# Genus numbers of cubic fields and Heilbronn's criterion

Kevin McGown

California State University, Chico

December 17, 2016

Joint work with Amanda Tucker
(University of Rochester)

West Coast Number Theory Conference
Pacific Grove, California

# The class group of a number field

Let $K$ be a number field with ring of integers $\mathcal{O}_K$. The class group $\mathrm{Cl}_K = \mathcal{I}_K/\mathcal{P}_K$ measures the failure of unique factorization.

$$1 \to \mathcal{O}_K^* \to K^* \to \mathcal{I}_K \to \mathrm{Cl}_K \to 1$$

The class number is defined as $h_K = \#\,\mathrm{Cl}_K$.

## Example

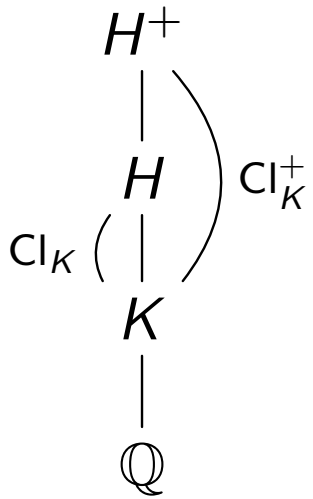
*The class group of* $K = \mathbb{Q}(\sqrt{-14})$ *equals*

$$\mathrm{Cl}_K = \left\{(1), (3, 1+\sqrt{-14}), (2, \sqrt{-14}), (3, 2+\sqrt{-14})\right\}$$

and thus we have $h_K = 4$.

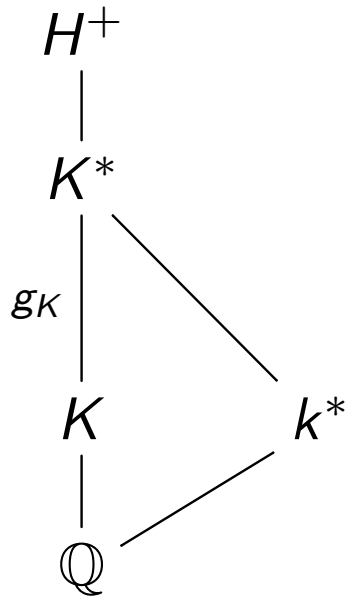
# The Hilbert class field

The Hilbert class field $H$ of $K$ is the maximal unramified abelian extension of $K$. By class field theory, the Galois group $\mathrm{Gal}(H/K)$ is isomorphic to the class group $\mathrm{Cl}_K$.



# The genus field

The genus field $K^*$ of $K$ is defined to be the maximal subfield of $H^+$ of the form $Kk^*$ where $k^*$ is absolutely abelian.




The genus number of $K$ is defined as $g_K = [K^* : K]$. It follows right away that $g_K$ divides $h_K^+$, where $h_K^+ = \#\,\mathrm{Cl}_K^+$ is the narrow class number of $K$.

# An example of the genus field of a quadratic field

$$
\begin{array}{c}
H^+ = \mathbb{Q}(\sqrt{2\sqrt{2}-1}, \sqrt{-7}) \\
| \\
K^* = \mathbb{Q}(\sqrt{2}, \sqrt{-7}) \\
| \quad g_K{=}2 \\
K = \mathbb{Q}(\sqrt{-14}) \\
| \\
\mathbb{Q}
\end{array}
$$

# An example of the genus field of a cubic field

- Let $\alpha$ denote a root of the polynomial $x^3 - x^2 - 9x + 8$.
- Then the field $K = \mathbb{Q}(\alpha)$ has discriminant $2597 = 7^2 \cdot 53$.
- It turns out that $k^* = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$.
- Thus the genus field in this case is $K^* = \mathbb{Q}(\alpha,\ \zeta_7 + \zeta_7^{-1})$.
- It follows that

$$\begin{aligned} g_K &= [K^* : K] \\ &= [\mathbb{Q}(\alpha,\ \zeta_7 + \zeta_7^{-1}) : \mathbb{Q}(\alpha)] \\ &= [\mathbb{Q}(\zeta_7 + \zeta_7^{-1}) : \mathbb{Q}] \\ &= 3 \end{aligned}$$

- Since $K$ is cubic, we have that $g_K$ divides $h_K$.

# Some data on cubic fields with $g_K = 1$

| $X$ | proportion of cubic fields with $0 < \Delta \leq X$ having $g_K = 1$ |
|---|---|
| $10^3$ | 0.8148 |
| $10^4$ | 0.9319 |
| $10^5$ | 0.9527 |
| $10^6$ | 0.9580 |
| $10^7$ | 0.9603 |
| $10^8$ | 0.9613 |
| $10^9$ | 0.9617 |

## Question

*What proportion of totally real cubic fields have $g_K = 1$?*

# Fröhlich's description of the genus number

Let $K$ be a totally real cubic field for the rest of this talk.

**Theorem (Fröhlich)**

*Let $e$ denote the number of odd primes $p$ such that $p$ is totally ramified in $K$ and $(d/p) = 1$, where $(d/p)$ is the usual Legendre symbol. Then we have:*

$$g_K = \begin{cases} 3^{e-1} & \text{if } K \text{ is cyclic} \\ 3^e & \text{if } K \text{ is not cyclic.} \end{cases}$$

Note that since the number of cyclic cubic fields with discriminant up to $X$ is $O(X^{1/2})$, for our purposes we may neglect these fields.

# Counting cubic fields

Our main tool is the following theorem, which is a strengthening of the classical Davenport–Heilbronn Theorem.

Theorem (Bhargava–Shankar–Tsimerman & Taniguchi–Thorne)

*The number of cubic fields satisfying* $0 < \Delta \leq X$ *equals*

$$\frac{1}{12\zeta(3)}X + \frac{4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O(X^{7/9+\varepsilon}).$$

# Proportion of cubic fields with genus number one

## Corollary (M., Tucker)

*The proportion of cubic fields with genus number one (of positive or negative discriminant) equals*

$$\frac{29\,\zeta(3)}{27\,\zeta(2)} \prod_{p \equiv 2 \pmod 3} \left(1 + \frac{1}{p(p+1)}\right) \approx 0.9623\,.$$

*Consequently, roughly* 96.23% *of totally real cubic fields and* 96.23% *of complex cubic fields have genus number one.*

# Norm-Euclidean cubic fields (cyclic)

Our initial motivation for looking at genus numbers was the study of norm-Euclidean fields.

### Definition

*A number field $K$ is called norm-Euclidean if the ring $\mathcal{O}_K$ is Euclidean with respect to the function $\partial(\alpha) = |N(\alpha)|$.*

### Theorem (M.)

*Assuming the GRH, the norm-Euclidean cyclic cubic fields are exactly those with discriminant*
$\Delta = 7^2, 9^2, 13^2, 19^2, 31^2, 37^2, 43^2, 61^2, 67^2, 103^2, 109^2, 127^2, 157^2$ .

### Theorem (M., Lezowski)

*Any norm-Euclidean cyclic cubic field not listed in the previous theorem must have discriminant $\Delta = f^2$ with $f \equiv 1 \pmod 3$ where $f$ is a prime in the interval $(2 \cdot 10^{14}, 10^{50})$.*

# Norm-Euclidean cubic fields (non-cyclic)

What is the situation for cubic fields that are not necessarily cyclic? Heilbronn speculates that there are infinitely many norm-Euclidean fields in this setting.

Lemmermeyer carried out computations to show that 81.8% of cubic fields with $0 < \Delta < 10^4$ are norm-Euclidean, and observed that the proportion is decreasing.

One would like to at least give an upper bound on the asymptotic density, but this seems difficult. However, we can prove the following:

**Theorem (M., Tucker)**

*A positive proportion of totally real cubic fields with genus number one fail to be norm-Euclidean.*

# Heilbronn's criterion

Let $K$ be a totally real cubic field and let $F$ denote the product of all the totally ramified primes in $K$.

## Lemma (Heilbronn's criterion)

*If we can write $F = a + b$ with $a, b \in \mathbb{Z}^+$ where $a, b$ are not norms and $a$ is a cubic residue modulo $F$, then $K$ is not norm-Euclidean.*

One amusing observation is that if we are in the genus number one setting then the cubic residue part of the condition is automatic.

# How often does Heilbronn's criterion apply?

Let $H(X)$ denote the number of genus number one cubic fields with $0 < \Delta \leq X$ to which Heilbronn's criterion applies, and let $H(F;X)$ denote the number of such fields with fixed $F$. We have

$$H(X) = \sum_{F \leq X^{1/2}} H(F;X)$$

## Proposition

$$H(F;X) = \frac{b_F}{12\zeta(2)} \prod_{p|F} \frac{1}{p(p+1)} X + O(e^{4F/17} X^{16/17+\varepsilon})$$

*for some explicitly computable* $b_F \in \mathbb{Q} \cap [0,1]$.

| $F$ | 1 | 2 | 3 | 5 | 6 | 10 | 11 | 15 | 17 | 22 |
|---|---|---|---|---|---|---|---|---|---|---|
| $b_F$ | 0 | 0 | 0 | $\frac{1}{18}$ | 0 | $\frac{7}{96}$ | $\frac{55}{288}$ | $\frac{1574}{15309}$ | $\frac{231205}{653184}$ | $\frac{1292771}{4354560}$ |
| $\approx$ | 0 | 0 | 0 | 0.556 | 0 | 0.0729 | 0.191 | 0.103 | 0.354 | 0.297 |

# A Computation

## Example

*When $F = 167$, we compute $B_F \approx 0.9421$. In fact, the precise number is:*

$$\frac{5707366742127207720711393876905481748779979640006818006913}{60580371253074136019571483465373990671120713833632497664 00}$$

**Upshot:** Suppose we know that 167 is the only totally ramified prime in $K$. Then $K$ has less than a 5.8% chance of being norm-Euclidean.