Questions of Euclideanity for the norm form

Why 2 is the oddest number

Jean-Paul Cerri

Bordeaux 1 University
IMB - Laboratory A2X
France

14.12.2007

Plan

1. Introduction
2. Old questions
3. New theoretical results
4. New practical results
5. Successive minima. k-stage Euclideanity. Central division algebras

- Let $K = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer.

- Let $K = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer.
- Let $\mathbb{Z}_K$ be the ring of integers of K and $N_{K/\mathbb{Q}}$ the norm form of K.

- Let $K = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer.
- Let $\mathbb{Z}_K$ be the ring of integers of K and $N_{K/\mathbb{Q}}$ the norm form of K.
- If $n \equiv 2$ or $3 \bmod 4$ then

$$\mathbb{Z}_K = \{A + B\sqrt{d};\ (A, B) \in \mathbb{Z}^2\}$$

$$N_{K/\mathbb{Q}}(x + y\sqrt{d}) = x^2 - dy^2$$

- Let $K = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer.
- Let $\mathbb{Z}_K$ be the ring of integers of K and $N_{K/\mathbb{Q}}$ the norm form of K.
- If $n \equiv 2$ or $3 \bmod 4$ then

$$\mathbb{Z}_K = \{A + B\sqrt{d};\ (A, B) \in \mathbb{Z}^2\}$$

$$N_{K/\mathbb{Q}}(x + y\sqrt{d}) = x^2 - dy^2$$

- If $n \equiv 1 \bmod 4$ then

$$\mathbb{Z}_K = \left\{A + B\frac{1+\sqrt{d}}{2};\ (A, B) \in \mathbb{Z}^2\right\}$$

$$N_{K/\mathbb{Q}}(x + y\frac{1+\sqrt{d}}{2}) = x^2 + xy - \frac{d-1}{4}y^2$$

Definition 1.

K is said norm-Euclidean iff for every $(\alpha, \beta) \in \mathbb{Z}_k^2$ with $\beta \neq 0$, there exists a $\Upsilon \in \mathbb{Z}_K$ such that

$$|N_{K/\mathbb{Q}}(\alpha - \beta\Upsilon)| < |N_{K/\mathbb{Q}}(\beta)|.$$

Definition 1.

K is said norm-Euclidean iff for every $(\alpha, \beta) \in \mathbb{Z}_k^2$ with $\beta \neq 0$, there exists a $\Upsilon \in \mathbb{Z}_K$ such that

$$|N_{K/\mathbb{Q}}(\alpha - \beta\Upsilon)| < |N_{K/\mathbb{Q}}(\beta)|.$$

This equivalent to:

$$\forall \xi \in K,\ \exists \Upsilon \in \mathbb{Z}_K;\ |N_{K/\mathbb{Q}}(\xi - \Upsilon)| < 1.$$

Definition 1.

K is said norm-Euclidean iff for every $(\alpha, \beta) \in \mathbb{Z}_k^2$ with $\beta \neq 0$, there exists a $\Upsilon \in \mathbb{Z}_K$ such that

$$|N_{K/\mathbb{Q}}(\alpha - \beta\Upsilon)| < |N_{K/\mathbb{Q}}(\beta)|.$$

This equivalent to:

$$\forall \xi \in K,\ \exists \Upsilon \in \mathbb{Z}_K;\ |N_{K/\mathbb{Q}}(\xi - \Upsilon)| < 1.$$

Elementary examples.

$\mathbb{Q}(\sqrt{-1})$ et $\mathbb{Q}(\sqrt{2})$ are norm-euclidean.

▸ Figures

Definition 2.

If $\xi \in K$, the *Euclidean minimum* of ξ is

$$m_K(\xi) = \inf\left\{|N_{K/\mathbb{Q}}(\xi - \Upsilon)|;\ \Upsilon \in \mathbb{Z}_K\right\}.$$

The set $\mathrm{sp}(K) = \{m_K(\xi);\ \xi \in K\}$ is called the *Euclidean spectrum* of K.

Definition 2.

If $\xi \in K$, the *Euclidean minimum* of ξ is

$$m_K(\xi) = \inf\left\{|N_{K/\mathbb{Q}}(\xi - \Upsilon)|;\ \Upsilon \in \mathbb{Z}_K\right\}.$$

The set $\mathrm{sp}(K) = \{m_K(\xi);\ \xi \in K\}$ is called the *Euclidean spectrum* of K.

For instance, if $K = \mathbb{Q}(\sqrt{2})$,

$$m_K(a + b\sqrt{2}) = \inf\left\{|(a - A)^2 - 2(b - B)^2|;\ (A, B) \in \mathbb{Z}^2\right\}.$$

We denote by $\overline{K}$ the product of the archimedian completions of K, $K \otimes_{\mathbb{Q}} \mathbb{R}$ which can be identified to $\mathbb{R}^2$.

We denote by $\overline{K}$ the product of the archimedian completions of K, $K \otimes_{\mathbb{Q}} \mathbb{R}$ which can be identified to $\mathbb{R}^2$.
The norm $N_{K/\mathbb{Q}}$ has a natural continuous extension to $\overline{K}$ denoted by $\mathcal{N}$.

We denote by $\overline{K}$ the product of the archimedian completions of K, $K \otimes_{\mathbb{Q}} \mathbb{R}$ which can be identified to $\mathbb{R}^2$.
The norm $N_{K/\mathbb{Q}}$ has a natural continuous extension to $\overline{K}$ denoted by $\mathcal{N}$.

Definition 3.

If $x \in \overline{K}$, the *inhomogeneous minimum* of x is

$$m_{\overline{K}}(x) = \inf\left\{|\mathcal{N}(x - \Upsilon)|;\ \Upsilon \in \mathbb{Z}_K\right\}.$$

The set $\mathrm{sp}(\overline{K}) = \{m_{\overline{K}}(x);\ x \in \overline{K}\}$ is called the *inhomogeneous spectrum* of K.

Definition 4.

We call *minimum inhomogeneous* of K the positive real number $M(\overline{K})$ defined by

$$M(\overline{K}) = \sup \{m_{\overline{K}}(x);\ x \in \overline{K}\}.$$

If $m_{\overline{K}}(x) = M(\overline{K})$, x will be said *critical*.

Definition 4.

We call *minimum inhomogeneous* of K the positive real number $M(\overline{K})$ defined by

$$M(\overline{K}) = \sup \{m_{\overline{K}}(x);\ x \in \overline{K}\}.$$

If $m_{\overline{K}}(x) = M(\overline{K})$, x will be said *critical*.

Definition 5.

We call *Euclidean minimum* of K the positive real number $M(K)$ defined by

$$M(K) = \sup \left\{m_K(\xi);\ \xi \in K\right\}.$$

$$M(K) \leq M(\overline{K}).$$

- If $K = \mathbb{Q}(\sqrt{-1})$, we have

$$M(K) = \sup_{(a,b)\in\mathbb{Q}^2} \inf \left\{ (a-A)^2 + (b-B)^2;\ (A,B) \in \mathbb{Z}^2 \right\},$$

- If $K = \mathbb{Q}(\sqrt{-1})$, we have

$$M(K) = \sup_{(a,b)\in\mathbb{Q}^2} \inf\left\{(a-A)^2 + (b-B)^2;\ (A,B) \in \mathbb{Z}^2\right\},$$

and

$$M(\overline{K}) = \sup_{(a,b)\in\mathbb{R}^2} \inf\left\{(a-A)^2 + (b-B)^2;\ (A,B) \in \mathbb{Z}^2\right\}.$$

- If $K = \mathbb{Q}(\sqrt{-1})$, we have

$$M(K) = \sup_{(a,b)\in\mathbb{Q}^2} \inf \left\{ (a-A)^2 + (b-B)^2;\ (A,B) \in \mathbb{Z}^2 \right\},$$

and

$$M(\overline{K}) = \sup_{(a,b)\in\mathbb{R}^2} \inf \left\{ (a-A)^2 + (b-B)^2;\ (A,B) \in \mathbb{Z}^2 \right\}.$$

- If $K = \mathbb{Q}(\sqrt{2})$, we have

$$M(K) = \sup_{(a,b)\in\mathbb{Q}^2} \inf \left\{ |(a-A)^2 - 2(b-B)^2|;\ (A,B) \in \mathbb{Z}^2 \right\},$$

- If $K = \mathbb{Q}(\sqrt{-1})$, we have

$$M(K) = \sup_{(a,b)\in\mathbb{Q}^2} \inf \left\{ (a-A)^2 + (b-B)^2;\ (A,B) \in \mathbb{Z}^2 \right\},$$

and

$$M(\overline{K}) = \sup_{(a,b)\in\mathbb{R}^2} \inf \left\{ (a-A)^2 + (b-B)^2;\ (A,B) \in \mathbb{Z}^2 \right\}.$$

- If $K = \mathbb{Q}(\sqrt{2})$, we have

$$M(K) = \sup_{(a,b)\in\mathbb{Q}^2} \inf \left\{ |(a-A)^2 - 2(b-B)^2|;\ (A,B) \in \mathbb{Z}^2 \right\},$$

and

$$M(\overline{K}) = \sup_{(a,b)\in\mathbb{R}^2} \inf \left\{ |(a-A)^2 - 2(b-B)^2|;\ (A,B) \in \mathbb{Z}^2 \right\}.$$

▸ Figures

Proposition 1.

If $K = \mathbb{Q}(\sqrt{-m})$ where $m > 0$ is squarefree, we have

$$M(K) = M(\overline{K}) = \begin{cases} \frac{m+1}{4} & \text{if } m \equiv 1 \text{ or } 2 \mod 4, \\ \frac{(m+1)^2}{16m} & \text{if } m \equiv 3 \mod 4. \end{cases}$$

Proposition 1.

If $K = \mathbb{Q}(\sqrt{-m})$ where $m > 0$ is squarefree, we have

$$M(K) = M(\overline{K}) = \begin{cases} \frac{m+1}{4} & \text{if } m \equiv 1 \text{ or } 2 \mod 4, \\ \frac{(m+1)^2}{16m} & \text{if } m \equiv 3 \mod 4. \end{cases}$$

Proposition 2.

We have

- *If $M(K) < 1$, K is norm-Euclidean.*

Proposition 1.

If $K = \mathbb{Q}(\sqrt{-m})$ where $m > 0$ is squarefree, we have

$$M(K) = M(\overline{K}) = \begin{cases} \frac{m+1}{4} & \text{if } m \equiv 1 \text{ or } 2 \mod 4, \\ \frac{(m+1)^2}{16m} & \text{if } m \equiv 3 \mod 4. \end{cases}$$

Proposition 2.

We have

- *If $M(K) < 1$, K is norm-Euclidean.*
- *If $M(K) > 1$, K is not norm-Euclidean.*

Proposition 1.

If $K = \mathbb{Q}(\sqrt{-m})$ where $m > 0$ is squarefree, we have

$$M(K) = M(\overline{K}) = \begin{cases} \frac{m+1}{4} & \text{if } m \equiv 1 \text{ or } 2 \mod 4, \\ \frac{(m+1)^2}{16m} & \text{if } m \equiv 3 \mod 4. \end{cases}$$

Proposition 2.

We have

- *If* $M(K) < 1$, *K is norm-Euclidean.*
- *If* $M(K) > 1$, *K is not norm-Euclidean.*
- *If* $M(K) = 1$, *we cannot conclude a priori.*

Theorem 1.

There are only 16 real quadratic number fields which are norm-Euclidean.

Theorem 1.

There are only 16 real quadratic number fields which are norm-Euclidean. For each of them we have $M(K) < 1$.

Theorem 1.

There are only 16 real quadratic number fields which are norm-Euclidean. For each of them we have $M(K) < 1$.

Definition 6.

We call *second inhomogeneous minimum* and *second Euclidean minimum* of K the following numbers

$$M_2(\overline{K}) = \sup_{\substack{x \in \overline{K} \\ m_{\overline{K}}(x) < M(\overline{K})}} \left(m_{\overline{K}}(x) \right) \text{ and } M_2(K) = \sup_{\substack{\xi \in K \\ m_K(\xi) < M(K)}} \left(m_K(\xi) \right).$$

We have

$$M_2(K) \leq M_2(\overline{K}) \leq M(\overline{K}).$$

We have

$$M_2(K) \leq M_2(\overline{K}) \leq M(\overline{K}).$$

Definition 7.

Going further we define (with $p \geq 2$)

$$M_{p+1}(\overline{K}) = \sup_{\substack{x \in \overline{K} \\ m_{\overline{K}}(x) < M_p(\overline{K})}} \left(m_{\overline{K}}(x) \right),$$

$$M_{p+1}(K) = \sup_{\substack{\xi \in K \\ m_K(\xi) < M_p(K)}} \left(m_K(\xi) \right).$$

We have

$$M_2(K) \leq M_2(\overline{K}) \leq M(\overline{K}).$$

Definition 7.

Going further we define (with $p \geq 2$)

$$M_{p+1}(\overline{K}) = \sup_{\substack{x \in \overline{K} \\ m_{\overline{K}}(x) < M_p(\overline{K})}} \left(m_{\overline{K}}(x) \right),$$

$$M_{p+1}(K) = \sup_{\substack{\xi \in K \\ m_K(\xi) < M_p(K)}} \left(m_K(\xi) \right).$$

Putting $M_1(\overline{K}) = M(\overline{K})$ and $M_1(K) = M(K)$, we obtain two decreasing sequences, with $M_p(K) \leq M_p(\overline{K})$, for every $p \geq 1$.

Generalization to number fields

All these notions can be generalized to an arbitrary number field K.

Generalization to number fields

All these notions can be generalized to an arbitrary number field K. In particular

- m_K and $m_{\overline{K}}$;
- $M(K)$ and $M(\overline{K})$;
- $\mathrm{sp}(K)$ and $\mathrm{sp}(\overline{K})$;
- $M_p(K)$ and $M_p(\overline{K})$.

Generalization to number fields

All these notions can be generalized to an arbitrary number field K. In particular

- m_K and $m_{\overline{K}}$;
- $M(K)$ and $M(\overline{K})$;
- $\mathrm{sp}(K)$ and $\mathrm{sp}(\overline{K})$;
- $M_p(K)$ and $M_p(\overline{K})$.

In what follows, K is a number field of degree n and signature (r_1, r_2).

Generalization to number fields

All these notions can be generalized to an arbitrary number field K.
In particular

- m_K and $m_{\overline{K}}$;
- $M(K)$ and $M(\overline{K})$;
- $\mathrm{sp}(K)$ and $\mathrm{sp}(\overline{K})$;
- $M_p(K)$ and $M_p(\overline{K})$.

In what follows, K is a number field of degree n and signature (r_1, r_2).
The rank $r_1 + r_2 - 1$ of its unit group will be denoted by r.

Plan

1 Introduction

2 Old questions

3 New theoretical results

4 New practical results

5 Successive minima. k-stage Euclideanity. Central division algebras

- Do we have $M(K) = M(\overline{K})$? (conjecture $\boldsymbol{C_1}$)

- Do we have $M(K) = M(\overline{K})$? (conjecture $\boldsymbol{C_1}$)
  True for $r \leq 1$ (Barnes and Swinnerton-Dyer 1952 for $n = r_1 = 2$, and Van der Linden 1985).

- Do we have $M(K) = M(\overline{K})$? (conjecture $\boldsymbol{C_1}$)
  True for $r \leq 1$ (Barnes and Swinnerton-Dyer 1952 for $n = r_1 = 2$, and Van der Linden 1985).
- Is there a $\xi \in K$ such that $M(\overline{K}) = m_K(\xi)$? (conjecture $\boldsymbol{C_2}$)

- Do we have $M(K) = M(\overline{K})$? (conjecture $\boldsymbol{C_1}$)
  True for $r \leq 1$ (Barnes and Swinnerton-Dyer 1952 for $n = r_1 = 2$, and Van der Linden 1985).
- Is there a $\xi \in K$ such that $M(\overline{K}) = m_K(\xi)$? (conjecture $\boldsymbol{C_2}$)
  - Obvious for $r = 0$. Conjectured for $n = r_1 = 2$ (Barnes and Swinnerton-Dyer 1952)

- Do we have $M(K) = M(\overline{K})$? (conjecture $\boldsymbol{C_1}$)
  True for $r \leq 1$ (Barnes and Swinnerton-Dyer 1952 for $n = r_1 = 2$, and Van der Linden 1985).
- Is there a $\xi \in K$ such that $M(\overline{K}) = m_K(\xi)$? (conjecture $\boldsymbol{C_2}$)
  - Obvious for $r = 0$. Conjectured for $n = r_1 = 2$ (Barnes and Swinnerton-Dyer 1952)
  - $\boldsymbol{C_2} \Rightarrow M(K) = M(\overline{K}) \in \mathbb{Q}$ (hence $\boldsymbol{C_1}$)

- Do we have $M(K) = M(\overline{K})$? (conjecture $\boldsymbol{C_1}$)
  True for $r \leq 1$ (Barnes and Swinnerton-Dyer 1952 for $n = r_1 = 2$, and Van der Linden 1985).
- Is there a $\xi \in K$ such that $M(\overline{K}) = m_K(\xi)$? (conjecture $\boldsymbol{C_2}$)
  - Obvious for $r = 0$. Conjectured for $n = r_1 = 2$ (Barnes and Swinnerton-Dyer 1952)
  - $\boldsymbol{C_2} \Rightarrow M(K) = M(\overline{K}) \in \mathbb{Q}$ (hence $\boldsymbol{C_1}$)
- Link between $M(K)$ and the norm-Euclideanity of K ?

- Do we have $M(K) = M(\overline{K})$? (conjecture $\boldsymbol{C_1}$)
  True for $r \leq 1$ (Barnes and Swinnerton-Dyer 1952 for $n = r_1 = 2$, and Van der Linden 1985).
- Is there a $\xi \in K$ such that $M(\overline{K}) = m_K(\xi)$? (conjecture $\boldsymbol{C_2}$)
  - Obvious for $r = 0$. Conjectured for $n = r_1 = 2$ (Barnes and Swinnerton-Dyer 1952)
  - $\boldsymbol{C_2} \Rightarrow M(K) = M(\overline{K}) \in \mathbb{Q}$ (hence $\boldsymbol{C_1}$)
- Link between $M(K)$ and the norm-Euclideanity of K ?
  If $\boldsymbol{C_2}$ is true then :

$$M(K) = 1 \Rightarrow K \quad \text{not norm-Euclidean.}$$

- We have

$$\forall \xi \in K,\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |N_{K/\mathbb{Q}}(\xi - \Upsilon)| \leq M(K).$$

- We have

$$\forall \xi \in K,\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |N_{K/\mathbb{Q}}(\xi - \Upsilon)| \leq M(K).$$

But

$$\forall x \in \overline{K},\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |\mathcal{N}(x - \Upsilon)| \leq M(\overline{K}),$$

is not always true ($K = \mathbb{Q}(\sqrt{13})$ - Inkeri 1949). ▸ Figures

- We have

$$\forall \xi \in K,\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |N_{K/\mathbb{Q}}(\xi - \Upsilon)| \leq M(K).$$

But

$$\forall x \in \overline{K},\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |\mathcal{N}(x - \Upsilon)| \leq M(\overline{K}),$$

is not always true ($K = \mathbb{Q}(\sqrt{13})$ - Inkeri 1949). ▸ Figures
If this is the case, we shall say that $M(\overline{K})$ is *attained*.

- We have

$$\forall \xi \in K,\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |N_{K/\mathbb{Q}}(\xi - \Upsilon)| \leq M(K).$$

But

$$\forall x \in \overline{K},\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |\mathcal{N}(x - \Upsilon)| \leq M(\overline{K}),$$

is not always true ($K = \mathbb{Q}(\sqrt{13})$ - Inkeri 1949). ▸ Figures
If this is the case, we shall say that $M(\overline{K})$ is *attained*.

- Do we have $M_2(\overline{K}) < M(\overline{K})$? (conjecture $\boldsymbol{C_3}$)

- We have

$$\forall \xi \in K,\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |N_{K/\mathbb{Q}}(\xi - \Upsilon)| \leq M(K).$$

But

$$\forall x \in \overline{K},\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |\mathcal{N}(x - \Upsilon)| \leq M(\overline{K}),$$

is not always true ($K = \mathbb{Q}(\sqrt{13})$ - Inkeri 1949). ▸ Figures
If this is the case, we shall say that $M(\overline{K})$ is *attained*.

- Do we have $M_2(\overline{K}) < M(\overline{K})$? (conjecture $\boldsymbol{C_3}$)
  - $M(\overline{K})$ is then said *isolated*.

- We have

$$\forall \xi \in K,\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |N_{K/\mathbb{Q}}(\xi - \Upsilon)| \leq M(K).$$

But

$$\forall x \in \overline{K},\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |\mathcal{N}(x - \Upsilon)| \leq M(\overline{K}),$$

is not always true ($K = \mathbb{Q}(\sqrt{13})$ - Inkeri 1949). ▸ Figures
If this is the case, we shall say that $M(\overline{K})$ is *attained*.

- Do we have $M_2(\overline{K}) < M(\overline{K})$? (conjecture $\boldsymbol{C_3}$)
  - $M(\overline{K})$ is then said *isolated*.
  - Obviously false if $r = 0$ but conjectured in the case $n = r_1 = 2$ (Barnes et Swinnerton-Dyer 1952).

- We have

$$\forall \xi \in K,\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |N_{K/\mathbb{Q}}(\xi - \Upsilon)| \leq M(K).$$

But

$$\forall x \in \overline{K},\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |\mathcal{N}(x - \Upsilon)| \leq M(\overline{K}),$$

is not always true ($K = \mathbb{Q}(\sqrt{13})$ - Inkeri 1949). ▸ Figures
If this is the case, we shall say that $M(\overline{K})$ is *attained*.

- Do we have $M_2(\overline{K}) < M(\overline{K})$? (conjecture $\boldsymbol{C_3}$)
  - $M(\overline{K})$ is then said *isolated*.
  - Obviously false if $r = 0$ but conjectured in the case $n = r_1 = 2$ (Barnes et Swinnerton-Dyer 1952).
  - If $\boldsymbol{C_1}$ is true, $\boldsymbol{C_3} \Rightarrow \boldsymbol{C_2}$

- Do we have $M_2(\overline{K}) = M_2(K)$?
  No ($K = \mathbb{Q}(\sqrt{73})$ - Godwin 1955).

- Do we have $M_2(\overline{K}) = M_2(K)$?
  No ($K = \mathbb{Q}(\sqrt{73})$ - Godwin 1955).

- More generally what is the behaviour of the sequences $(M_p(K))$ and $(M_p(\overline{K}))$. Possible equality, limits ?
  When $n = r_1 = 2$, $(M_p(\overline{K}))$ and $(M_p(K))$ can be stationnary ($K = \mathbb{Q}(\sqrt{23})$ - Godwin 1963), both sequences can be strictly decreasing, equal, and converge to a $\lambda > 0$ ($K = \mathbb{Q}(\sqrt{5})$ - Davenport 1948).

- Do we have $M_2(\overline{K}) = M_2(K)$?
  No ($K = \mathbb{Q}(\sqrt{73})$ - Godwin 1955).

- More generally what is the behaviour of the sequences $(M_p(K))$ and $(M_p(\overline{K}))$. Possible equality, limits ?
  When $n = r_1 = 2$, $(M_p(\overline{K}))$ and $(M_p(K))$ can be stationnary ($K = \mathbb{Q}(\sqrt{23})$ - Godwin 1963), both sequences can be strictly decreasing, equal, and converge to a $\lambda > 0$ ($K = \mathbb{Q}(\sqrt{5})$ - Davenport 1948).

- Properties of spectra ? If $n = r_1 = 2$ the inhomogeneous spectrum of K is closed (Barnes and Swinnerton-Dyer 1952).

- Do we have $M_2(\overline{K}) = M_2(K)$?
  No ($K = \mathbb{Q}(\sqrt{73})$ - Godwin 1955).

- More generally what is the behaviour of the sequences $(M_p(K))$ and $(M_p(\overline{K}))$. Possible equality, limits ?
  When $n = r_1 = 2$, $(M_p(\overline{K}))$ and $(M_p(K))$ can be stationnary ($K = \mathbb{Q}(\sqrt{23})$ - Godwin 1963), both sequences can be strictly decreasing, equal, and converge to a $\lambda > 0$ ($K = \mathbb{Q}(\sqrt{5})$ - Davenport 1948).

- Properties of spectra ? If $n = r_1 = 2$ the inhomogeneous spectrum of K is closed (Barnes and Swinnerton-Dyer 1952).

- Effective computation of $M(K)$, of $M(\overline{K})$, and of the upper part of the spectra ?

Plan

1 Introduction

2 Old questions

3 New theoretical results

4 New practical results

5 Successive minima. k-stage Euclideanity. Central division algebras

Theorem 2.

For every number field K, the inhomogeneous spectrum of K is closed.

Theorem 2.

For every number field K, the inhomogeneous spectrum of K is closed.

Theorem 3 (conjecture C_2).

If $r > 1$, there exists a $\xi \in K$ such that

$$M(\overline{K}) = m_K(\xi).$$

Theorem 2.

For every number field K, the inhomogeneous spectrum of K is closed.

Theorem 3 (conjecture C_2).

If $r > 1$, there exists a $\xi \in K$ such that

$$M(\overline{K}) = m_K(\xi).$$

Corollary 1 (conjecture C_1).

For every number field K we have $M(K) = M(\overline{K})$.

Theorem 2.

For every number field K, the inhomogeneous spectrum of K is closed.

Theorem 3 (conjecture C_2).

If $r > 1$, there exists a $\xi \in K$ such that

$$M(\overline{K}) = m_K(\xi).$$

Corollary 1 (conjecture C_1).

For every number field K we have $M(K) = M(\overline{K})$.

If moreover $r > 1$ then $M(K) = M(\overline{K}) \in \mathbb{Q}$.

Corollary 2.

If $r > 1$ and if $M(K) = 1$, K is not norm-Euclidean.

Corollary 2.

If $r > 1$ and if $M(K) = 1$, K is not norm-Euclidean.

Corollary 3 (conjectured by Lenstra).

If $r > 1$ and if

$$\mathcal{A} = \{z \in \overline{K} \text{ such that } \mathcal{N}(z) < 1\},$$

$$K \text{ is norm-Euclidean} \Longleftrightarrow \mathbb{Z}_K + \mathcal{A} = \overline{K}.$$

Corollary 2.

If $r > 1$ and if $M(K) = 1$, K is not norm-Euclidean.

Corollary 3 (conjectured by Lenstra).

If $r > 1$ and if

$$\mathcal{A} = \{z \in \overline{K} \text{ such that } \mathcal{N}(z) < 1\},$$

$$K \text{ is norm-Euclidean} \Longleftrightarrow \mathbb{Z}_K + \mathcal{A} = \overline{K}.$$

Corollary 4.

K being given with $r > 1$, the question whether K is norm-Euclidean or not is decidable.

Theorem 4.

If $r > 1$ and if K is not a CM-field,

Theorem 4.

If $r > 1$ and if K is not a CM-field,

(i) $\forall p \geq 1,\ M_p(K) = M_p(\overline{K}) \in \mathbb{Q}$.

Theorem 4.

If $r > 1$ and if K is not a CM-field,

(i) $\forall p \geq 1,\ M_p(K) = M_p(\overline{K}) \in \mathbb{Q}$.

(ii) $\forall p \geq 1,\ M_{p+1}(K) < M_p(K)$ *and* $\lim_{p \to +\infty} M_p(K) = 0$.

Theorem 4.

If $r > 1$ and if K is not a CM-field,

(i) $\forall p \geq 1,\ M_p(K) = M_p(\overline{K}) \in \mathbb{Q}$.

(ii) $\forall p \geq 1,\ M_{p+1}(K) < M_p(K)$ *and* $\lim_{p \to +\infty} M_p(K) = 0$.

(iii) $\mathrm{sp}(K) = \mathrm{sp}(\overline{K}) = \{M_p(K);\ p \geq 1\} \cup \{0\}$.

Theorem 4.

If $r > 1$ and if K is not a CM-field,

(i) $\forall p \geq 1,\ M_p(K) = M_p(\overline{K}) \in \mathbb{Q}$.

(ii) $\forall p \geq 1,\ M_{p+1}(K) < M_p(K)$ *and* $\lim_{p \to +\infty} M_p(K) = 0$.

(iii) $\mathrm{sp}(K) = \mathrm{sp}(\overline{K}) = \{M_p(K);\ p \geq 1\} \cup \{0\}$.

(iv) *For every $p \geq 1$ the set of x in $\overline{K}$ such that $m_{\overline{K}}(x) = M_p(K)$ is finite modulo $\mathbb{Z}_K$ and is included in K. In particular, if $x \notin K$ then $m_{\overline{K}}(x) = 0$.*

Theorem 4.

If $r > 1$ and if K is not a CM-field,

(i) $\forall p \geq 1,\ M_p(K) = M_p(\overline{K}) \in \mathbb{Q}$.

(ii) $\forall p \geq 1,\ M_{p+1}(K) < M_p(K)$ *and* $\lim_{p \to +\infty} M_p(K) = 0$.

(iii) $\mathrm{sp}(K) = \mathrm{sp}(\overline{K}) = \{M_p(K);\ p \geq 1\} \cup \{0\}$.

(iv) *For every $p \geq 1$ the set of x in $\overline{K}$ such that $m_{\overline{K}}(x) = M_p(K)$ is finite modulo $\mathbb{Z}_K$ and is included in K. In particular, if $x \notin K$ then $m_{\overline{K}}(x) = 0$.*

Corollary 5.

Under the same hypothesis, $M(\overline{K})$ is attained and isolated (conjecture $\boldsymbol{C_3}$).

Plan

1 Introduction

2 Old questions

3 New theoretical results

4 New practical results

5 Successive minima. k-stage Euclideanity. Central division algebras

- An algorithm which computes $M(K)$ for totally real fields K ;

- An algorithm which computes $M(K)$ for totally real fields K ;
- Easy generalization to general number fields ;

- An algorithm which computes $M(K)$ for totally real fields K ;
- Easy generalization to general number fields ;
- $n = 2$: 200 (known before : less than 100 + some exceptional families) ;

- An algorithm which computes $M(K)$ for totally real fields K ;
- Easy generalization to general number fields ;
- $n = 2$: 200 (known before : less than 100 + some exceptional families) ;
- $n = 3$: 400 (known before : less than 100) ;

- An algorithm which computes $M(K)$ for totally real fields K ;
- Easy generalization to general number fields ;
- $n = 2$: 200 (known before : less than 100 + some exceptional families) ;
- $n = 3$: 400 (known before : less than 100) ;
- $n = 4$: 300 (known before : 1) ;

- An algorithm which computes $M(K)$ for totally real fields K ;
- Easy generalization to general number fields ;
- $n = 2$: 200 (known before : less than 100 + some exceptional families) ;
- $n = 3$: 400 (known before : less than 100) ;
- $n = 4$: 300 (known before : 1) ;
- $n = 5$: 250 (known before : 0) ;

- An algorithm which computes $M(K)$ for totally real fields K ;
- Easy generalization to general number fields ;
- $n = 2$: 200 (known before : less than 100 + some exceptional families) ;
- $n = 3$: 400 (known before : less than 100) ;
- $n = 4$: 300 (known before : 1) ;
- $n = 5$: 250 (known before : 0) ;
- $n = 6$: 160 (known before : 0) ;

- An algorithm which computes $M(K)$ for totally real fields K ;
- Easy generalization to general number fields ;
- $n = 2$: 200 (known before : less than 100 + some exceptional families) ;
- $n = 3$: 400 (known before : less than 100) ;
- $n = 4$: 300 (known before : 1) ;
- $n = 5$: 250 (known before : 0) ;
- $n = 6$: 160 (known before : 0) ;
- $n = 7$: 140 (known before : 0) ;

- An algorithm which computes $M(K)$ for totally real fields K ;
- Easy generalization to general number fields ;
- $n = 2$: 200 (known before : less than 100 + some exceptional families) ;
- $n = 3$: 400 (known before : less than 100) ;
- $n = 4$: 300 (known before : 1) ;
- $n = 5$: 250 (known before : 0) ;
- $n = 6$: 160 (known before : 0) ;
- $n = 7$: 140 (known before : 0) ;
- $n = 8$: 20 (known before : 1).

- An algorithm which computes $M(K)$ for totally real fields K ;
- Easy generalization to general number fields ;
- $n = 2$: 200 (known before : less than 100 + some exceptional families) ;
- $n = 3$: 400 (known before : less than 100) ;
- $n = 4$: 300 (known before : 1) ;
- $n = 5$: 250 (known before : 0) ;
- $n = 6$: 160 (known before : 0) ;
- $n = 7$: 140 (known before : 0) ;
- $n = 8$: 20 (known before : 1).
- A beautiful phenomenon : for smallest discriminants of a given degree

$$M(K) = \frac{1}{\min_{\substack{\Upsilon \in \mathbb{Z}_K - \{0\} \\ \Upsilon \text{ not unit}}} |N_{K/\mathbb{Q}}(\Upsilon)|} < 1,$$

and the number of such discriminants grows rapidly with n.

Plan

1 Introduction

2 Old questions

3 New theoretical results

4 New practical results

5 Successive minima. k-stage Euclideanity. Central division algebras

- New number fields with class number 1 but not norm-Euclidean.

- New number fields with class number 1 but not norm-Euclidean.
- The algorithm allows to compute upper parts of $\mathrm{sp}(K)$. We have established conjectures on the second inhomogeneous minimum of some K (H. Cohn).

- New number fields with class number 1 but not norm-Euclidean.
- The algorithm allows to compute upper parts of $\mathrm{sp}(K)$. We have established conjectures on the second inhomogeneous minimum of some K (H. Cohn).
- It allows to check whether a number field is k-stage Euclidean (Cooke 1974).

- New number fields with class number 1 but not norm-Euclidean.
- The algorithm allows to compute upper parts of $\mathrm{sp}(K)$. We have established conjectures on the second inhomogeneous minimum of some K (H. Cohn).
- It allows to check whether a number field is k-stage Euclidean (Cooke 1974).
  - Before, no explicit known example for $n \geq 3$ and $k = 2$.

- New number fields with class number 1 but not norm-Euclidean.
- The algorithm allows to compute upper parts of $\mathrm{sp}(K)$. We have established conjectures on the second inhomogeneous minimum of some K (H. Cohn).
- It allows to check whether a number field is k-stage Euclidean (Cooke 1974).
  - Before, no explicit known example for $n \geq 3$ and $k = 2$.
  - In fact, the 81 first totally real cubic number fields which are principal but not norm-Euclidean are 2-stage Euclidean.

- New number fields with class number 1 but not norm-Euclidean.
- The algorithm allows to compute upper parts of $\mathrm{sp}(K)$. We have established conjectures on the second inhomogeneous minimum of some K (H. Cohn).
- It allows to check whether a number field is k-stage Euclidean (Cooke 1974).
  - Before, no explicit known example for $n \geq 3$ and $k = 2$.
  - In fact, the 81 first totally real cubic number fields which are principal but not norm-Euclidean are 2-stage Euclidean.
  - Many examples in degree 4 and 5.

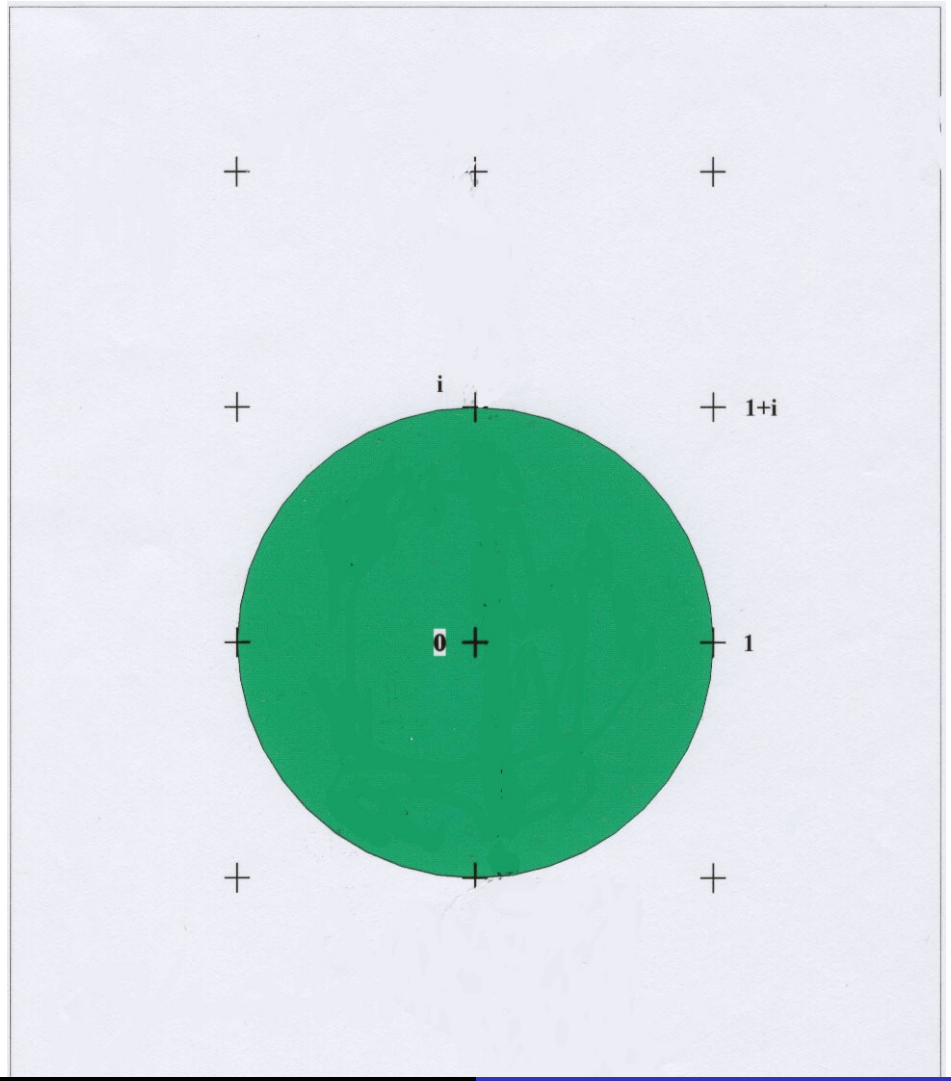
- Generalization to central division algebras over number fields (in collaboration with Eva Bayer-Fluckiger and Jérôme Chaubert).

- Generalization to central division algebras over number fields (in collaboration with Eva Bayer-Fluckiger and Jérôme Chaubert).
- If Λ is a maximal order of a central division algebra D over a number field K, we have similar properties for equality and rationality of the inhomogeneous and Euclidean minima.

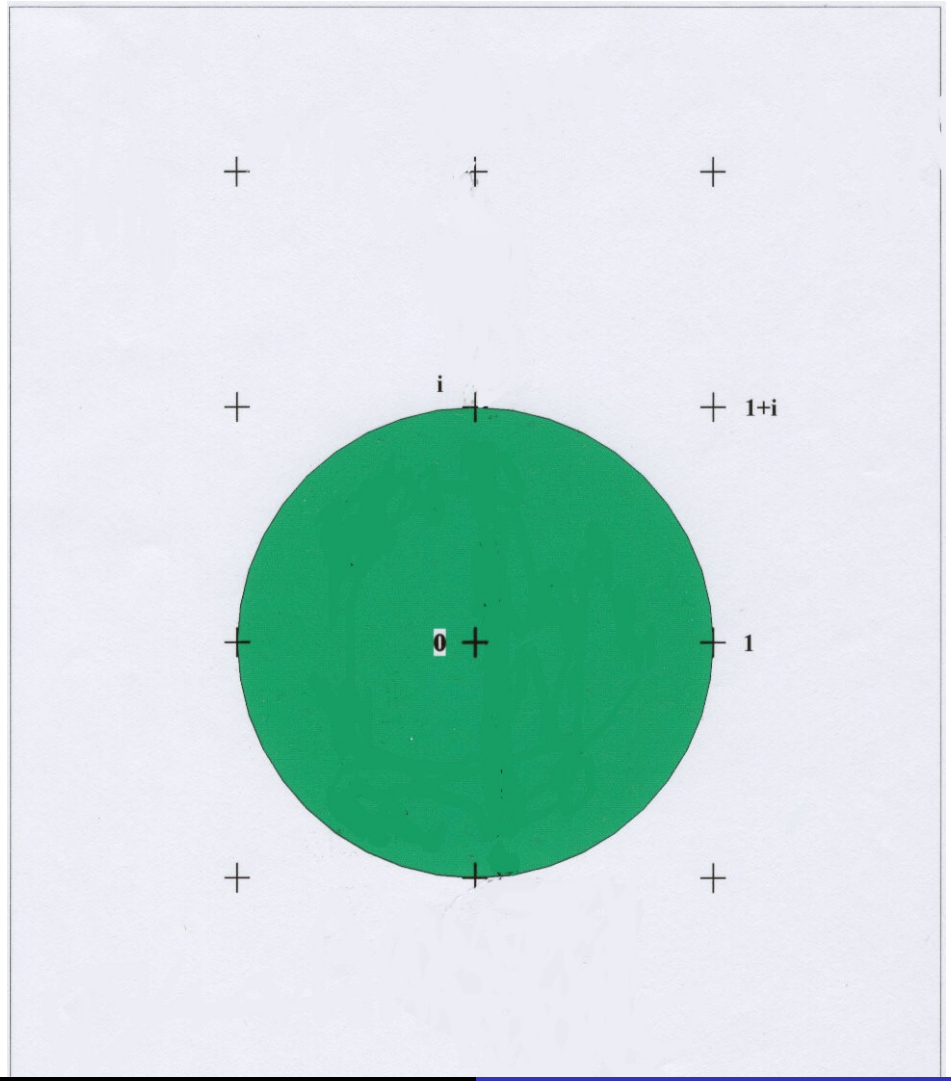
- Generalization to central division algebras over number fields (in collaboration with Eva Bayer-Fluckiger and Jérôme Chaubert).
- If Λ is a maximal order of a central division algebra D over a number field K, we have similar properties for equality and rationality of the inhomogeneous and Euclidean minima.
- Bounds for $M(\Lambda)$ which generalizes bounds established by E. Bayer in the number field case.

- Generalization to central division algebras over number fields (in collaboration with Eva Bayer-Fluckiger and Jérôme Chaubert).
- If Λ is a maximal order of a central division algebra D over a number field K, we have similar properties for equality and rationality of the inhomogeneous and Euclidean minima.
- Bounds for $M(\Lambda)$ which generalizes bounds established by E. Bayer in the number field case.
- Lists of definite Euclidean quaternion algebras over quadratic fields (in progress).

$\mathbb{Q}(\sqrt{-1})$ is norm-Euclidean

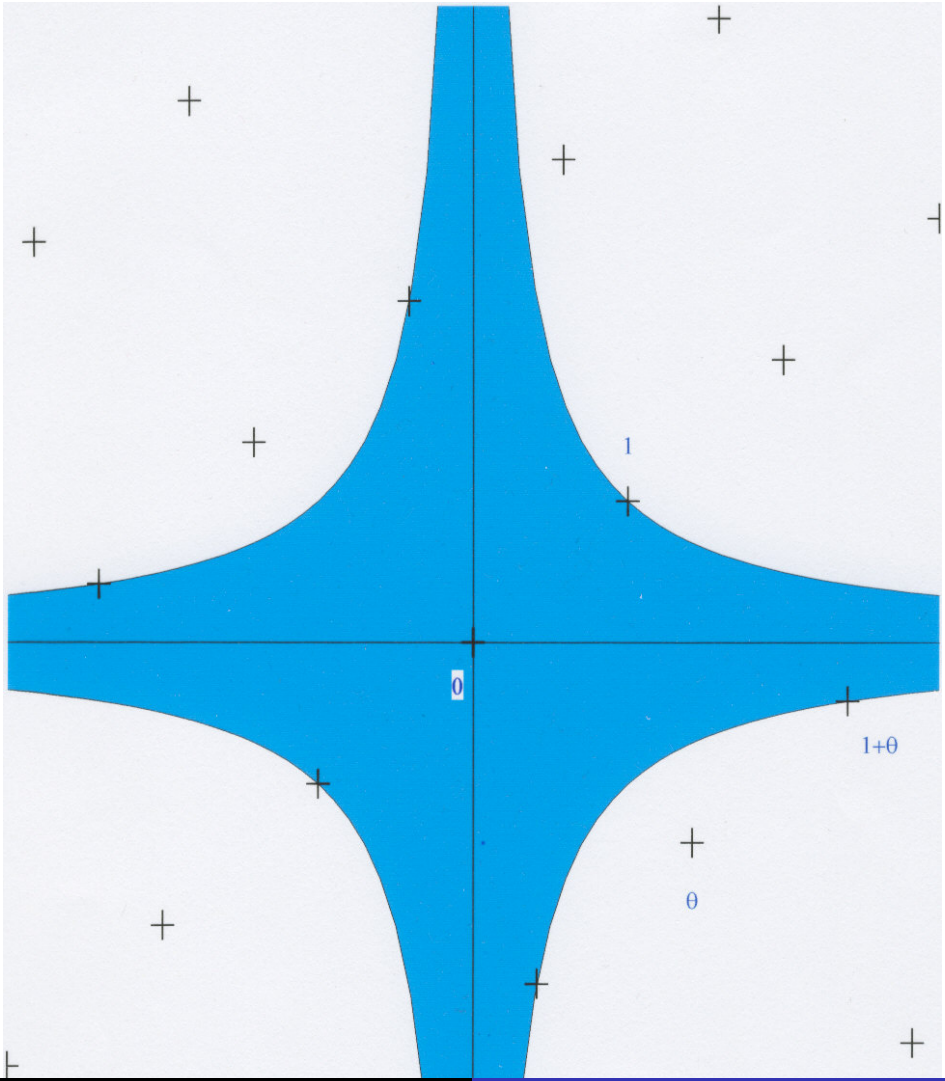


$\mathbb{Q}(\sqrt{-1})$ is norm-Euclidean

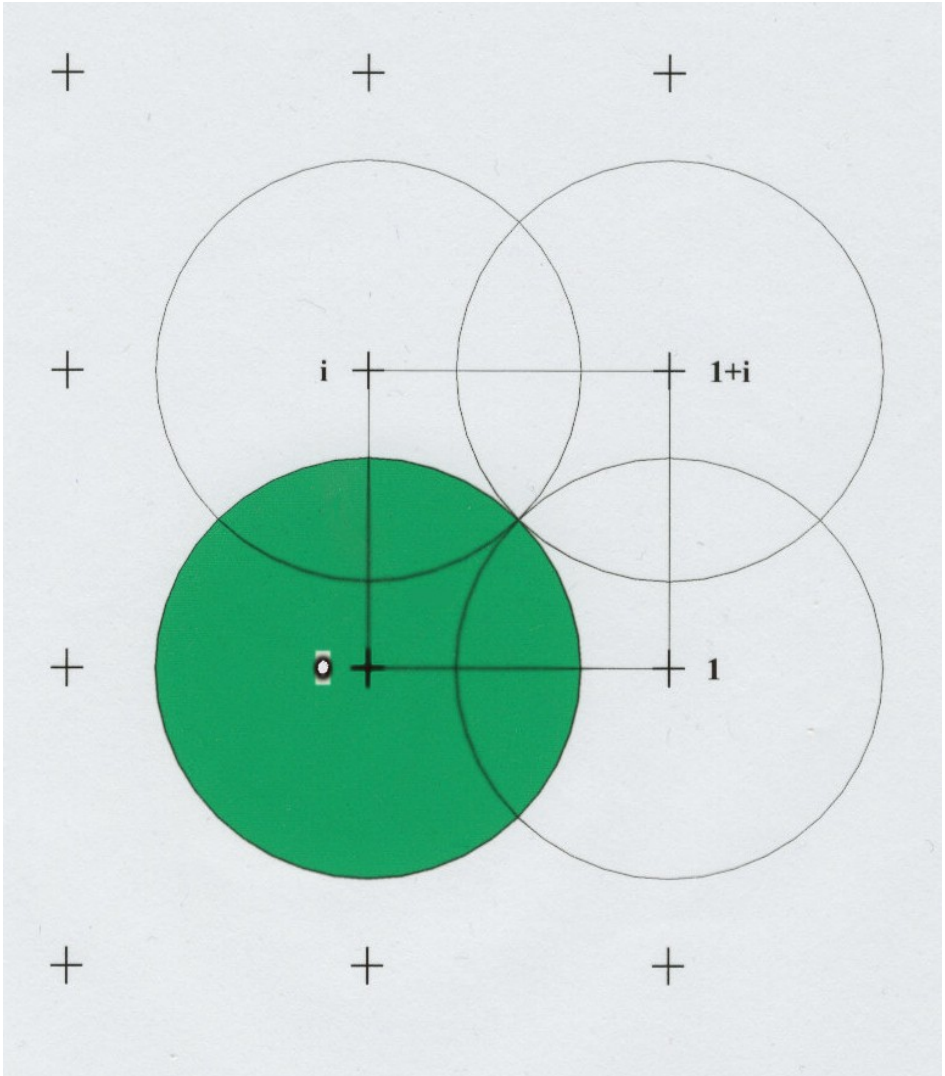


$\mathbb{Q}(\sqrt{2})$ is norm-Euclidean

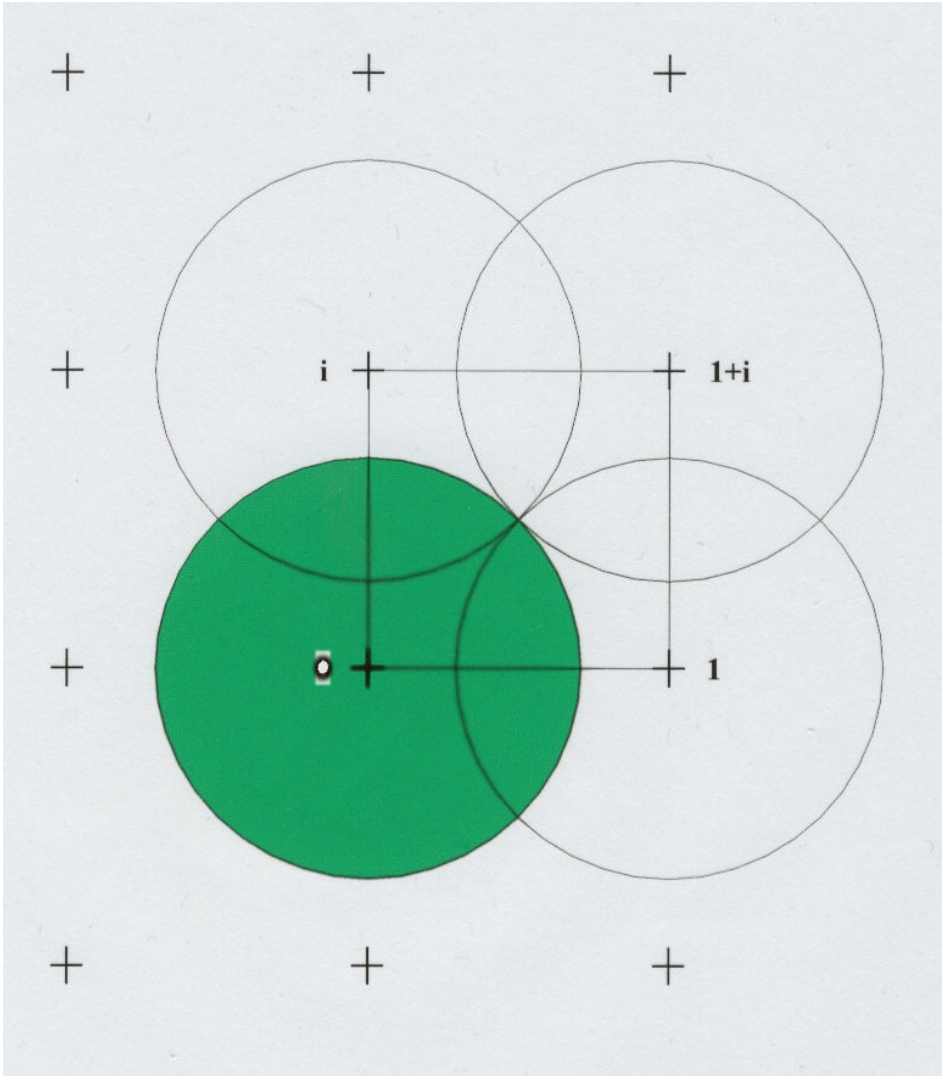
Back



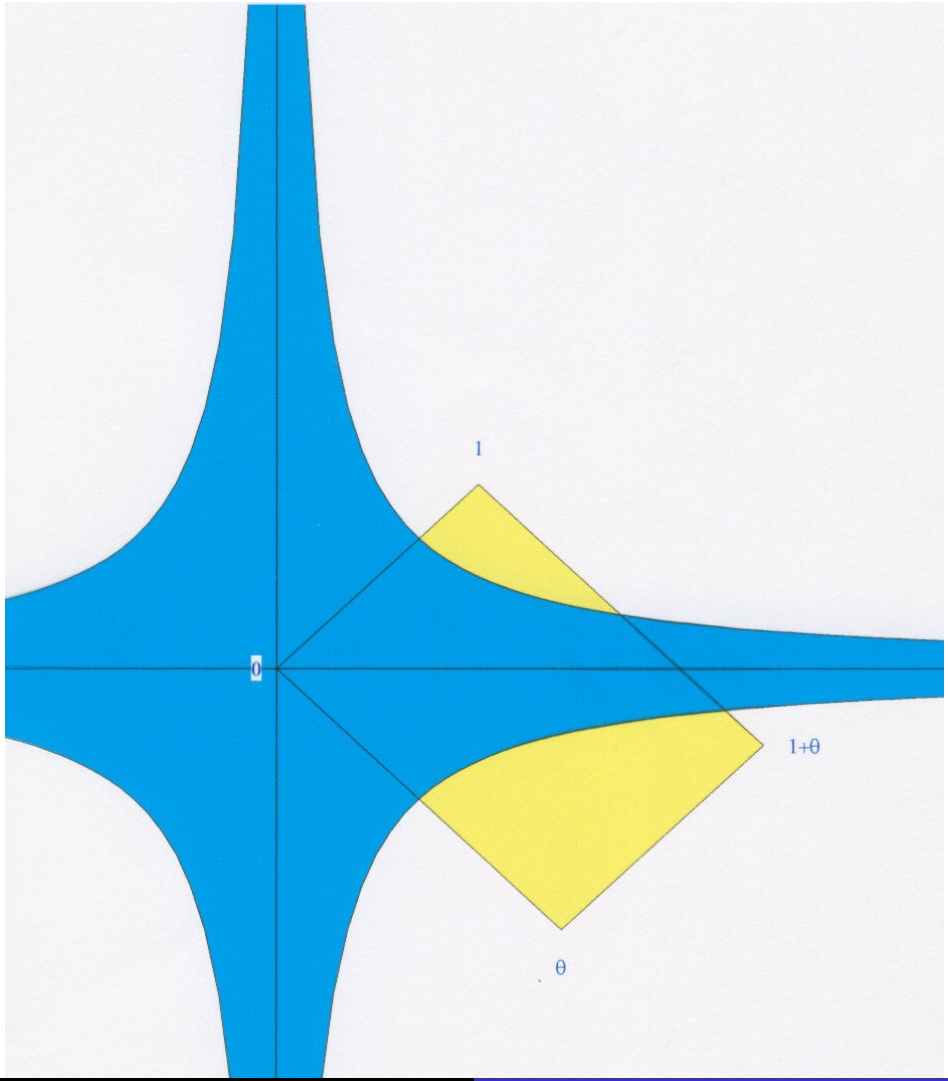
$M(\mathbb{Q}(\sqrt{-1})) = M(\overline{\mathbb{Q}(\sqrt{-1})}) = 1/2$



$M(\mathbb{Q}(\sqrt{-1})) = M(\overline{\mathbb{Q}(\sqrt{-1})}) = 1/2$

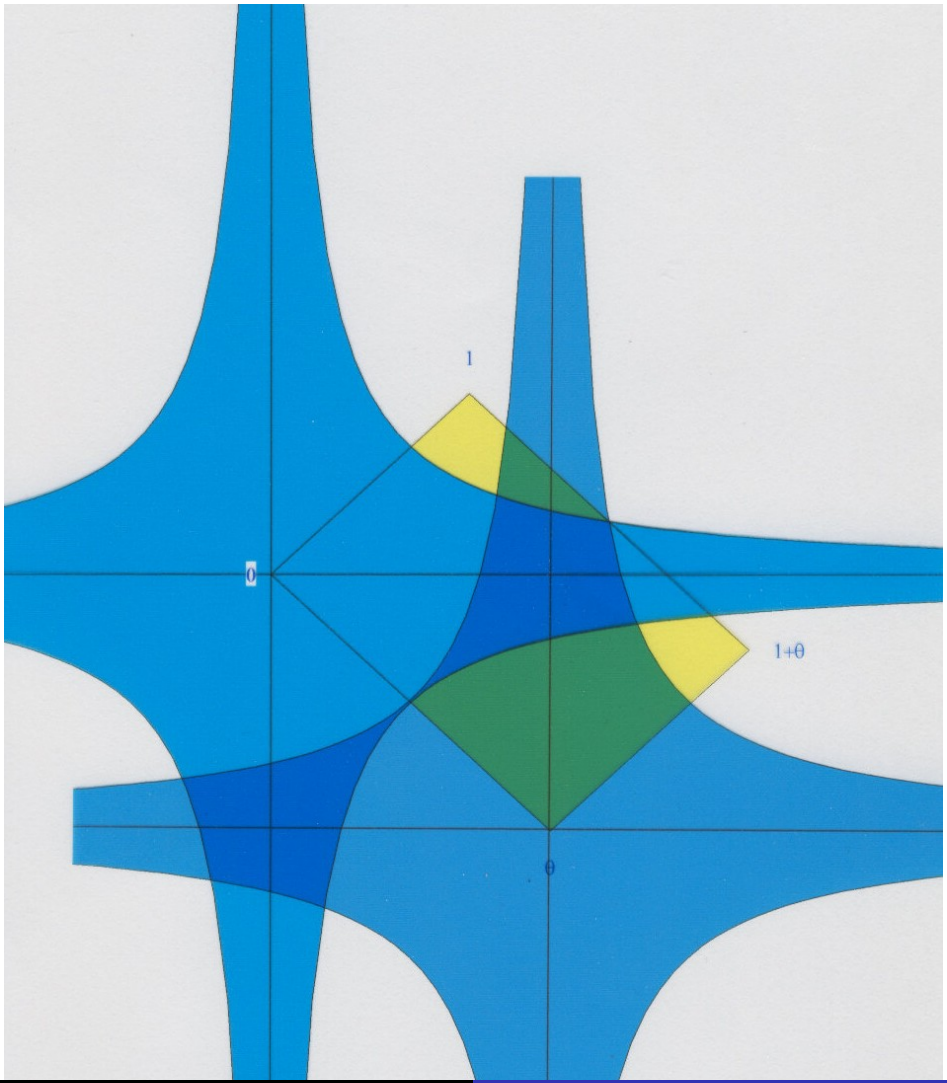


$M(\mathbb{Q}(\sqrt{2})) = M(\overline{\mathbb{Q}(\sqrt{2})}) = 1/2$

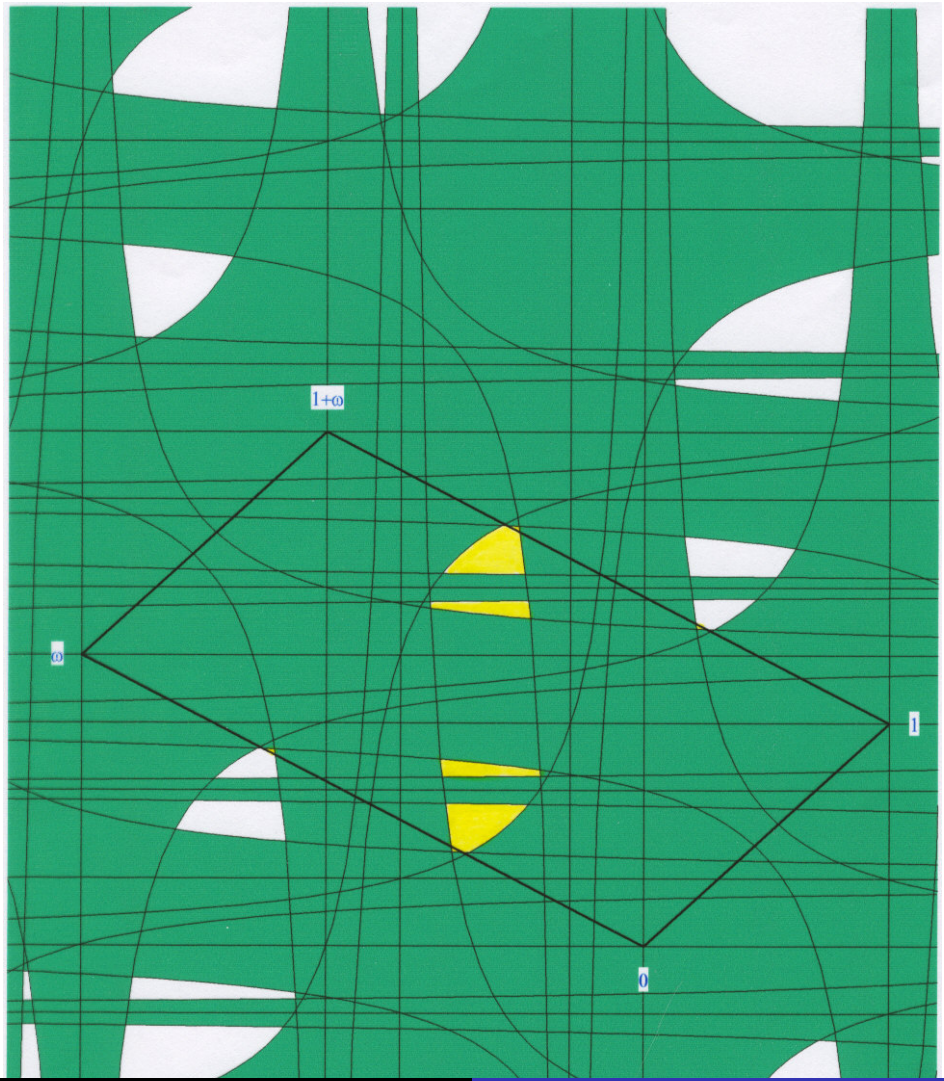


$M(\mathbb{Q}(\sqrt{2})) = \overline{M(\mathbb{Q}(\sqrt{2}))} = 1/2$

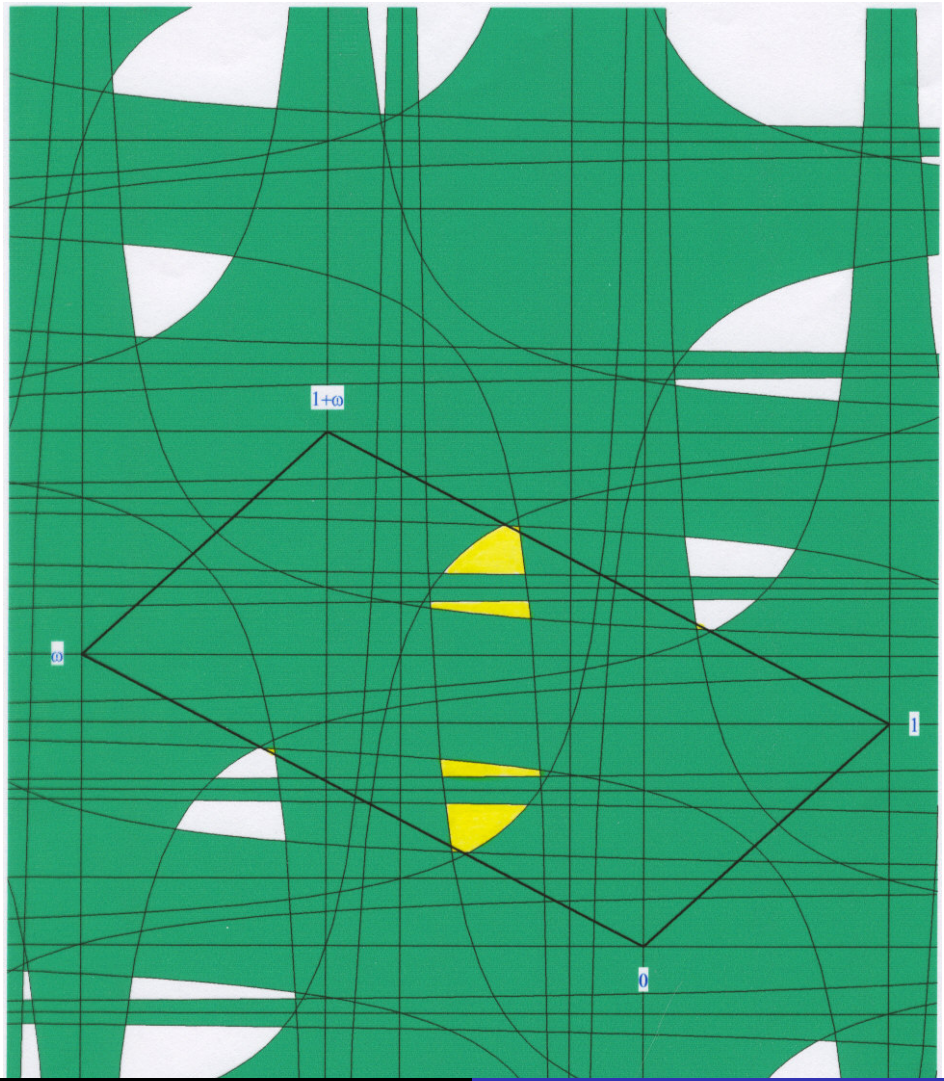
Back

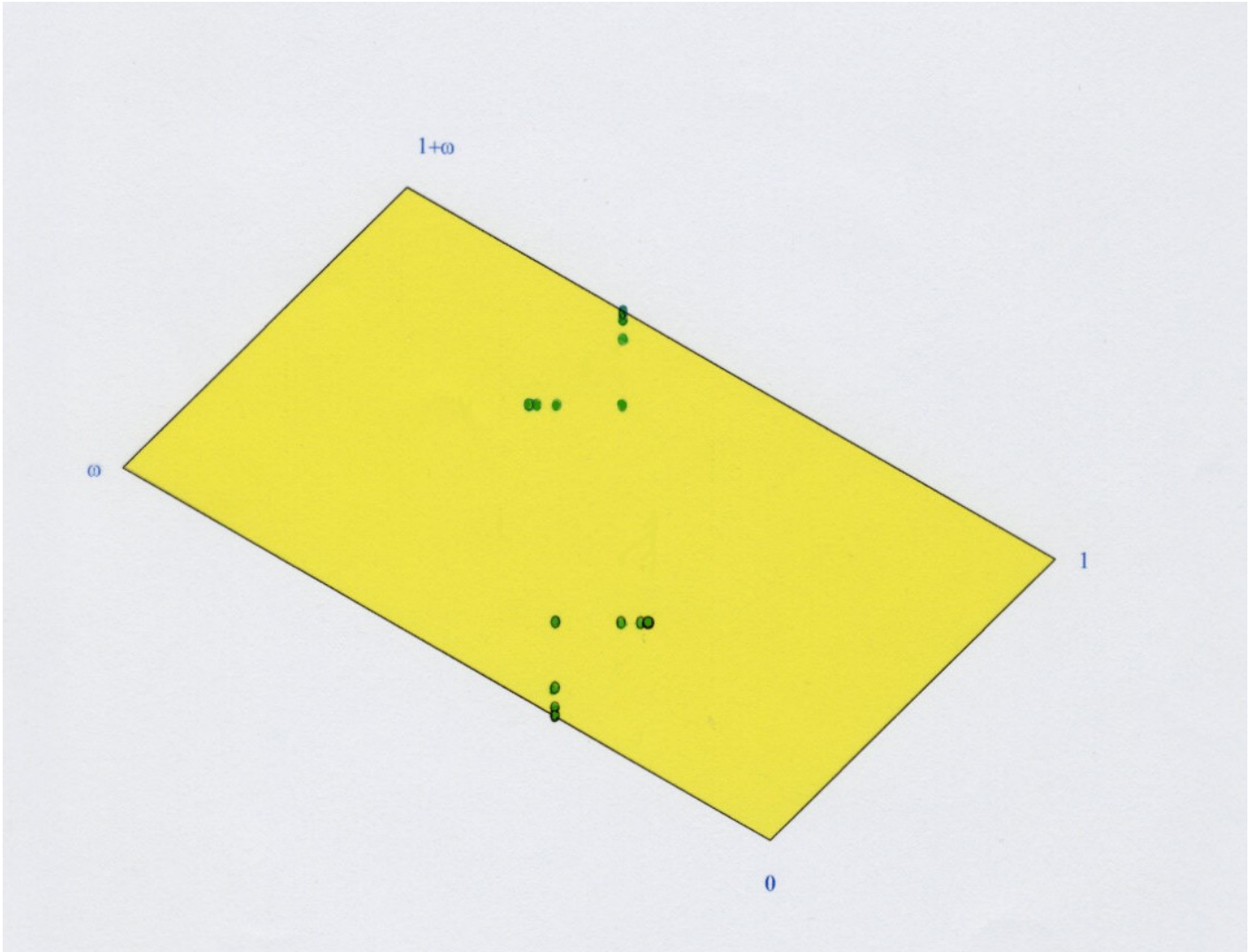


The case $\mathbb{Q}(\sqrt{13})$



The case $\mathbb{Q}(\sqrt{13})$



The case $\mathbb{Q}(\sqrt{13})$

Back