Norm-Euclidean Ideals in Galois Cubic Fields

Kelly Emmrich and Clark Lyons
University of Wisconsin-La Crosse, University of California, Berkeley

2017 West Coast Number Theory Conference
December 18, 2017

Euclidean Rings

Definition

A ring R is **Euclidean** if there exists a function $\phi : R \to \mathbb{Z}_{\geq 0}$ satisfying:

1. $\phi(x) = 0$ if and only if $x = 0$
2. for all $x, y \in R$ there exists $q, r \in R$ such that $x = qy + r$ and $\phi(r) < \phi(y)$.

Euclidean Rings

Definition

A ring R is **Euclidean** if there exists a function $\phi : R \to \mathbb{Z}_{\geq 0}$ satisfying:

1. $\phi(x) = 0$ if and only if $x = 0$
2. for all $x, y \in R$ there exists $q, r \in R$ such that $x = qy + r$ and $\phi(r) < \phi(y)$.

Examples

1. $\mathbb{Z}$ with $\phi(n) = |n|$
2. $\mathbb{Q}[x]$ with $\phi(f) = \deg f + 1$

Euclidean Rings

Definition

A ring R is **Euclidean** if there exists a function $\phi : R \to \mathbb{Z}_{\geq 0}$ satisfying:

1. $\phi(x) = 0$ if and only if $x = 0$
2. for all $x, y \in R$ there exists $q, r \in R$ such that $x = qy + r$ and $\phi(r) < \phi(y)$.

Examples

1. $\mathbb{Z}$ with $\phi(n) = |n|$
2. $\mathbb{Q}[x]$ with $\phi(f) = \deg f + 1$

A Euclidean function allows us to perform the Euclidean algorithm through repeated division. This lets us find greatest common divisors.

Theorem

R is Euclidean $\Rightarrow$ R is a PID $\Rightarrow$ R is a UFD

Euclidean Number Fields

Definition

We say that a number field K is **norm-Euclidean** if the norm map defines a Euclidean function on its ring of integers.

Euclidean Number Fields

Definition

We say that a number field K is **norm-Euclidean** if the norm map defines a Euclidean function on its ring of integers.

It is an important classical question in algebraic number theory to classify which number fields are norm-Euclidean. In the quadratic case, $\mathbb{Q}(\sqrt{d})$ is norm-Euclidean precisely when

$d = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$

Euclidean Number Fields

Definition

We say that a number field K is **norm-Euclidean** if the norm map defines a Euclidean function on its ring of integers.

It is an important classical question in algebraic number theory to classify which number fields are norm-Euclidean. In the quadratic case, $\mathbb{Q}(\sqrt{d})$ is norm-Euclidean precisely when

$$d = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Because the norm map is multiplicative, N is a Euclidean function on $\mathcal{O}_K$ if and only if

$$\text{for all } \frac{x}{y} \in K \text{ there exists } q \in \mathcal{O}_K \text{ such that } N\left(\frac{x}{y} - q\right) < 1.$$

Euclidean Number Fields

Definition

We say that a number field K is **norm-Euclidean** if the norm map defines a Euclidean function on its ring of integers.

It is an important classical question in algebraic number theory to classify which number fields are norm-Euclidean. In the quadratic case, $\mathbb{Q}(\sqrt{d})$ is norm-Euclidean precisely when

$$d = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Because the norm map is multiplicative, N is a Euclidean function on $\mathcal{O}_K$ if and only if

$$\text{for all } \frac{x}{y} \in K \text{ there exists } q \in \mathcal{O}_K \text{ such that } N\left(\frac{x}{y} - q\right) < 1.$$

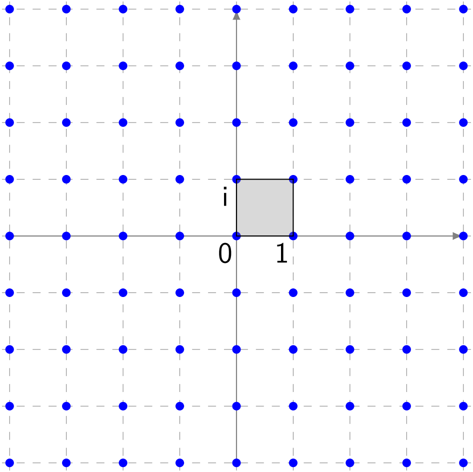
In the imaginary quadratic case this condition becomes geometric since

$$N(a + b\sqrt{-d}) = (a + b\sqrt{-d})(a - b\sqrt{-d}) = |a + b\sqrt{-d}|^2.$$

Norm Euclidean Number Field Examples

Example

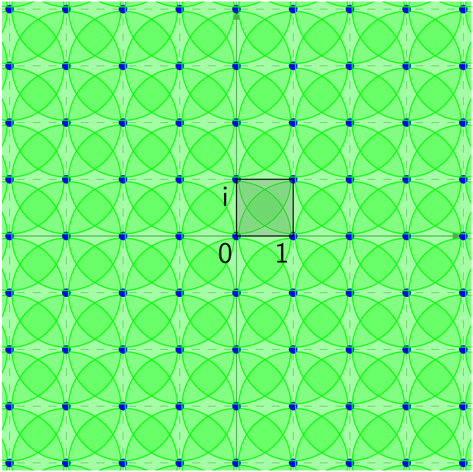
$K = \mathbb{Q}(i) = \mathbb{Q}[x]/(x^2+1) = \{a + bi \mid a, b \in \mathbb{Q}\}$
$\mathcal{O}_K = \{a + bi \mid a, b \in \mathbb{Z}\}$



Norm Euclidean Number Field Examples

Example

$K = \mathbb{Q}(i) = \mathbb{Q}[x]/(x^2+1) = \{a + bi \mid a, b \in \mathbb{Q}\}$
$\mathcal{O}_K = \{a + bi \mid a, b \in \mathbb{Z}\}$

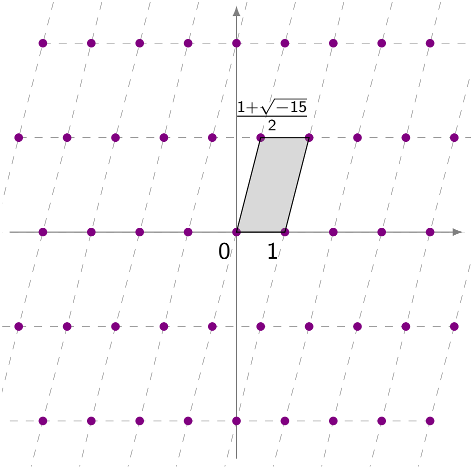


Norm-Euclidean Number Field Examples cont.

Example

$K = \mathbb{Q}(\sqrt{-15}) = \mathbb{Q}[x]/(x^2+15) = \{a + b\sqrt{-15} \mid a, b \in \mathbb{Q}\}$

$\mathcal{O}_K = \{a + b\frac{1+\sqrt{-15}}{2} \mid a, b \in \mathbb{Z}\}$

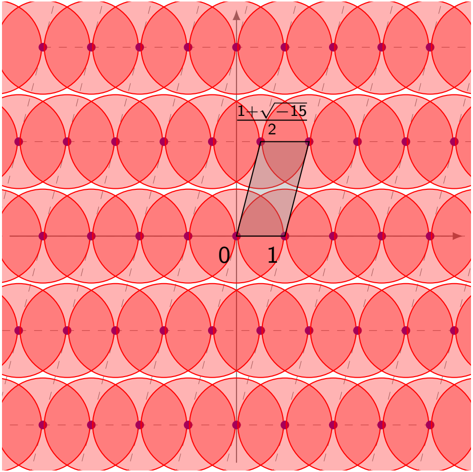


Norm-Euclidean Number Field Examples cont.

Example

$K = \mathbb{Q}(\sqrt{-15}) = \mathbb{Q}[x]/(x^2+15) = \{a + b\sqrt{-15} \mid a, b \in \mathbb{Q}\}$

$\mathcal{O}_K = \{a + b\frac{1+\sqrt{-15}}{2} \mid a, b \in \mathbb{Z}\}$

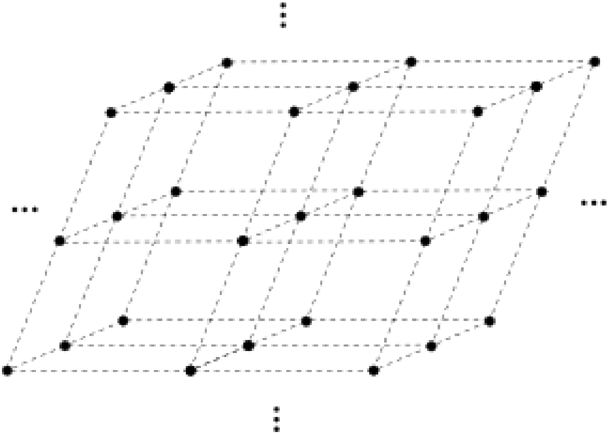


Norm-Euclidean Number Field Examples cont.

Example

$K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(x^3 - x^2 - 44x - 69) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$

$\mathcal{O}_K = \{a + b\frac{\alpha+\alpha^2}{3} + c\alpha^2 \mid a, b, c \in \mathbb{Z}\}$

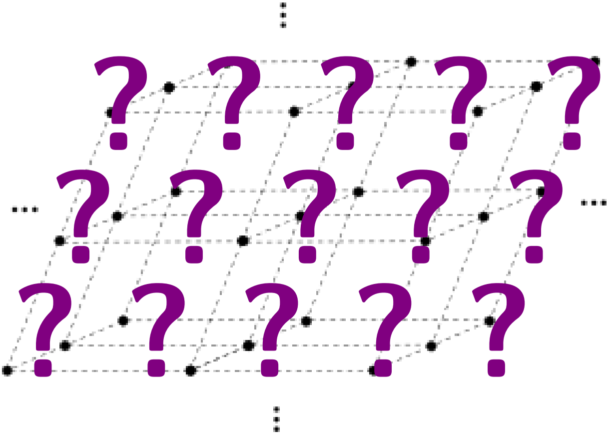


Norm-Euclidean Number Field Examples cont.

Example

$K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(x^3 - x^2 - 44x - 69) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$

$\mathcal{O}_K = \{a + b\frac{\alpha+\alpha^2}{3} + c\alpha^2 \mid a, b, c \in \mathbb{Z}\}$



Norm Euclidean Ideals

Lenstra (79) generalized norm-Euclidean number fields in the following way:

Definition

We say that a number field K is a **norm-Euclidean** if

$$\text{for all } \frac{x}{y} \in K \text{ there exists } q \in \mathcal{O}_K \text{ such that } N\left(\frac{x}{y} - q\right) < 1.$$

Norm Euclidean Ideals

Lenstra (79) generalized norm-Euclidean number fields in the following way:

Definition

We say that a number field K is a **norm-Euclidean** if

$$\text{for all } \frac{x}{y} \in K \text{ there exists } q \in \mathcal{O}_K \text{ such that } N\left(\frac{x}{y} - q\right) < 1.$$

We say that an ideal I of $\mathcal{O}_K$ is a **norm-Euclidean ideal** if

$$\text{for all } \frac{x}{y} \in K \text{ there exists } q \in I \text{ such that } N\left(\frac{x}{y} - q\right) < N(I).$$

Norm Euclidean Ideals

Lenstra (79) generalized norm-Euclidean number fields in the following way:

Definition

We say that a number field K is a **norm-Euclidean** if

$$\text{for all } \frac{x}{y} \in K \text{ there exists } q \in \mathcal{O}_K \text{ such that } N\left(\frac{x}{y} - q\right) < 1.$$

We say that an ideal I of $\mathcal{O}_K$ is a **norm-Euclidean ideal** if

$$\text{for all } \frac{x}{y} \in K \text{ there exists } q \in I \text{ such that } N\left(\frac{x}{y} - q\right) < N(I).$$

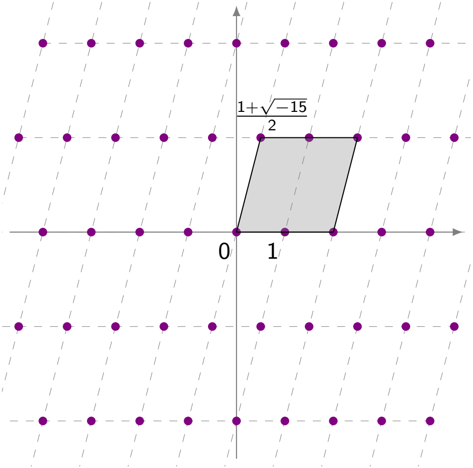
If I is the unit ideal (1), then I is norm-Euclidean if and only if K is.
This property is determined only by the ideal class of I.
Lenstra showed $K = \mathbb{Q}(\sqrt{d})$ possesses a nontrivial norm-Euclidean ideal exactly when $d = -15, -5, 10, 15, 85$.

Norm-Euclidean Ideal Example

Example

$K = \mathbb{Q}(\sqrt{-15}) = \mathbb{Q}[x]/(x^2+15) = \{a + b\sqrt{-15} \mid a, b \in \mathbb{Q}\}$

$\mathcal{O}_K = \{a + b\frac{1+\sqrt{-15}}{2} \mid a, b \in \mathbb{Z}\} \quad I = (2, \frac{1+\sqrt{-15}}{2})$

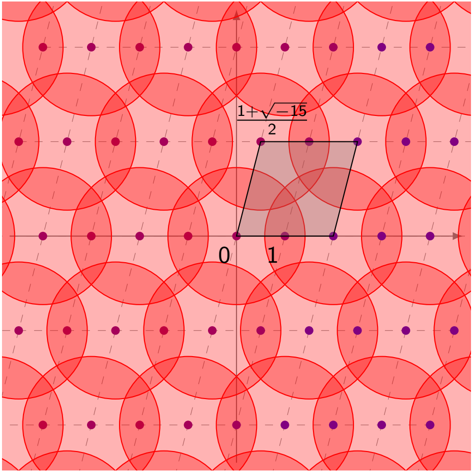


Norm-Euclidean Ideal Example

Example

$K = \mathbb{Q}(\sqrt{-15}) = \mathbb{Q}[x]/(x^2 + 15) = \{a + b\sqrt{-15} \mid a, b \in \mathbb{Q}\}$

$\mathcal{O}_K = \{a + b\frac{1+\sqrt{-15}}{2} \mid a, b \in \mathbb{Z}\} \quad I = (2, \frac{1+\sqrt{-15}}{2})$



Egami's Criterion

Theorem (Egami 1984)

Let K be a number field of degree n, and let f be an arbitrary product of different rational primes that are totally ramified in $K/\mathbb{Q}$. Then K has no norm-Euclidean ideal class, if for every rational integer r relatively prime to f there exists a pair of rational integers a, b such that $f = a + b$ and satisfies:

1. $a > 0, b > 0$
2. there exists $x \in \mathbb{Z}$ such that $x^n \equiv r \cdot a \mod f$
3. neither a nor b is a norm of an integral ideal in K.

Although this criterion is very technical, it has proven very useful for proving that there are very few number fields of certain types with norm-Euclidean ideals. In fact Egami showed that only finitely many Galois cubic fields have a norm-Euclidean ideal, but he did not produce an explicit bound on the discriminant of such a number field.

Our Project

For our project, we are investigating which Galois cubic fields have norm-Euclidean ideals. For discriminant $D < 10^{12}$ we showed that Egami's criterion passed in all but 23 cases.
Of these, nine did not have class number 1:

$$
\begin{array}{ll}
x^3 - 21x - 35, & f = 63 = 9 \times 7 \\
x^3 - 21x + 28, & f = 63 = 9 \times 7 \\
x^3 - x^2 - 30x - 27, & f = 91 = 7 \times 13 \\
x^3 - x^2 - 30x + 64, & f = 91 = 7 \times 13 \\
x^3 - 39x - 26, & f = 117 = 9 \times 13 \\
x^3 - x^2 - 44x - 69, & f = 133 = 7 \times 19 \\
x^3 - x^3 - 44x + 64, & f = 133 = 7 \times 19 \\
x^3 - x^2 - 82x + 64, & f = 247 = 13 \times 19 \\
x^3 - x^2 - 86x - 48, & f = 259 = 7 \times 37
\end{array}
$$

Our Project

For our project, we are investigating which Galois cubic fields have norm-Euclidean ideals. For discriminant $D < 10^{12}$ we showed that Egami's criterion passed in all but 23 cases.
Of these, nine did not have class number 1:

$$x^3 - 21x - 35, \qquad f = 63 = 9 \times 7$$

$$x^3 - 21x + 28, \qquad f = 63 = 9 \times 7$$

$$x^3 - x^2 - 30x - 27, \qquad f = 91 = 7 \times 13$$

$$x^3 - x^2 - 30x + 64, \qquad f = 91 = 7 \times 13$$

$$x^3 - 39x - 26, \qquad f = 117 = 9 \times 13$$

$$x^3 - x^2 - 44x - 69, \qquad f = 133 = 7 \times 19$$

$$x^3 - x^3 - 44x + 64, \qquad f = 133 = 7 \times 19$$

~~$x^3 - x^2 - 82x + 64, \qquad f = 247 = 13 \times 19$~~

$$x^3 - x^2 - 86x - 48, \qquad f = 259 = 7 \times 37$$

Our Project

For our project, we are investigating which Galois cubic fields have norm-Euclidean ideals. For discriminant $D < 10^{12}$ we showed that Egami's criterion passed in all but 23 cases.
Of these, nine did not have class number 1:

$x^3 - 21x - 35,$	$f = 63 = 9 \times 7$
$x^3 - 21x + 28,$	$f = 63 = 9 \times 7$
$x^3 - x^2 - 30x - 27,$	$f = 91 = 7 \times 13$
$x^3 - x^2 - 30x + 64,$	$f = 91 = 7 \times 13$
~~$x^3 - 39x - 26,$~~	~~$f = 117 = 9 \times 13$~~
~~$x^3 - x^2 - 44x - 69,$~~	~~$f = 133 = 7 \times 19$~~
~~$x^3 - x^3 - 44x + 64,$~~	~~$f = 133 = 7 \times 19$~~
~~$x^3 - x^2 - 82x + 64,$~~	~~$f = 247 = 13 \times 19$~~
$x^3 - x^2 - 86x - 48,$	$f = 259 = 7 \times 37$

Our Project

For our project, we are investigating which Galois cubic fields have norm-Euclidean ideals. For discriminant $D < 10^{12}$ we showed that Egami's criterion passed in all but 23 cases.

Of these, nine did not have class number 1:

~~$x^3 - 21x - 35,$~~	~~$f = 63 = 9 \times 7$~~
~~$x^3 - 21x + 28,$~~	~~$f = 63 = 9 \times 7$~~
~~$x^3 - x^2 - 30x - 27,$~~	~~$f = 91 = 7 \times 13$~~
~~$x^3 - x^2 - 30x + 64,$~~	~~$f = 91 = 7 \times 13$~~
~~$x^3 - 39x - 26,$~~	~~$f = 117 = 9 \times 13$~~
~~$x^3 - x^2 - 44x - 69,$~~	~~$f = 133 = 7 \times 19$~~
~~$x^3 - x^3 - 44x + 64,$~~	~~$f = 133 = 7 \times 19$~~
~~$x^3 - x^2 - 82x + 64,$~~	~~$f = 247 = 13 \times 19$~~
~~$x^3 - x^2 - 86x - 48,$~~	~~$f = 259 = 7 \times 37$~~

Our Project

For our project, we are investigating which Galois cubic fields have norm-Euclidean ideals. For discriminant $D < 10^{12}$ we showed that Egami's criterion passed in all but 23 cases.
Of these, nine did not have class number 1:

~~$x^3 - 21x - 35,$~~	~~$f = 63 = 9 \times 7$~~
~~$x^3 - 21x + 28,$~~	~~$f = 63 = 9 \times 7$~~
$x^3 - x^2 - 30x - 27,$	$f = 91 = 7 \times 13$
$x^3 - x^2 - 30x + 64,$	$f = 91 = 7 \times 13$
~~$x^3 - 39x - 26,$~~	~~$f = 117 = 9 \times 13$~~
~~$x^3 - x^2 - 44x - 69,$~~	~~$f = 133 = 7 \times 19$~~
~~$x^3 - x^3 - 44x + 64,$~~	~~$f = 133 = 7 \times 19$~~
~~$x^3 - x^2 - 82x + 64,$~~	~~$f = 247 = 13 \times 19$~~
~~$x^3 - x^2 - 86x - 48,$~~	~~$f = 259 = 7 \times 37$~~

Egami's Criterion Under GRH

Abelian number fields correspond to groups of Dirichlet characters, and the splitting behavior of primes is determined by the values of these characters. To verify Egami's criterion, we write

$$f = uq_1 + vq_2$$

for $q_1 < q_2$ the least two inert primes. We must then control the cubic character values $\chi(u) = \zeta$ and $\psi(u) = \omega$.

Egami's Criterion Under GRH

Abelian number fields correspond to groups of Dirichlet characters, and the splitting behavior of primes is determined by the values of these characters. To verify Egami's criterion, we write

$$f = uq_1 + vq_2$$

for $q_1 < q_2$ the least two inert primes. We must then control the cubic character values $\chi(u) = \zeta$ and $\psi(u) = \omega$.
To show that such a decomposition is possible, we need GRH bounds the least nonresidues of characters. These roughly say

$$q_i = O(\log(f)^2).$$

Our goal is to use this to prove that there are no more Galois cubic number fields with norm-Euclidean ideal classes with discriminant greater than some value.

Acknowledgments

We would like to extend thanks to our mentor, Dr. Kevin McGown, the Chico State REUT, and the National Science Foundation Grant DMS-1559788 for their support.

References

1. S. Egami, *On finiteness of the numbers of Euclidean fields in some classes of number fields*. Tokyo J. Math. Vol. 7, No. 1, 1984 .
2. H.W. Lenstra, Jr., *Euclidéan ideal classes*, Soc. Math. France Asterisque, 1979.
3. The On-Line Encyclopedia of Integer Sequences, The OEIS Foundation , 7 July 2017. Accessed 7 July 2017.