Computing class groups and unit groups in magma

Andreas-Stephan Elsenhans

Universität Würzburg – University of Sydney

July 2026

Joint work with John Voight

Start

Types of algorithms

1. Heuristic algorithms (not proven to be correct)
2. Randomised algorithms (fast/correct with high probability)
3. Conditional algorithms (e.g., relative to GRH)
4. Rigorous algorithms (e.g., proven floating point precision)
5. Formalisable algorithms (e.g., using ball arithmetic)
6. Formalised algorithms (e.g., generate a proof in Lean)

Our project

- Place the class group algorithms into the above scheme.
- Update to the latests GRH-conditional results.
- Systematic testing – fix what we find.

Algebraic number theory in `magma` dates back to the 1990's.

Setup

Problem
Given the maximal order $\mathcal{O}_K$ of a number field $K = \mathbb{Q}[X]/f$, compute the class group and the unit group of $\mathcal{O}_K$.

Earlier Work
The generation of Zassenhaus, Pohst, Cohen, Buchmann and plenty others spend at lot of time on the question.

Application
Various problems such as the computation of Mordell-Weil groups and class fields require class groups and unit groups.

The structure as abstract groups

Theorem (Dirichlet)
Let K be a number field with r_1 distinct real embeddings and r_2 pairs of complex conjugate embeddings. Then we have

$$\mathcal{O}_K^\times \cong \mu \times \mathbb{Z}^{r_1+r_2-1}.$$

Here, μ is the finite group of roots of unity contained in K.

Theorem
The quotient of multiplicative semigroups

$$\mathrm{Cl}(\mathcal{O}_K) := \frac{\text{non-zero ideals of } \mathcal{O}_K}{\text{non-zero principal ideals of } \mathcal{O}_K}$$

is a finite abelian group. It is called *class group*.

Data structures
Finitely generated abelian groups are well supported by using $\mathbb{Z}$-linear algebra in `magma`.

More on the groups

The unit group as a lattice
Applying logarithms to the absolute values of the real and complex images maps the unit group to a lattice of rank $r_1 + r_2 - 1$.

The covolume of this lattice is called *regulator*.

Cohen-Lenstra Heuristic for class groups
The probability that an abelian group A is the class group is proportional to $\frac{1}{\#\mathrm{Aut}(A)}$.

Interpretation
The trivial group and $\mathbb{Z}/2\mathbb{Z}$ are the most frequent class groups. Further, cyclic groups are frequent.

More on the groups II

Theorem (Minkowski)
Every ideal class of $\mathcal{O}_K$ has a representative $\mathfrak{a}$ with

$$\|\mathfrak{a}\| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} \cdot \sqrt{|\mathrm{disc}(\mathcal{O}_K)|}\,.$$

Remark

- Note that the right hand side is $O(\sqrt{|D|})$, but the constant is very small, e.g. (n = 10) results in 0.0012.
- Zimmert's result yields an even smaller constant.

Theorem (Gauss, Dirichlet, Kummer, . . .)
For every number field K we have

$$\operatorname*{res}_{s=1} \zeta_K(s) = \frac{2^{r_1+r_2}\pi^{r_2}\mathrm{Reg}(\mathcal{O}_K)\mathrm{h}(\mathcal{O}_K)}{w\sqrt{|\mathrm{disc}(\mathcal{O}_K)|}}\,.$$

Here, w is the number of roots of unity in K.

Computing the residue

Theorem
The infinite product

$$\operatorname*{res}_{s=1} \zeta_K(s) = \lim_{s\to 1}\frac{\zeta_K(s)}{\zeta(s)} = \prod_{p\in\mathbb{P}} \frac{1-\frac{1}{p}}{\prod_{\mathfrak{p}|p} 1-\frac{1}{\|\mathfrak{p}\|}}$$

converges. An explicit unconditional estimate for the speed of convergence is known.

Eric Bach gave a GRH-conditional estimate for the speed of convergence.

Using modularity
One can compute the residue by using Tim Dokchitser's package. The complexity is $O(\sqrt{|D|})$. This is only practical for small discriminants.

Interpretation
One can compute the product $\mathrm{Reg}(\mathcal{O}_K)\mathrm{h}(\mathcal{O}_K)$ in an analytic way.

A summation scheme

Notation

$$A_K(X) := \sum_{\substack{\mathfrak{p}\subset\mathcal{O}_K \\ N(\mathfrak{p}^m)<X}} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^{m/2}}\left(\frac{\sqrt{X}\log(X)}{N(\mathfrak{p})^{m/2}\log(N(\mathfrak{p})^m)} - 1\right)$$

$$f_K(X) := \frac{3(A_K(X) - A_{\mathbb{Q}}(X) + A_{\mathbb{Q}}(X/9) - A_K(X/9))}{2\sqrt{X}\log(3X)}$$

Assuming GRH

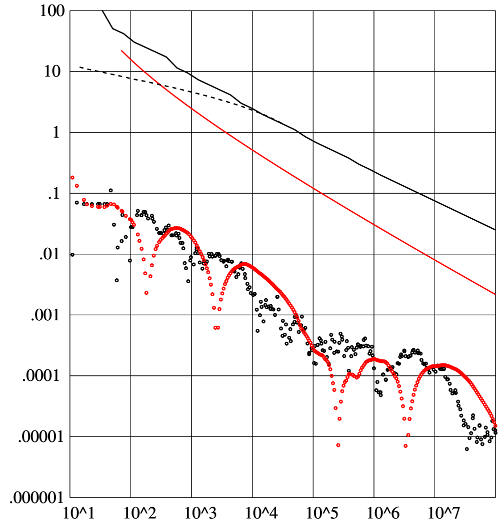
Theorem (Belabas, Friedman, Bach)
Let K be a degree n number field and D its discriminant.

$$\left|\log\left(\operatorname*{res}_{s=1}\zeta_K(s)\right) - f_K(X)\right| \leq \frac{2.324\log(|D|)}{\sqrt{X}\log(3X)}C$$

$$C := \left(\left(1+\frac{3.88}{\log(X/9)}\right)\left(1+\frac{2}{\sqrt{\log|D|}}\right)^2 + \left(\frac{4.26(n-1)}{\sqrt{X}\log|D|}\right)\right)$$

Conclusion
Assuming GRH, one can compute a sufficient approximation and use the analytic class number formula.

Experimental rate of convergence

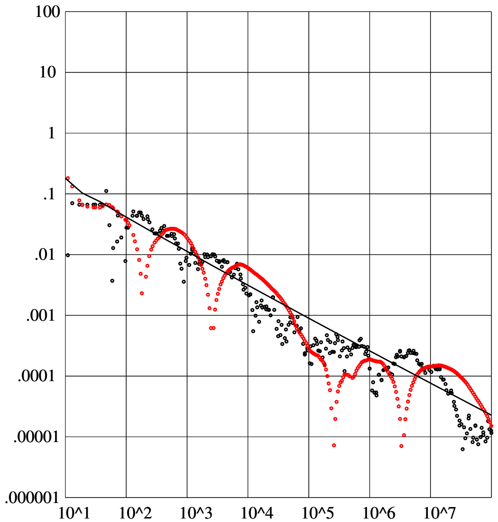


$$f = t^8 + 9127t^3 + 9127t^2 + 9127t + 18254,$$
$$\Delta = -2.5917 \cdot 10^{44}$$

Black dots: Error of Euler product
Black line: Bach's GRH-estimate
Dashed line: Combined estimate

Red dots: Error of summation scheme
Red line: Belabas's GRH-estimate

Comparison with random Euler products



Black line: Standard deviation of random Euler products

Assuming GRH II

Theorem (Bach)

$$\left\{\mathfrak{p} \subset \mathcal{O}_K \,\middle|\, \|\mathfrak{p}\| \leq 12\left(\log|\mathrm{disc}(\mathcal{O}_K)|\right)^2\right\}.$$

generates $\mathrm{Cl}(K)$.

Remark
Belabas, Diaz y Diaz, Friedman and Grenie, Molteni proved further GRH bouds.

Remark
Not assuming GRH, no bound for a generating set of the class group is known. Thus, one has to use the Minkowski / Zimmert bound that gives a bound for all classes.

The factor base method

Definition
We call all the prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_\ell$ up to a given norm B a factor base with bound B.
We assume that the factor base generates the class group.

Remark
The map

$$\phi\colon \mathbb{Z}^\ell \to \mathrm{Cl}(K), (e_1, \dots, e_\ell) \mapsto [\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_\ell^{e_\ell}]$$

is surjective. If we know its kernel, we know the class group.

Relations
Assume a principal ideal (a) can be factored using only elements of the factor base, then we have an expression of the shape

$$(a) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_\ell^{e_\ell} \,.$$

This gives us $(e_1, \dots, e_\ell) \in \ker(\phi)$.

Using relations

Searching for relations
Many people have worked on different approaches to generate relations. For this talk it is sufficient to know, that we have some code that does it. The longer we run it, the more relations we get.

Connections to units
Assume that two elements lead to the same factorisation

$$(a) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_\ell^{e_\ell} = (b) \,.$$

Then, $\frac{a}{b}$ is a unit in $\mathcal{O}$.

Given sufficiently many relations

- One can compute a sublattice of $\ker(\phi)$.
- One can find units.

When to stop searching for relations?

Question
How does a lack of relations look like?

Units
If we miss units, the unit group does not have the expected rank or the covolume of the unit lattice (regulator) is larger than it should be.

Class group
If we miss relations, we have only a submodule of $\ker(\phi)$. Thus, the order $\mathbb{Z}^\ell / (\text{Known part of } \ker(\phi))$ is larger than the class number.

Conclusion
We are finished as soon as the product $\mathrm{h}(K) \cdot \mathrm{Reg}(K)$ is close to the GRH-conditional value.

Finishing class and unit group

Small units
By enumerating small elements in $\mathcal{O}_K$ one can find all small units. This results in a lower bound for the regulator.

Saturation
Now we have to check for ℓ-saturation

- of the unit group for all primes up to

$$\frac{\text{regulator found}}{\text{lower regulator bound}}$$

- of the relations of the class group for all $\ell \mid h$.

Both checks follow the same approach.

Check for saturation

Questions

Can we confirm that no ℓ-th root of a known unit is a new unit?
Given an ideal $(a) = I^\ell$, can we confirm that I is not principal?

Modulo $\mathfrak{p}$ analysis for ℓ-saturation

- Take sufficiently many (say m) prime ideals $\mathfrak{p}_i$ with $\ell \mid (\mathcal{O}/\mathfrak{p}_i)^\times$.
- A ℓ-th power of $\mathcal{O}^\times$ reduces to an ℓ-th power in $(\mathcal{O}/\mathfrak{p}_i)^\times$.
- A ℓ-th power is contained in an index ℓ^m subgroup of $\prod(\mathcal{O}/\mathfrak{p}_i)^\times$.
- The discrete logarithms maps each $(\mathcal{O}/\mathfrak{p}_i)^\times$ to $(\mathbb{Z}/\ell\mathbb{Z}, +)$.
- This turns a search for ℓ-th powers into linear algebra over $\mathbb{Z}/\ell\mathbb{Z}$.

Check for saturation II

Checking units

If only ℓ-th powers of known units map to the index ℓ^m subgroup, the unit group is ℓ-saturated.

Checking an ideal class

Determine all units u such that $u \cdot a$ maps to the index ℓ^m subgroup. If such a unit does not exist, I is not principal.

Remark

If the class group is non-cyclic, e.g., $(a) = I^\ell, (b) = J^\ell$, one has to work with $a^i \cdot b^j \cdot u$ instead.

Optimisation

The elements a, b are only computed modulo h-th powers.

Conclusion

Implementation

Since, 2025 a new implementation of the class group proof is available.

Interpretation

1. `magma` can compute class groups and unit groups GRH-conditionally.
2. `magma` can compute class groups formalisable.
3. `magma` can compute unit groups rigorous.

Thank you!