Explicit computations in Iwasawa theory

Reinier Broker
Center for Communications Research, Princeton

Joint with David Hubbard, Larry Washington

Two extensions

Let $K/\mathbf{Q}$ be imaginary quadratic, and $p \in \mathbf{Z}$ prime.

There are two "distinguished" $\mathbf{Z}_p$-extensions of K according to how $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ acts on the Galois group:

- $+1$-eigenspace: *cyclotomic* $\mathbf{Z}_p$-extension
- -1-eigenspace: *anticyclotomic* $\mathbf{Z}_p$-extension.

These two extensions are linearly disjoint over K for $p \geq 3$. Computing layers of the cyclotomic $\mathbf{Z}_p$-extension is well-understood.

Today. Focus on the *anticyclotomic* extension. Fix $p = 3$ and assume that 3 ramifies in K.

Anticyclotomic $\mathbf{Z}_3$-extension

Let K_n be the n-th layer of the anticyclotomic $\mathbf{Z}_3$-extension.

We have

$$\mathrm{Gal}(K_n/K) \cong C_{3^n} \quad \text{and} \quad \mathrm{Gal}(K_n/\mathbf{Q}) \cong D_{3^n}.$$

Goal. Given n, compute $f \in K[X]$ with $K[X]/(f(X)) \cong K_n$.

In paper. Two approaches: using CM-theory and using Kummer theory. We focus on CM-theory in this talk.

Ring class fields

For $m \geq 0$, let

$$\mathcal{O}_m = \mathbf{Z} + 3^m \mathcal{O}_K$$

be the order of index 3^m inside the maximal order $\mathcal{O}_K$.

The Picard group

$$\mathrm{Pic}(\mathcal{O}_m) = \frac{\{\text{ fractional invertible } \mathcal{O}_m\text{-ideals }\}}{\{\text{ principal } \mathcal{O}_m\text{-ideals }\}}$$

is a finite abelian group, just like the class group $\mathrm{Pic}(\mathcal{O}_0)$.

By class field theory, there is a unique extension H_m such that the Artin map induces

$$\mathrm{Pic}(\mathcal{O}_m) \xrightarrow{\sim} \mathrm{Gal}(H_m/K).$$

Ring class fields, part II

The Galois group $\mathrm{Gal}(H_m/\mathbf{Q})$ is generalized dihedral.

Lemma. (Bruckner) $K_n \subset H_m$ for some m.

Questions.

- $\diamond$ Which m?
- $\diamond$ Which subfield?
- $\diamond$ How to compute everything?

Galois groups and local unit groups

Restriction. Restrict to $-3 > \mathrm{disc}(\mathcal{O}_K) \equiv -3 \bmod 9$.

We have

$$1 \to (\mathcal{O}_K/3^m\mathcal{O}_K)^*/(\mathbf{Z}/3^m\mathbf{Z})^* \to \mathrm{Pic}(\mathcal{O}_m) \to \mathrm{Pic}(\mathcal{O}_K) \to 1,$$

and $\mathrm{Gal}(H_m/H_0) \cong \mathrm{Ker}(\mathrm{Pic}(\mathcal{O}_m) \to \mathrm{Pic}(\mathcal{O}_K))$.

We will analyze this kernel first, and then "descend" from H_m/H_0 to K.

An almost cyclic group

Lemma. $(\mathcal{O}_K/3^m\mathcal{O}_K)^*/(\mathbf{Z}/3^m\mathbf{Z})^* \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3^{m-1}\mathbf{Z}$ *for* $m \geq 1$.

Proof: Localize at $P|(3)$ to get the ramified extension $A = \mathbf{Z}_3[\zeta_3]$ of $\mathbf{Z}_3$. We have

$$A^* = \langle -\zeta_3 \rangle \times (1 + P^2).$$

The module $(1 + P^2)$ is torsion free, and hence free of rank 2. We get

$$(A/3^m A)^* \cong \langle -\zeta_3 \rangle \times (1 + P^2)/(1 + P^{2m}) \cong \mathbf{Z}/6\mathbf{Z} \times (\mathbf{Z}/3^{m-1}\mathbf{Z})^2.$$

Now quotient by $(\mathbf{Z}/3^m\mathbf{Z})^* \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3^{m-1}\mathbf{Z}$. □

Consequences so far

Assume that 3 does not divide the class number of K.

To compute K_n, we can:

- $\diamond$ compute H_{n+1}
- $\diamond$ take the unique subfield $\widetilde{K}_{n+1}$ of degree 3^{n+1} over K
- $\diamond$ select the right index 3 subfield of $\widetilde{K}_{n+1}$.

Towards computing

Three questions:

1. How do we compute ring class fields?

2. How do we pick out the right subfield?

3. What do we do if $\#\mathrm{Pic}(\mathcal{O}_K)$ is divisible by 3?

Three high-level answers:

1. CM-theory + Shimura reciprocity.

2. Class field theory.

3 Galois theory.

CM-theory

Theorem. *We have* $H_n = K(j(\mathbf{C}/\mathcal{O}_n))$, *with* j *the* j*-invariant of the elliptic curve* $\mathbf{C}/\mathcal{O}_n$.

Computing the minimal polynomial of $j(\mathbf{C}/\mathcal{O}_n)$ is well-understood.

Two drawbacks:

- ◇ the run time is exponential in $|\mathrm{disc}(\mathcal{O}_n)|$
- ◇ the minimal polynomial has *very large* coefficients.

Smaller functions

The exponential run time cannot be helped.

However, instead of j, we can use a modular function of higher *level*. This goes back to Weber; the modern tool to use is *Shimura reciprocity*.

For any $\mathcal{O}_n = \mathbf{Z}[\tau]$, we can find a modular function h such that

$$H_n = K(h(\tau))$$

and the minimal polynomial of $h(\tau)$ has smaller coefficients than that of $j(\tau)$.

Smaller modular functions, example

For $\mathrm{disc}(\mathcal{O}_0) = -39$, the constant term of the minimal polynomial of $j(\mathbf{C}/\mathcal{O}_0)$ equals

$$20919104368024767633.$$

For $h = (\sqrt{2}\eta(2z)/\eta(z))^3$ we obtain the minimal polynomial

$$X^4 + 2X^3 + 4X^2 + 3X - 1.$$

Note. For $\mathrm{disc}(\mathcal{O}_n) \to -\infty$, we gain a *constant factor* in the size of the coefficients.

Picking out the right subfield

We can compute H_{n+1}, and its unique subfield $\widetilde{K}_{n+1}$ with $[\widetilde{K}_{n+1} : K] = 3^{n+1}$. One of its index 3 subfields is the K_n we are after.

The proof of

$$\mathrm{Gal}(\widetilde{K}_{n+1}/K) \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3^n\mathbf{Z}$$

gives a method to find the right subfield.

Let $\alpha_{n+1} \in \mathcal{O}_K$ be locally congruent to $\zeta_3 \bmod 3^{n+1}$. Then: the fixed field for the *Artin symbol* of α_{n+1} equals K_n.

Example: $K = \mathbf{Q}(\sqrt{-21})$

We have $\mathrm{Pic}(\mathcal{O}_0) \cong (\mathbf{Z}/2\mathbf{Z})^2$, and $\mathrm{Pic}(\mathcal{O}_1) \cong (\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})^2$.

The index 4 subfield of H_1 is generated by $X^3 - 6X - 12$. It is *not* part of the anticyclotomic $\mathbf{Z}_3$-extension of K.

We have $\mathrm{Pic}(\mathcal{O}_2) \cong (\mathbf{Z}/3\mathbf{Z})^2 \times (\mathbf{Z}/2\mathbf{Z})^2$. The index 4 subfield of H_2 is generated by

$$X^9 + 12X^6 + 81X^5 + 144X^4 + 30X^3 - 324X^2 - 504X - 336.$$

The element $\alpha_2 = 1 + \sqrt{-21}$ is locally congruent to ζ_3 mod 9. The fixed field of its Artin symbol equals K_1. It is generated by

$$X^3 + 9X - 12.$$

What if $3 \mid \#\mathbf{Pic}(\mathcal{O}_0)$?

Let L_n be the fixed field of $\widetilde{K}_{n+1}$ for the Artin symbol of α_{n+1}, with α_{n+1} locally congruent to ζ_3 mod 3^{n+1}. (So: $\mathrm{Gal}(L_n/H_0) \cong C_{3^n}$.)
Observation: if

$$1 \to \mathrm{Gal}(L_n/H_0) \to \mathrm{Gal}(L_n/K) \to \mathrm{Gal}(H_0/K) \to 1$$

splits, then H_0 is disjont from the anticyclotomic $\mathbf{Z}_3$-extension.

If it does not split, we need to look at the "maximal subgroup" of $\mathrm{Gal}(H_0/K)$ for which the corresponding sequence splits. See paper.

Two examples

Example 1. $K = \mathbf{Q}(\sqrt{-87})$. We have $\mathrm{Pic}(\mathcal{O}_1) \cong \mathbf{Z}/18\mathbf{Z}$ and $\mathrm{Pic}(\mathcal{O}_0) \cong \mathbf{Z}/6\mathbf{Z}$. The sequence becomes

$$1 \to \mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}/18\mathbf{Z} \to \mathbf{Z}/6\mathbf{Z} \to 1.$$

This is evidently nonsplit. Hence: the 3-Hilbert class field of K equals K_1.

Example 2. For $K = \mathbf{Q}(\sqrt{-771})$ we obtain

$$1 \to \mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z} \to \mathbf{Z}/6\mathbf{Z} \to 1.$$

The Hilbert class field is disjoint from K_1.

Future work

Two follow-up projects:

- ◇ $p = 2$. More technical; nearly complete.
- ◇ general $p \neq 2$. Much easier. To be done soon.