# On Divisibility of Class Numbers of Cubic Fields by Three

(BIRS Workshop: Alberta Number Theory Days XV)

Abbas Maarefparvar

Department of Mathematics & Computer Science

University of Lethbridge

March 23, 2024

**Notations:**

- $K$: a number field, i.e., a finite extension of $\mathbb{Q}$;
- $[K:\mathbb{Q}]$: the degree of $K$ over $\mathbb{Q}$;
- $\mathcal{O}_K$: the ring of integers of $K$;
- $\mathrm{Cl}(K)$: the ideal class group of $K$;
- $h_K$: the class number of $K$.

# Decomposition of primes in number fields

For $K$, a number field with ring of integers $\mathcal{O}_K$, and a prime number $p$:

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g},$$

where $\mathfrak{P}_i$'s are distinct prime ideals of $\mathcal{O}_K$ and $e_i$'s are positive integers.

- The integers $e_i$'s are called the ramification indices of $p$ in $K$;

# Decomposition of primes in number fields

For $K$, a number field with ring of integers $\mathcal{O}_K$, and a prime number $p$:

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g},$$

where $\mathfrak{P}_i$'s are distinct prime ideals of $\mathcal{O}_K$ and $e_i$'s are positive integers.

- The integers $e_i$'s are called the ramification indices of $p$ in $K$;
- If $e_i > 1$, for at least one $i$, then we say $p$ ramifies in $K$;

# Decomposition of primes in number fields

For $K$, a number field with ring of integers $\mathcal{O}_K$, and a prime number $p$:

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_g^{e_g},$$

where $\mathfrak{P}_i$'s are distinct prime ideals of $\mathcal{O}_K$ and $e_i$'s are positive integers.

- The integers $e_i$'s are called the ramification indices of $p$ in $K$;
- If $e_i > 1$, for at least one $i$, then we say $p$ ramifies in $K$;
- If $p\mathcal{O}_K = \mathfrak{P}^{[K:\mathbb{Q}]}$, we say $p$ totally ramifies in $K$.

# Decomposition of primes in number fields

For $K$, a number field with ring of integers $\mathcal{O}_K$, and a prime number $p$:

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g},$$

where $\mathfrak{P}_i$'s are distinct prime ideals of $\mathcal{O}_K$ and $e_i$'s are positive integers.

- The integers $e_i$'s are called the ramification indices of $p$ in $K$;
- If $e_i > 1$, for at least one $i$, then we say $p$ ramifies in $K$;
- If $p\mathcal{O}_K = \mathfrak{P}^{[K:\mathbb{Q}]}$, we say $p$ totally ramifies in $K$.

**Example**

The prime 2 totally ramifies in $K = \mathbb{Q}(\sqrt[3]{2})$, since $2\mathcal{O}_K = (\sqrt[3]{2})^3$.

# On Class Number Problems

Class number problems arise from studies of class groups of number fields of a specific degree.

Class number problems arise from studies of class groups of number fields of a specific degree.

### Gauss' class number one problems for quadratic fields (1801)

1. An imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ has class number one, if and only if $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.

# On Class Number Problems

Class number problems arise from studies of class groups of number fields of a specific degree.

## Gauss' class number one problems for quadratic fields (1801)

1. An imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ has class number one, if and only if $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.
    - This problem was solved by Heegner (1954), Baker (1966), and Stark (1967).

# On Class Number Problems

Class number problems arise from studies of class groups of number fields of a specific degree.

**Gauss' class number one problems for quadratic fields (1801)**

1. An imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ has class number one, if and only if $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.
   - This problem was solved by Heegner (1954), Baker (1966), and Stark (1967).

2. There are infinitely many real quadratic number fields with class number one
   - This is still an open problem!

# On Class Number Problems

Class number problems arise from studies of class groups of number fields of a specific degree.

**Gauss' class number one problems for quadratic fields (1801)**

1. An imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ has class number one, if and only if $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.
   - This problem was solved by Heegner (1954), Baker (1966), and Stark (1967).
2. There are infinitely many real quadratic number fields with class number one
   - This is still an open problem!

Class groups of cubic fields have been investigated by many authors, e.g., Gerth, Honda, Barrucand, Cohn, Louboutin, Uchida, etc.

### Theorem (Ishida, 1969)

Let $K$ be a number field of degree $\ell$, an odd prime, and denote its ring of integers by $\mathcal{O}_K$. If

1. $K$ is non-pure, i.e., $K \neq \mathbb{Q}(\sqrt[\ell]{m})$ for any $\ell$-th power free integer $m$;
2. $\#\{\text{primes ramify totally in } K\} > \operatorname{rank}_{\mathbb{Z}}(\mathcal{O}_K^\times)$,

then the class number of $K$ is divisible by $\ell$.

## Theorem (Ishida, 1969)

Let $K$ be a number field of degree $\ell$, an odd prime, and denote its ring of integers by $\mathcal{O}_K$. If

1. $K$ is non-pure, i.e., $K \neq \mathbb{Q}(\sqrt[\ell]{m})$ for any $\ell$-th power free integer $m$;
2. $\#\{\text{primes ramify totally in } K\} > \operatorname{rank}_{\mathbb{Z}}(\mathcal{O}_K^{\times})$,

then the class number of $K$ is divisible by $\ell$.

## Example

Let $K = \mathbb{Q}(\theta)$ be a non-pure cubic field, where $\theta$ is a root of the cubic polynomial

$$f(X) = X^3 + aX + b, \quad a, b \in \mathbb{Z}.$$

In the following cases, the class number of $K$ is divisible by three:

1. $-4a^3 - 27b^2 > 0$, and $\#\{\text{primes ramify totally in } K\} > 2$,
2. $-4a^3 - 27b^2 < 0$, and $\#\{\text{primes ramify totally in } K\} > 1$.

### Theorem (M.-Rajaei, 2019)

Let $m \neq \pm 1$ be a cube free integer and $K = \mathbb{Q}(\sqrt[3]{m})$ be a pure cubic field. If

$$\#\{\text{primes ramify totally in } K\} > \mathrm{rank}_{\mathbb{Z}}(\mathcal{O}_K^\times) + 1 = 2,$$

then the class number of $K$ is divisible by three.

### Corollary

If $m \neq \pm 1$, a cube free integer, has at least three distinct prime divisors then the class number of $K = \mathbb{Q}(\sqrt[3]{m})$ is divisible by three.

### Example

Let $K = \mathbb{Q}(\sqrt[3]{30})$. Then $h_K = 3$.

# Ramified primes in pure cubic fields

### Proposition

Let $m = ab^2$ be a cube-free integer, where $a, b \neq 1$ are relatively prime.Then a prime $p$ ramifies in $K = \mathbb{Q}(\sqrt[3]{m})$ if and only if $p \mid \mathrm{disc}(K/\mathbb{Q})$, where

$$\mathrm{disc}(K/\mathbb{Q}) = \begin{cases} -3(3ab)^2, & m \not\equiv \pm 1 \pmod 9, \\ -3(ab)^2, & m \equiv \pm 1 \pmod 9. \end{cases}$$

Moreover, $p$ totally ramifies if and only if $p \mid \frac{\mathrm{disc}(K/\mathbb{Q})}{3}$.

# Proof of Main Theorems

**Theorem 1 (Ishida, 1969)**

Let $K = \mathbb{Q}(\theta)$ be a non-pure cubic field. If

$$\#\{\text{totally ramified primes in } K\} > \text{rank}_{\mathbb{Z}}(\mathcal{O}_K^{\times}),$$

then $3 \mid h_K$.

**Theorem 2 (M.-Rajaei, 2019)**

Let $m \neq \pm 1$ be a cube free integer and $K = \mathbb{Q}(\sqrt[3]{m})$ be a pure cubic field. If

$$\#\{\text{totally ramified primes in } K\} > \text{rank}_{\mathbb{Z}}(\mathcal{O}_K^{\times}) + 1,$$

then $3 \mid h_K$.

**Proof of Theorem 2.** Let $K = \mathbb{Q}(\sqrt[3]{m})$ and $L = \mathbb{Q}(\sqrt[3]{m}, \sqrt{-3})$. By a result of Zantema, the following sequence is exact

$$0 \to H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathcal{O}_L^\times) \to \bigoplus_{p \text{ prime}} \frac{\mathbb{Z}}{e_{p(L/\mathbb{Q})}\mathbb{Z}} \to \mathrm{Cl}(L)_{\mathrm{sa}}^G \to 0,$$

where $e_{p(L/\mathbb{Q})}$ denotes the ramification index of $p$ in $L$, and $\mathrm{Cl}(L)_{\mathrm{sa}}^G$ denotes the group of strongly ambiguous ideal classes of $L$, i.e.,

$$\mathrm{Cl}(L)_{\mathrm{sa}}^G = \{[\mathfrak{a}] \in \mathrm{Cl}(L) \,:\, \mathfrak{a}^\sigma = \mathfrak{a}, \forall \sigma \in \mathrm{Gal}(L/\mathbb{Q})\}.$$

**Proof of Theorem 2.** Let $K = \mathbb{Q}(\sqrt[3]{m})$ and $L = \mathbb{Q}(\sqrt[3]{m}, \sqrt{-3})$. By a result of Zantema, the following sequence is exact

$$0 \to H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathcal{O}_L^\times) \to \bigoplus_{p \text{ prime}} \frac{\mathbb{Z}}{e_{p(L/\mathbb{Q})}\mathbb{Z}} \to \mathrm{Cl}(L)_{\mathrm{sa}}^G \to 0,$$

where $e_{p(L/\mathbb{Q})}$ denotes the ramification index of $p$ in $L$, and $\mathrm{Cl}(L)_{\mathrm{sa}}^G$ denotes the group of strongly ambiguous ideal classes of $L$, i.e.,

$$\mathrm{Cl}(L)_{\mathrm{sa}}^G = \{[\mathfrak{a}] \in \mathrm{Cl}(L) \,:\, \mathfrak{a}^\sigma = \mathfrak{a}, \forall \sigma \in \mathrm{Gal}(L/\mathbb{Q})\}.$$

**Lemma (M.-Rajaei, 2019)**

- If a prime $p$ totally ramifies in $K$, then $3 \mid e_{p(L/\mathbb{Q})}$.
- We have $\left(\mathrm{Cl}(L)_{\mathrm{sa}}^G\right)_3 = \left\{[\mathfrak{a}] \in \mathrm{Cl}(L)_{\mathrm{sa}}^G \,:\, [\mathfrak{a}]^3 = 1\right\} \hookrightarrow \mathrm{Cl}(K)$.

For $K = \mathbb{Q}(\sqrt[3]{m})$ and $E = \mathbb{Q}(\sqrt{-3})$, the restriction maps

$$\mathrm{res}_{L/K} : H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathcal{O}_L^\times) \to H^1(\mathrm{Gal}(L/K), \mathcal{O}_L^\times),$$

and

$$\mathrm{res}_{L/E} : H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathcal{O}_L^\times) \to H^1(\mathrm{Gal}(L/E), \mathcal{O}_L^\times),$$

are injective on the 2-subgroup and 3-subgroup of $H^1(\mathrm{Gal}(L/\mathbb{Q}, \mathcal{O}_L^\times)$, respectively.

For $K = \mathbb{Q}(\sqrt[3]{m})$ and $E = \mathbb{Q}(\sqrt{-3})$, the restriction maps

$$\mathrm{res}_{L/K} : H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathcal{O}_L^\times) \to H^1(\mathrm{Gal}(L/K), \mathcal{O}_L^\times),$$

and

$$\mathrm{res}_{L/E} : H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathcal{O}_L^\times) \to H^1(\mathrm{Gal}(L/E), \mathcal{O}_L^\times),$$

are injective on the 2-subgroup and 3-subgroup of $H^1(\mathrm{Gal}(L/\mathbb{Q}, \mathcal{O}_L^\times)$, respectively. Therefore,

$$\#H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathcal{O}_L^\times) \mid \underbrace{\#H^1(\mathrm{Gal}(L/K), \mathcal{O}_L^\times)}_{\text{a power of 2}} \cdot \underbrace{\#H^1(\mathrm{Gal}(L/E), \mathcal{O}_L^\times)}_{\text{a power of 3}}.$$

Since $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L/E)$ are cyclic, their Herbrand quotients are given by

$$1 = Q(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) = \frac{\#\widehat{H^0}(\mathrm{Gal}(L/K), \mathcal{O}_L^\times)}{\#H^1(\mathrm{Gal}(L/K), \mathcal{O}_L^\times)},$$

$$\frac{1}{3} = Q(\mathrm{Gal}(L/E), \mathcal{O}_L^\times) = \frac{\#\widehat{H^0}(\mathrm{Gal}(L/E), \mathcal{O}_L^\times)}{\#H^1(\mathrm{Gal}(L/E), \mathcal{O}_L^\times)}.$$

Since $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L/E)$ are cyclic, their Herbrand quotients are given by

$$1 = Q(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) = \frac{\#\widehat{H^0}(\mathrm{Gal}(L/K), \mathcal{O}_L^\times)}{\#H^1(\mathrm{Gal}(L/K), \mathcal{O}_L^\times)},$$

$$\frac{1}{3} = Q(\mathrm{Gal}(L/E), \mathcal{O}_L^\times) = \frac{\#\widehat{H^0}(\mathrm{Gal}(L/E), \mathcal{O}_L^\times)}{\#H^1(\mathrm{Gal}(L/E), \mathcal{O}_L^\times)}.$$

We have

$$\#\widehat{H^0}(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) \mid \#\frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^2} = \#\frac{\{\pm 1\} \cdot < \xi_K >}{\{(\pm 1)^2\} \cdot < \xi_K^2 >} = 2^2,$$

$$\#\widehat{H^0}(\mathrm{Gal}(L/E), \mathcal{O}_L^\times) \mid \#\frac{\mathcal{O}_E^\times}{(\mathcal{O}_E^\times)^3} = \#\frac{\{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}}{\{(\pm 1)^3, (\pm\zeta_3)^3, (\pm\zeta_3^2)^3\}} = 3,$$

where $\xi_K$ is the fundamental unit of $K$ and $\zeta_3$ is a third primitive root of unity.

Consequently,

$$\#H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathcal{O}_L^\times) \mid \#H^1(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) \cdot \#H^1(\mathrm{Gal}(L/E), \mathcal{O}_L^\times) \mid 2^2 \cdot 3^2.$$

$$0 \to H^1(G, \mathcal{O}_L^\times) \to \bigoplus_{p \text{ prime}} \frac{\mathbb{Z}}{e_{p(L/\mathbb{Q})}\mathbb{Z}} \to \mathrm{Cl}(L)_{\mathrm{sa}}^G \to 0, \ G = \mathrm{Gal}(L/\mathbb{Q}).$$

Consequently,

$$\#H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathcal{O}_L^\times) \mid \#H^1(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) \cdot \#H^1(\mathrm{Gal}(L/E), \mathcal{O}_L^\times) \mid 2^2 \cdot 3^2.$$

**Lemma (M.-Rajaei, 2019)**

- If a prime $p$ totally ramifies in $K$, then $3 \mid e_{p(L/\mathbb{Q})}$.
- We have $\left(\mathrm{Cl}(L)_{\mathrm{sa}}^G\right)_3 = \left\{[\mathfrak{a}] \in \mathrm{Cl}(L)_{\mathrm{sa}}^G \ : \ [\mathfrak{a}]^3 = 1\right\} \hookrightarrow \mathrm{Cl}(K)$.

Now if at least three primes totally ramify in $K$, then

$$3^3 \mid \prod_{p \text{ prime}} e_{p(L/\mathbb{Q})} = \#H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathcal{O}_L^\times) \cdot \#\,\mathrm{Cl}(L)_{\mathrm{sa}}^G.$$

Consequently,

$$\#H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathcal{O}_L^\times) \mid \#H^1(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) \cdot \#H^1(\mathrm{Gal}(L/E), \mathcal{O}_L^\times) \mid 2^2 \cdot 3^2.$$

**Lemma (M.-Rajaei, 2019)**

- If a prime $p$ totally ramifies in $K$, then $3 \mid e_{p(L/\mathbb{Q})}$.
- We have $\left(\mathrm{Cl}(L)_{\mathrm{sa}}^G\right)_3 = \left\{[\mathfrak{a}] \in \mathrm{Cl}(L)_{\mathrm{sa}}^G \ : \ [\mathfrak{a}]^3 = 1\right\} \hookrightarrow \mathrm{Cl}(K)$.

Now if at least three primes totally ramify in $K$, then

$$3^3 \mid \prod_{p \text{ prime}} e_{p(L/\mathbb{Q})} = \#H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathcal{O}_L^\times) \cdot \#\,\mathrm{Cl}(L)_{\mathrm{sa}}^G.$$

Hence $\#\,\mathrm{Cl}(L)_{\mathrm{sa}}^G$ is divisible by three, so is $h_K$.

**Remarks.**

1. The above method can be used to prove Ishida's result for cubic fields.
2. More generally, a similar result holds for number fields of degree $\ell$ (an odd prime) whose Galois closures have Galois group isomorphic to $D_\ell$, the dihedral group of order $2\ell$ (M.-Rajaei, 2020).


THANK YOU
Any Questions?