_0}^+ / \mathrm{N}_{K/K_0}(\mathcal{O}^*) = 1$, let $r' = r$; otherwise let $r' = r+1$ and $(\mathfrak{a}_{r'}, \alpha_{r'}) = (\mathcal{O}_K, \epsilon_0)$.
6. Expand the basis of 3) into a basis for the lattice L of relations between the generators $(\mathfrak{a}_1, \alpha_1), \ldots, (\mathfrak{a}_{r'}, \alpha_{r'})$ such that $\mathfrak{C} \simeq \mathbb{Z}^{r'}/L$.
7. Determine a polycyclic basis of $\mathfrak{C}$.

`shimura_group_identity_element`, `shimura_group_structure` etc.

Type norm subgroup from abstract groups

- Have generalised discrete logarithms in $\mathfrak{C}$ from exact sequence (and Smith transformation matrix).
  `shimura_group_element_dlog`
- Compute image of

$$\mathrm{Cl}_{K^r} \xrightarrow{\mathsf{N}_\Phi} \mathfrak{C}$$

  - generalised discrete logarithms in $\mathfrak{C}$ of generators of Cl_{K^r}
  - relations between images: HNF
  - polycyclic basis: SNF

  `shimura_group_type_norm_subgroup`
- Compute cosets of image

Can all this be made more automatic? Exported from Pari to GP?

Running times

"Record" example

```
#
\r shimura.gp
A=1357; B=3299;
cm=init_cmfield (A, B);
\r shimura-naive.gp
cm=init_cmfield (A, B);
C=shimura_subgroup (cm);
```

Running times

"Record" example

```
#
\r shimura.gp
A=1357; B=3299;
cm=init_cmfield (A, B);
\r shimura-naive.gp
cm=init_cmfield (A, B);
C=shimura_subgroup (cm);
```

Then 7 minutes for symbolic period matrices.
Then 9 days on up to 640 cores for class polynomials.

Software

http://cmh.gforge.inria.fr/

- GPLv3+