# Cyclotomic Number Fields

Daniel Fretwell

School of Mathematics and Statistics, University of Sheffield

Semester 1, 2010/2011

# Outline of talk

1. Introduction to cyclotomic number fields
2. A bit of Galois theory
3. Galois theory for cyclotomic number fields
4. What's next?

# What is a cyclotomic number field?

We begin with a basic definition.

## Definition

A number field is a field $K \supseteq \mathbb{Q}$ such that the degree of the field extension $K/\mathbb{Q}$ is finite. We refer to the degree of a number field as the degree of the field extension $K/\mathbb{Q}$, i.e. the dimension of $K$ as a $\mathbb{Q}$-vector space.

## Examples

The fields:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

and

$$\mathbb{Q}(\sqrt[3]{7}) = \{a + b\sqrt[3]{7} + c(\sqrt[3]{7})^2 \mid a, b, c \in \mathbb{Q}\}$$

are number fields. They have degrees 2 and 3 respectively.

# What is a cyclotomic number field?

We begin with a basic definition.

## Definition

A number field is a field $K \supseteq \mathbb{Q}$ such that the degree of the field extension $K/\mathbb{Q}$ is finite. We refer to the degree of a number field as the degree of the field extension $K/\mathbb{Q}$, i.e. the dimension of $K$ as a $\mathbb{Q}$-vector space.

## Examples

The fields:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

and

$$\mathbb{Q}(\sqrt[3]{7}) = \{a + b\sqrt[3]{7} + c(\sqrt[3]{7})^2 \mid a, b, c \in \mathbb{Q}\}$$

are number fields. They have degrees 2 and 3 respectively.

We can create number fields using primitive *n*th roots of unity, in doing this we get the cyclotomic number fields.

**Definition**

A cyclotomic number field is a number field of the form $\mathbb{Q}(\zeta_n)$ for some primitive *n*th root of unity.

It can be shown that the degree of the cyclotomic number field $\mathbb{Q}(\zeta_n)$ is $\phi(n)$ where $\phi$ is the Euler phi function.

**Example**

When $n = 4$ we can take $\zeta_4 = i$ and so we see that the familliar number field $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ is actually a cyclotomic number field. This is clearly a number field of degree $2 = \phi(4)$.

For the purposes of this talk we only consider the case where $n$ is a prime $p$. Then we see that $\mathbb{Q}(\zeta_p)$ has degree $\phi(p) = p - 1$.

We can create number fields using primitive $n$th roots of unity, in doing this we get the cyclotomic number fields.

**Definition**

A cyclotomic number field is a number field of the form $\mathbb{Q}(\zeta_n)$ for some primitive $n$th root of unity.

It can be shown that the degree of the cyclotomic number field $\mathbb{Q}(\zeta_n)$ is $\phi(n)$ where $\phi$ is the Euler phi function.

**Example**

When $n = 4$ we can take $\zeta_4 = i$ and so we see that the familliar number field $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ is actually a cyclotomic number field. This is clearly a number field of degree $2 = \phi(4)$.

For the purposes of this talk we only consider the case where $n$ is a prime $p$. Then we see that $\mathbb{Q}(\zeta_p)$ has degree $\phi(p) = p - 1$.

We can create number fields using primitive $n$th roots of unity, in doing this we get the cyclotomic number fields.

**Definition**

A cyclotomic number field is a number field of the form $\mathbb{Q}(\zeta_n)$ for some primitive $n$th root of unity.

It can be shown that the degree of the cyclotomic number field $\mathbb{Q}(\zeta_n)$ is $\phi(n)$ where $\phi$ is the Euler phi function.

**Example**

When $n = 4$ we can take $\zeta_4 = i$ and so we see that the familliar number field $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ is actually a cyclotomic number field. This is clearly a number field of degree $2 = \phi(4)$.

For the purposes of this talk we only consider the case where $n$ is a prime $p$. Then we see that $\mathbb{Q}(\zeta_p)$ has degree $\phi(p) = p - 1$.

In the prime case, letting $\zeta_p = \zeta$ for ease of reading, we can use the theory of field extensions to tell us that a generating set for $\mathbb{Q}(\zeta)$ is simply $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$.

This tells us that:

**Theorem**

The field $\mathbb{Q}(\zeta)$ can be written explicitly as:

$$\mathbb{Q}(\zeta) = \{a_0 + a_1\zeta + a_2\zeta^2 \ldots + a_{p-2}\zeta^{p-2} \mid a_0, a_1, \ldots, a_{p-2} \in \mathbb{Q}\}$$

The aim of this talk is to show that there is actually a surprising subfield of $\mathbb{Q}(\zeta)$ for each prime $p$.

In the prime case, letting $\zeta_p = \zeta$ for ease of reading, we can use the theory of field extensions to tell us that a generating set for $\mathbb{Q}(\zeta)$ is simply $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$.

This tells us that:

**Theorem**

The field $\mathbb{Q}(\zeta)$ can be written explicitly as:

$$\mathbb{Q}(\zeta) = \{a_0 + a_1\zeta + a_2\zeta^2 \ldots + a_{p-2}\zeta^{p-2} \mid a_0, a_1, \ldots, a_{p-2} \in \mathbb{Q}\}$$

The aim of this talk is to show that there is actually a surprising subfield of $\mathbb{Q}(\zeta)$ for each prime $p$.

In the prime case, letting $\zeta_p = \zeta$ for ease of reading, we can use the theory of field extensions to tell us that a generating set for $\mathbb{Q}(\zeta)$ is simply $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$.

This tells us that:

**Theorem**

The field $\mathbb{Q}(\zeta)$ can be written explicitly as:

$$\mathbb{Q}(\zeta) = \{a_0 + a_1\zeta + a_2\zeta^2 \ldots + a_{p-2}\zeta^{p-2} \mid a_0, a_1, \ldots, a_{p-2} \in \mathbb{Q}\}$$

The aim of this talk is to show that there is actually a surprising subfield of $\mathbb{Q}(\zeta)$ for each prime $p$.

# What are cyclotomic number fields used for?

Cyclotomic number fields have a wide range of uses in number theory:

- Proving quadratic reciprocity. This can be achieved using the Gauss sum that we investigate later.
- Forming more general reciprocity laws for higher powers. The cyclotomic number fields turn out to be the perfect setting in which to study higher reciprocity laws.
- We can make codes out of cyclotomic number fields.
- Kummer used factorisations of certain ideals in cyclotomic number fields to prove a large portion of Fermat's last theorem, when the exponent is a so called regular prime. This was one of the major achievements of algebraic number theory in the 19th century.

- Gauss used cyclotomic number fields in his studies of polygon construction. He proved that the regular 17-gon is constuctible using only ruler and compass. His argument extends to prove an amazing theorem, that for a prime $p > 2$ the regular $p$-gon is constructible if and only if $p$ is a Fermat prime.
- Cyclotomic number fields feature in class field theory - the topic of my project - although we won't be seeing much of this, we will get to see the Kronecker-Weber theorem in action.

# Outline of talk

# The Galois group of a field extension

If we have a field extension $L/K$, we can consider the automorphisms of $L$ that fix the elements of $K$. These are the maps from $L$ to $L$ that respect the operations of $L$ and send the elements of $K$ to themselves.

It is easy to check that:

**Theorem**

The set of these automorphisms form a group under composition. This is called the Galois group of the field extension $L/K$, denoted $\mathrm{Gal}(L/K)$.

# The Galois group of a field extension

If we have a field extension $L/K$, we can consider the automorphisms of $L$ that fix the elements of $K$. These are the maps from $L$ to $L$ that respect the operations of $L$ and send the elements of $K$ to themselves.

It is easy to check that:

**Theorem**

The set of these automorphisms form a group under composition. This is called the Galois group of the field extension $L/K$, denoted $\mathrm{Gal}(L/K)$.

### Example

The field $\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}$ has two automorphisms:

$$\iota(a + bi) = a + bi$$

$$\sigma(a + bi) = a - bi$$

Both of these automorphisms fix elements of $\mathbb{Q}$ (set $b = 0$). It can easily be shown that there are no more automorphisms, thus $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{\iota, \sigma\}$ and so is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, the cyclic group of order 2.

We can impose certain conditions on a field extension to make it so that the Galois group has the same order as the degree of the extension. These extensions are called Galois extensions.

## Example

The field $\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}$ has two automorphisms:

$$\iota(a + bi) = a + bi$$

$$\sigma(a + bi) = a - bi$$

Both of these automorphisms fix elements of $\mathbb{Q}$ (set $b = 0$). It can easily be shown that there are no more automorphisms, thus $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{\iota, \sigma\}$ and so is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, the cyclic group of order 2.

We can impose certain conditions on a field extension to make it so that the Galois group has the same order as the degree of the extension. These extensions are called Galois extensions.

# Motivating the Galois correspondence

The Galois correspondence demonstrates the true power of Galois theory.

Roughly, it says that when we work inside a Galois extension $L/K$ of finite degree, there is a one-to-one correspondence between the subgroups of the Galois group $\mathrm{Gal}(L/K)$ and the fields lying in between $L$ and $K$, the so called intermediate fields.

An exact result here is that if we find a subgroup of order $m$ then there is a corresponding intermediate field of degree $\frac{|\mathrm{Gal}(L/K)|}{m}$ over $\mathbb{Q}$.

# Outline of talk

# What does Galois theory tell us about cyclotomic number fields?

Let $p$ be an odd prime and let $\zeta$ be a primitive $p$th root of unity.

The maps defined on $\mathbb{Q}(\zeta)$ by:

$$\sigma_i : \zeta \longmapsto \zeta^i$$

for $i = 1, 2, \ldots, p-1$ are all automorphisms of $\mathbb{Q}(\zeta)$ that fix $\mathbb{Q}$. In fact these are them all.

Thus:

$$\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_{p-1}\} \text{ with operation } \sigma_i\sigma_j = \sigma_{ij}$$

It is now easy to see that we have an isomorphism with $(\mathbb{Z}/p\mathbb{Z})^\times$ via $\sigma_i \longmapsto i$.

# What does Galois theory tell us about cyclotomic number fields?

Let $p$ be an odd prime and let $\zeta$ be a primitive $p$th root of unity.

The maps defined on $\mathbb{Q}(\zeta)$ by:

$$\sigma_i \,:\, \zeta \longmapsto \zeta^i$$

for $i = 1, 2, \ldots, p-1$ are all automorphisms of $\mathbb{Q}(\zeta)$ that fix $\mathbb{Q}$. In fact these are them all.

Thus:

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_{p-1}\} \text{ with operation } \sigma_i\sigma_j = \sigma_{ij}$$

It is now easy to see that we have an isomorphism with $(\mathbb{Z}/p\mathbb{Z})^\times$ via $\sigma_i \longmapsto i$.

# What does Galois theory tell us about cyclotomic number fields?

Let $p$ be an odd prime and let $\zeta$ be a primitive $p$th root of unity.

The maps defined on $\mathbb{Q}(\zeta)$ by:

$$\sigma_i \; : \; \zeta \longmapsto \zeta^i$$

for $i = 1, 2, \ldots, p - 1$ are all automorphisms of $\mathbb{Q}(\zeta)$ that fix $\mathbb{Q}$. In fact these are them all.

Thus:

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_{p-1}\} \text{ with operation } \sigma_i\sigma_j = \sigma_{ij}$$

It is now easy to see that we have an isomorphism with $(\mathbb{Z}/p\mathbb{Z})^\times$ via $\sigma_i \longmapsto i$.

Now $(\mathbb{Z}/p\mathbb{Z})^\times$ has a subgroup of order $\frac{p-1}{2}$, the subgroup of squares mod $p$.

By the Galois correspondence and the fact that the Galois group is Abelian here, this implies the existence of a unique intermediate field $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta)$ that has degree $\frac{p-1}{\left(\frac{p-1}{2}\right)} = 2$ over $\mathbb{Q}$.

The interesting question is, what is this intermediate field $K$?

Now $(\mathbb{Z}/p\mathbb{Z})^\times$ has a subgroup of order $\frac{p-1}{2}$, the subgroup of squares mod $p$.

By the Galois correspondence and the fact that the Galois group is Abelian here, this implies the existence of a unique intermediate field $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta)$ that has degree $\frac{p-1}{\left(\frac{p-1}{2}\right)} = 2$ over $\mathbb{Q}$.

The interesting question is, what is this intermediate field $K$?

# The quadratic Gauss sum

Gauss answered this question in his Disquisitiones Arithmeticae. He cleverly constructed the following element of $\mathbb{Q}(\zeta)$ using the Legendre symbol:

$$G = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a$$

This is known as a Gauss sum. He then carried out a nice manipulation and found that:

$$G^2 = (-1)^{\frac{p-1}{2}} p := p^*$$

This shows that $G = \sqrt{p^*}$ lies in $\mathbb{Q}(\zeta)$. It was then clear to Gauss that $\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta)$. Since $\mathbb{Q}(\sqrt{p^*})$ does in fact have degree 2 over $\mathbb{Q}$, we have found our quadratic subfield.

# The quadratic Gauss sum

Gauss answered this question in his Disquisitiones Arithmeticae. He cleverly constructed the following element of $\mathbb{Q}(\zeta)$ using the Legendre symbol:

$$G = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a$$

This is known as a Gauss sum. He then carried out a nice manipulation and found that:

$$G^2 = (-1)^{\frac{p-1}{2}} p := p^*$$

This shows that $G = \sqrt{p^*}$ lies in $\mathbb{Q}(\zeta)$. It was then clear to Gauss that $\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta)$. Since $\mathbb{Q}(\sqrt{p^*})$ does in fact have degree 2 over $\mathbb{Q}$, we have found our quadratic subfield.

# The quadratic Gauss sum

Gauss answered this question in his Disquisitiones Arithmeticae. He cleverly constructed the following element of $\mathbb{Q}(\zeta)$ using the Legendre symbol:

$$G = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a$$

This is known as a Gauss sum. He then carried out a nice manipulation and found that:

$$G^2 = (-1)^{\frac{p-1}{2}} p := p^*$$

This shows that $G = \sqrt{p^*}$ lies in $\mathbb{Q}(\zeta)$. It was then clear to Gauss that $\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta)$. Since $\mathbb{Q}(\sqrt{p^*})$ does in fact have degree 2 over $\mathbb{Q}$, we have found our quadratic subfield.

# Examples of the Gauss sum and the quadratic subfield

We carry out the constructions in the previous slide explicitly for the cases when $p = 3$ and $p = 5$.

**$p = 3$**

We have that $G = \zeta - \zeta^2$ so that $G^2 = (\zeta - \zeta^2)^2 = \zeta^2 - 2\zeta^3 + \zeta^4$. But $\zeta^3 = 1$ and also since $\zeta \neq 1$, we have that $\zeta^2 + \zeta + 1 = 0$. Using these facts we see that $G^2 = \zeta^2 - 2 + \zeta = -1 - 2 = -3$, so that $G = \sqrt{-3}$ and thus $\mathbb{Q}(\sqrt{-3}) \subseteq \mathbb{Q}(\zeta_3)$.

**$p = 5$**

We have that $G = \zeta - \zeta^2 - \zeta^3 + \zeta^4$ and we see that $G^2 = \ldots = -\zeta - \zeta^2 - \zeta^3 - \zeta^4 + 4\zeta^5 = -(-1) + 4 = 5$ using the facts that $\zeta^5 = 1$ and $\zeta^4 + \zeta^3 + \zeta^2 + 1 = 0$. This shows us that $G = \sqrt{5}$ and so $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta)$.

# Examples of the Gauss sum and the quadratic subfield

We carry out the constructions in the previous slide explicitly for the cases when $p = 3$ and $p = 5$.

**$p = 3$**

We have that $G = \zeta - \zeta^2$ so that $G^2 = (\zeta - \zeta^2)^2 = \zeta^2 - 2\zeta^3 + \zeta^4$. But $\zeta^3 = 1$ and also since $\zeta \neq 1$, we have that $\zeta^2 + \zeta + 1 = 0$. Using these facts we see that $G^2 = \zeta^2 - 2 + \zeta = -1 - 2 = -3$, so that $G = \sqrt{-3}$ and thus $\mathbb{Q}(\sqrt{-3}) \subseteq \mathbb{Q}(\zeta_3)$.

**$p = 5$**

We have that $G = \zeta - \zeta^2 - \zeta^3 + \zeta^4$ and we see that $G^2 = \ldots = -\zeta - \zeta^2 - \zeta^3 - \zeta^4 + 4\zeta^5 = -(-1) + 4 = 5$ using the facts that $\zeta^5 = 1$ and $\zeta^4 + \zeta^3 + \zeta^2 + 1 = 0$. This shows us that $G = \sqrt{5}$ and so $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta)$.

# Outline of talk

# Generalising this - The Kronecker-Weber theorem

In class field theory we study certain extensions of a number field $K$. Specifically we look at the ones with Abelian Galois group. Such an extension is called an Abelian extension.
The Kronecker-Weber theorem is a corollary of more general theorems in class field theory. It says that:

**Kronecker - Weber Theorem**

Each finite abelian extension $L$ of $\mathbb{Q}$ is contained inside a cyclotomic number field $\mathbb{Q}(\zeta_n)$ for some $n \in \mathbb{N}$.

We have seen this in action in the previous slide. We have the Abelian extension $\mathbb{Q}(\sqrt{p^*})$ of $\mathbb{Q}$. This is an Abelian extension since it has Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}$, which is an Abelian group. We then saw that this is contained inside the cyclotomic field $\mathbb{Q}(\zeta_p)$, which is predicted by the theorem above.

# Generalising this - The Kronecker-Weber theorem

In class field theory we study certain extensions of a number field $K$. Specifically we look at the ones with Abelian Galois group. Such an extension is called an Abelian extension.
The Kronecker-Weber theorem is a corollary of more general theorems in class field theory. It says that:

**Kronecker - Weber Theorem**

Each finite abelian extension $L$ of $\mathbb{Q}$ is contained inside a cyclotomic number field $\mathbb{Q}(\zeta_n)$ for some $n \in \mathbb{N}$.

We have seen this in action in the previous slide. We have the Abelian extension $\mathbb{Q}(\sqrt{p^*})$ of $\mathbb{Q}$. This is an Abelian extension since it has Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}$, which is an Abelian group. We then saw that this is contained inside the cyclotomic field $\mathbb{Q}(\zeta_p)$, which is predicted by the theorem above.

# Generalising this - The Kronecker-Weber theorem

In class field theory we study certain extensions of a number field $K$. Specifically we look at the ones with Abelian Galois group. Such an extension is called an Abelian extension.
The Kronecker-Weber theorem is a corollary of more general theorems in class field theory. It says that:

**Kronecker - Weber Theorem**

Each finite abelian extension $L$ of $\mathbb{Q}$ is contained inside a cyclotomic number field $\mathbb{Q}(\zeta_n)$ for some $n \in \mathbb{N}$.

We have seen this in action in the previous slide. We have the Abelian extension $\mathbb{Q}(\sqrt{p^*})$ of $\mathbb{Q}$. This is an Abelian extension since it has Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}$, which is an Abelian group. We then saw that this is contained inside the cyclotomic field $\mathbb{Q}(\zeta_p)$, which is predicted by the theorem above.

# That's all folks

The end.