Annihilators of the minus class group of an imaginary cyclic field

Pavel Francírek

Department of Mathematics and Statistics,
Faculty of Science, Masaryk University,
Brno

25 June 2018

Introduction

Introduction

Let L be an imaginary abelian field, so $G = \mathrm{Gal}\,(L/\mathbb{Q})$ is an abelian group.

Introduction

Let L be an imaginary abelian field, so $G = \mathrm{Gal}\,(L/\mathbb{Q})$ is an abelian group. Let ℓ be an odd prime.

Introduction

Let L be an imaginary abelian field, so $G = \mathrm{Gal}\,(L/\mathbb{Q})$ is an abelian group. Let ℓ be an odd prime. The ℓ-Sylow subgroup A_ℓ of the class group $\mathcal{C}\ell(L)$ of L forms a $\mathbb{Z}_\ell[G]$-module.

Introduction

Let L be an imaginary abelian field, so $G = \mathrm{Gal}\,(L/\mathbb{Q})$ is an abelian group. Let ℓ be an odd prime. The ℓ-Sylow subgroup A_ℓ of the class group $\mathcal{C}\ell(L)$ of L forms a $\mathbb{Z}_\ell[G]$-module. The elements

$$e^- = \frac{1-\tau}{2} \in \mathbb{Z}_\ell[G] \qquad \text{and} \qquad e^+ = \frac{1+\tau}{2} \in \mathbb{Z}_\ell[G],$$

where τ is the complex conjugation, form a full set of orthogonal idempotents.

Introduction

Let L be an imaginary abelian field, so $G = \mathrm{Gal}\,(L/\mathbb{Q})$ is an abelian group. Let ℓ be an odd prime. The ℓ-Sylow subgroup A_ℓ of the class group $\mathcal{C}\ell(L)$ of L forms a $\mathbb{Z}_\ell[G]$-module. The elements

$$e^- = \frac{1-\tau}{2} \in \mathbb{Z}_\ell[G] \qquad \text{and} \qquad e^+ = \frac{1+\tau}{2} \in \mathbb{Z}_\ell[G],$$

where τ is the complex conjugation, form a full set of orthogonal idempotents. This gives us the following decomposition

$$A_\ell = e^- A_\ell \oplus e^+ A_\ell.$$

The minus part $e^- A_\ell$ will be denoted by A_ℓ^-.

Introduction

Let L be an imaginary abelian field, so $G = \mathrm{Gal}\,(L/\mathbb{Q})$ is an abelian group. Let ℓ be an odd prime. The ℓ-Sylow subgroup A_ℓ of the class group $\mathcal{C}\ell(L)$ of L forms a $\mathbb{Z}_\ell[G]$-module. The elements

$$e^- = \frac{1-\tau}{2} \in \mathbb{Z}_\ell[G] \qquad \text{and} \qquad e^+ = \frac{1+\tau}{2} \in \mathbb{Z}_\ell[G],$$

where τ is the complex conjugation, form a full set of orthogonal idempotents. This gives us the following decomposition

$$A_\ell = e^- A_\ell \oplus e^+ A_\ell.$$

The minus part $e^- A_\ell$ will be denoted by A_ℓ^-.
Our goal is to find annihilators of A_ℓ^-, i.e. the elements $\xi \in \mathbb{Z}[G]$ (or $\mathbb{Z}_\ell[G]$) such that for any ideal $\mathfrak{a}$ representing arbitrary class of A_ℓ^- the ideal $\mathfrak{a}^\xi$ is principal.

Kummer, Stickelberger, Sinnott

How to produce an annihilator of A_ℓ^-?

Kummer, Stickelberger, Sinnott

How to produce an annihilator of A_ℓ^-? By factoring Gauss sums!

Kummer, Stickelberger, Sinnott

How to produce an annihilator of A_ℓ^-? By factoring Gauss sums!

Notation:

Kummer, Stickelberger, Sinnott

How to produce an annihilator of A_ℓ^-? By factoring Gauss sums!

Notation:
$\mathbb{Q}_n = \mathbb{Q}(\zeta_n) =$ the n-th cyclotomic field, $\zeta_n = e^{2\pi i/n}$

Kummer, Stickelberger, Sinnott

How to produce an annihilator of A_ℓ^-? By factoring Gauss sums!

Notation:
$\mathbb{Q}_n = \mathbb{Q}(\zeta_n) =$ the n-th cyclotomic field, $\zeta_n = e^{2\pi i/n}$
$\mathbb{Z}[\zeta_n] =$ the ring of algebraic integers of $\mathbb{Q}_n$

Kummer, Stickelberger, Sinnott

How to produce an annihilator of A_ℓ^-? By factoring Gauss sums!

Notation:
$\mathbb{Q}_n = \mathbb{Q}(\zeta_n) =$ the n-th cyclotomic field, $\zeta_n = e^{2\pi i/n}$
$\mathbb{Z}[\zeta_n] =$ the ring of algebraic integers of $\mathbb{Q}_n$
$\sigma_a =$ the automorphism of $\mathbb{Q}_n$ given by $\zeta_n \mapsto \zeta_n^a$ (for $(a, n) = 1$)

Kummer, Stickelberger, Sinnott

How to produce an annihilator of A_ℓ^-? By factoring Gauss sums!

Notation:
$\mathbb{Q}_n = \mathbb{Q}(\zeta_n) =$ the n-th cyclotomic field, $\zeta_n = e^{2\pi i/n}$
$\mathbb{Z}[\zeta_n] =$ the ring of algebraic integers of $\mathbb{Q}_n$
$\sigma_a =$ the automorphism of $\mathbb{Q}_n$ given by $\zeta_n \mapsto \zeta_n^a$ (for $(a, n) = 1$)
$p =$ an odd prime that splits completely in $\mathbb{Q}_n$

Kummer, Stickelberger, Sinnott

How to produce an annihilator of A_ℓ^-? By factoring Gauss sums!

Notation:
$\mathbb{Q}_n = \mathbb{Q}(\zeta_n) =$ the n-th cyclotomic field, $\zeta_n = e^{2\pi i/n}$
$\mathbb{Z}[\zeta_n] =$ the ring of algebraic integers of $\mathbb{Q}_n$
$\sigma_a =$ the automorphism of $\mathbb{Q}_n$ given by $\zeta_n \mapsto \zeta_n^a$ (for $(a, n) = 1$)
$p =$ an odd prime that splits completely in $\mathbb{Q}_n$
$\mathfrak{p} =$ some prime ideal of $\mathbb{Q}_n$ such that $\mathfrak{p} \mid p$

Kummer, Stickelberger, Sinnott

How to produce an annihilator of A_ℓ^-? By factoring Gauss sums!

Notation:
$\mathbb{Q}_n = \mathbb{Q}(\zeta_n) =$ the n-th cyclotomic field, $\zeta_n = e^{2\pi i/n}$
$\mathbb{Z}[\zeta_n] =$ the ring of algebraic integers of $\mathbb{Q}_n$
$\sigma_a =$ the automorphism of $\mathbb{Q}_n$ given by $\zeta_n \mapsto \zeta_n^a$ (for $(a, n) = 1$)
$p =$ an odd prime that splits completely in $\mathbb{Q}_n$
$\mathfrak{p} =$ some prime ideal of $\mathbb{Q}_n$ such that $\mathfrak{p} \mid p$

For any $a \in \mathbb{Z}[\zeta_n]$ such that $\mathfrak{p} \nmid a$ we define (n-th power residue symbol)

$$\omega(a \bmod \mathfrak{p}) \equiv a^{(p-1)/n} \pmod{\mathfrak{p}}.$$

Using this character we form a Gauss sum

$$g = -\sum_{t=1}^{p-1} \omega^{-1}(t)\zeta_p^t \in \mathbb{Q}_{np}.$$

Using this character we form a Gauss sum

$$g = -\sum_{t=1}^{p-1} \omega^{-1}(t)\zeta_p^t \in \mathbb{Q}_{np}.$$

It can be shown that $g^n \in \mathbb{Q}_n$ and since $|g|^2 = p$, g^n is supported only on conjugates of $\mathfrak{p}$.

Using this character we form a Gauss sum

$$g = -\sum_{t=1}^{p-1} \omega^{-1}(t)\zeta_p^t \in \mathbb{Q}_{np}.$$

It can be shown that $g^n \in \mathbb{Q}_n$ and since $|g|^2 = p$, g^n is supported only on conjugates of $\mathfrak{p}$. Factoring g^n we obtain

$$g^n \cdot \mathbb{Z}[\zeta_n] = \mathfrak{p}^{n\theta_n},$$

Using this character we form a Gauss sum

$$g = -\sum_{t=1}^{p-1} \omega^{-1}(t)\zeta_p^t \in \mathbb{Q}_{np}.$$

It can be shown that $g^n \in \mathbb{Q}_n$ and since $|g|^2 = p$, g^n is supported only on conjugates of $\mathfrak{p}$. Factoring g^n we obtain

$$g^n \cdot \mathbb{Z}[\zeta_n] = \mathfrak{p}^{n\theta_n},$$

where

$$\theta_n = \sum_{\substack{1 \le a < n \\ (a,n)=1}} \frac{a}{n} \cdot \sigma_a^{-1} \in \mathbb{Q}[\mathrm{Gal}\,(\mathbb{Q}_n/\mathbb{Q})],$$

which does not depend on p!

Using this character we form a Gauss sum

$$g = -\sum_{t=1}^{p-1} \omega^{-1}(t)\zeta_p^t \in \mathbb{Q}_{np}.$$

It can be shown that $g^n \in \mathbb{Q}_n$ and since $|g|^2 = p$, g^n is supported only on conjugates of $\mathfrak{p}$. Factoring g^n we obtain

$$g^n \cdot \mathbb{Z}[\zeta_n] = \mathfrak{p}^{n\theta_n},$$

where

$$\theta_n = \sum_{\substack{1 \le a < n \\ (a,n)=1}} \frac{a}{n} \cdot \sigma_a^{-1} \in \mathbb{Q}[\mathrm{Gal}\,(\mathbb{Q}_n/\mathbb{Q})],$$

which does not depend on p! Since each ideal class contains such an ideal $\mathfrak{p}$, it follows that

$$(\theta_n \cdot \mathbb{Z}[\mathrm{Gal}\,(\mathbb{Q}_n/\mathbb{Q})]) \cap \mathbb{Z}[\mathrm{Gal}\,(\mathbb{Q}_n/\mathbb{Q})]$$

annihilates the ideal class group of $\mathbb{Q}_n$.

How to get some more annihilators?

How to get some more annihilators? Using restriction and correstriction.

How to get some more annihilators? Using restriction and correstriction.

Notation:

$L =$ an imaginary abelian field, $G = \mathrm{Gal}\,(L/\mathbb{Q})$

How to get some more annihilators? Using restriction and correstriction.

Notation:

$L =$ an imaginary abelian field, $G = \mathrm{Gal}\,(L/\mathbb{Q})$

$M =$ a subfield of L, $H = \mathrm{Gal}\,(L/M)$

How to get some more annihilators? Using restriction and correstriction.

Notation:
$L =$ an imaginary abelian field, $G = \mathrm{Gal}\,(L/\mathbb{Q})$
$M =$ a subfield of L, $H = \mathrm{Gal}\,(L/M)$

The natural projection $G \to G/H$ induces a ring homomorphism

$$\mathrm{res}_{L/M} \colon \mathbb{Q}[G] \to \mathbb{Q}[G/H].$$

How to get some more annihilators? Using restriction and correstriction.

Notation:
$L =$ an imaginary abelian field, $G = \mathrm{Gal}\,(L/\mathbb{Q})$
$M =$ a subfield of L, $H = \mathrm{Gal}\,(L/M)$

The natural projection $G \to G/H$ induces a ring homomorphism

$$\mathrm{res}_{L/M} \colon \mathbb{Q}[G] \to \mathbb{Q}[G/H].$$

We also have a $\mathbb{Z}[G]$-module homomorphism

$$\mathrm{cor}_{L/M} \colon \mathbb{Q}[G/H] \to \mathbb{Q}[G],$$

How to get some more annihilators? Using restriction and correstriction.

Notation:
$L =$ an imaginary abelian field, $G = \mathrm{Gal}\,(L/\mathbb{Q})$
$M =$ a subfield of L, $H = \mathrm{Gal}\,(L/M)$

The natural projection $G \to G/H$ induces a ring homomorphism

$$\mathrm{res}_{L/M} \colon \mathbb{Q}[G] \to \mathbb{Q}[G/H].$$

We also have a $\mathbb{Z}[G]$-module homomorphism

$$\mathrm{cor}_{L/M} \colon \mathbb{Q}[G/H] \to \mathbb{Q}[G],$$

which is given by $\mathrm{cor}_{L/M}(\sigma) = \sum_{\tau|_M=\sigma} \tau$.

How to get some more annihilators? Using restriction and correstriction.

Notation:
$L =$ an imaginary abelian field, $G = \mathrm{Gal}\,(L/\mathbb{Q})$
$M =$ a subfield of L, $H = \mathrm{Gal}\,(L/M)$

The natural projection $G \to G/H$ induces a ring homomorphism

$$\mathrm{res}_{L/M} \colon \mathbb{Q}[G] \to \mathbb{Q}[G/H].$$

We also have a $\mathbb{Z}[G]$-module homomorphism

$$\mathrm{cor}_{L/M} \colon \mathbb{Q}[G/H] \to \mathbb{Q}[G],$$

which is given by $\mathrm{cor}_{L/M}(\sigma) = \sum_{\tau|_M=\sigma} \tau$.
We set $\theta'_n = \mathrm{cor}_{L/L\cap\mathbb{Q}_n} \mathrm{res}_{\mathbb{Q}_n/L\cap\mathbb{Q}_n} \theta_n$.

How to get some more annihilators? Using restriction and correstriction.

Notation:
$L =$ an imaginary abelian field, $G = \mathrm{Gal}\,(L/\mathbb{Q})$
$M =$ a subfield of L, $H = \mathrm{Gal}\,(L/M)$

The natural projection $G \to G/H$ induces a ring homomorphism

$$\mathrm{res}_{L/M} \colon \mathbb{Q}[G] \to \mathbb{Q}[G/H].$$

We also have a $\mathbb{Z}[G]$-module homomorphism

$$\mathrm{cor}_{L/M} \colon \mathbb{Q}[G/H] \to \mathbb{Q}[G],$$

which is given by $\mathrm{cor}_{L/M}(\sigma) = \sum_{\tau|_M=\sigma} \tau$.
We set $\theta'_n = \mathrm{cor}_{L/L\cap\mathbb{Q}_n}\mathrm{res}_{\mathbb{Q}_n/L\cap\mathbb{Q}_n}\theta_n$. Let S' be the $\mathbb{Z}[G]$-module in $\mathbb{Q}[G]$ generated by the elements θ'_n for all $n \geq 1$.

How to get some more annihilators? Using restriction and correstriction.

Notation:
$L =$ an imaginary abelian field, $G = \mathrm{Gal}\,(L/\mathbb{Q})$
$M =$ a subfield of L, $H = \mathrm{Gal}\,(L/M)$

The natural projection $G \to G/H$ induces a ring homomorphism

$$\mathrm{res}_{L/M} \colon \mathbb{Q}[G] \to \mathbb{Q}[G/H].$$

We also have a $\mathbb{Z}[G]$-module homomorphism

$$\mathrm{cor}_{L/M} \colon \mathbb{Q}[G/H] \to \mathbb{Q}[G],$$

which is given by $\mathrm{cor}_{L/M}(\sigma) = \sum_{\tau|_M=\sigma} \tau$.
We set $\theta'_n = \mathrm{cor}_{L/L\cap\mathbb{Q}_n}\mathrm{res}_{\mathbb{Q}_n/L\cap\mathbb{Q}_n}\theta_n$. Let S' be the $\mathbb{Z}[G]$-module in $\mathbb{Q}[G]$ generated by the elements θ'_n for all $n \geq 1$. Then $S = S' \cap \mathbb{Z}[G]$ is the *Stickelberger ideal* of L (in the sense of Sinnott).

How to get some more annihilators? Using restriction and correstriction.

Notation:
$L =$ an imaginary abelian field, $G = \mathrm{Gal}\,(L/\mathbb{Q})$
$M =$ a subfield of L, $H = \mathrm{Gal}\,(L/M)$

The natural projection $G \to G/H$ induces a ring homomorphism

$$\mathrm{res}_{L/M} \colon \mathbb{Q}[G] \to \mathbb{Q}[G/H].$$

We also have a $\mathbb{Z}[G]$-module homomorphism

$$\mathrm{cor}_{L/M} \colon \mathbb{Q}[G/H] \to \mathbb{Q}[G],$$

which is given by $\mathrm{cor}_{L/M}(\sigma) = \sum_{\tau|_M=\sigma} \tau$.
We set $\theta'_n = \mathrm{cor}_{L/L\cap\mathbb{Q}_n}\mathrm{res}_{\mathbb{Q}_n/L\cap\mathbb{Q}_n}\theta_n$. Let S' be the $\mathbb{Z}[G]$-module in $\mathbb{Q}[G]$ generated by the elements θ'_n for all $n \geq 1$. Then $S = S' \cap \mathbb{Z}[G]$ is the *Stickelberger ideal* of L (in the sense of Sinnott). Sinnott proved that it annihilates $\mathcal{C}\ell(L)$.

Problem: Can we obtain still more annihilators in a systematic way?

Problem: Can we obtain still more annihilators in a systematic way? Yes, we can do so under certain asumptions on L:

Problem: Can we obtain still more annihilators in a systematic way? Yes, we can do so under certain asumptions on L:

- L is cyclic, i.e. $G = \mathrm{Gal}\,(L/\mathbb{Q}) = \langle \gamma \rangle$,

Problem: Can we obtain still more annihilators in a systematic way? Yes, we can do so under certain asumptions on L:

- L is cyclic, i.e. $G = \mathrm{Gal}\,(L/\mathbb{Q}) = \langle \gamma \rangle$,
- ℓ is an odd prime dividing the degree $[L\colon \mathbb{Q}]$.

Problem: Can we obtain still more annihilators in a systematic way? Yes, we can do so under certain asumptions on L:

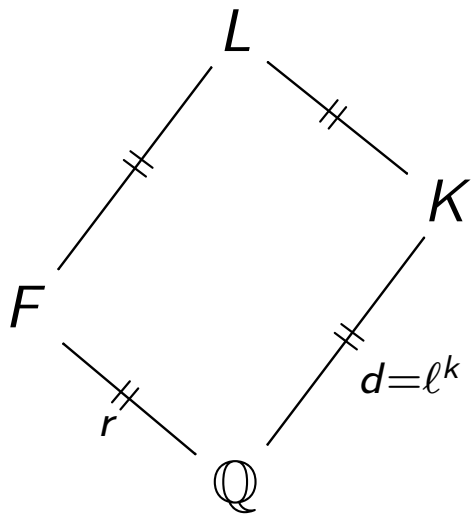
- L is cyclic, i.e. $G = \mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$,
- ℓ is an odd prime dividing the degree $[L\colon \mathbb{Q}]$.

It follows, that L is the compositum of a real cyclic field K of ℓ-power degree and an imaginary cyclic field F, $\ell \nmid [F\colon \mathbb{Q}]$.

Problem: Can we obtain still more annihilators in a systematic way? Yes, we can do so under certain asumptions on L:

- L is cyclic, i.e. $G = \mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$,
- ℓ is an odd prime dividing the degree $[L\colon \mathbb{Q}]$.

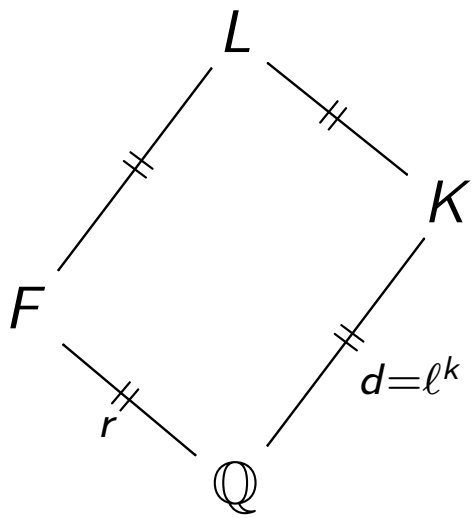
It follows, that L is the compositum of a real cyclic field K of ℓ-power degree and an imaginary cyclic field F, $\ell \nmid [F\colon \mathbb{Q}]$.



Problem: Can we obtain still more annihilators in a systematic way? Yes, we can do so under certain asumptions on L:

- L is cyclic, i.e. $G = \mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$,
- ℓ is an odd prime dividing the degree $[L\colon \mathbb{Q}]$.

It follows, that L is the compositum of a real cyclic field K of ℓ-power degree and an imaginary cyclic field F, $\ell \nmid [F\colon \mathbb{Q}]$.

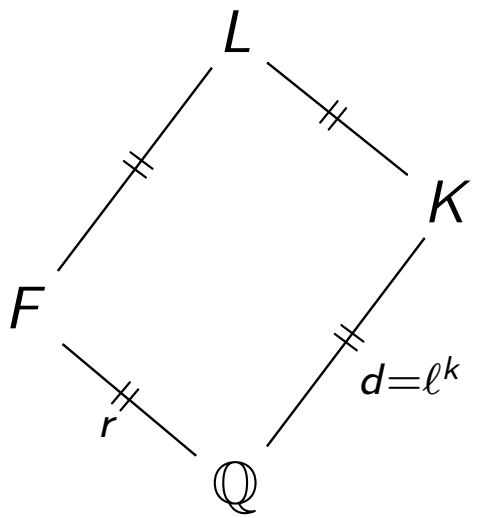


Let us denote f and m the conductors of F and K, respectively.

Problem: Can we obtain still more annihilators in a systematic way? Yes, we can do so under certain asumptions on L:

- L is cyclic, i.e. $G = \mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$,
- ℓ is an odd prime dividing the degree $[L\colon \mathbb{Q}]$.

It follows, that L is the compositum of a real cyclic field K of ℓ-power degree and an imaginary cyclic field F, $\ell \nmid [F\colon \mathbb{Q}]$.



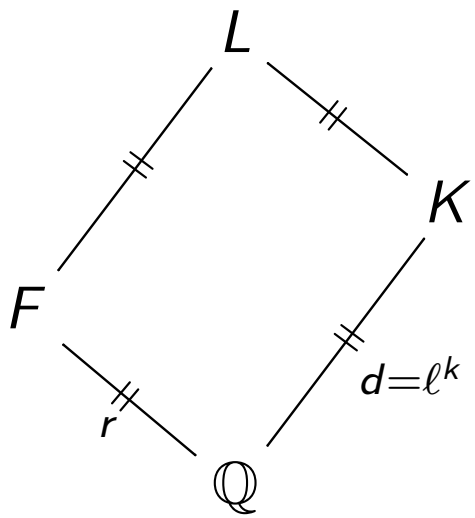
Let us denote f and m the conductors of F and K, respectively. We further assume

- ℓ does not ramify in L (so $\ell \nmid fm$),

Problem: Can we obtain still more annihilators in a systematic way? Yes, we can do so under certain asumptions on L:

- L is cyclic, i.e. $G = \mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$,
- ℓ is an odd prime dividing the degree $[L\colon \mathbb{Q}]$.

It follows, that L is the compositum of a real cyclic field K of ℓ-power degree and an imaginary cyclic field F, $\ell \nmid [F\colon \mathbb{Q}]$.



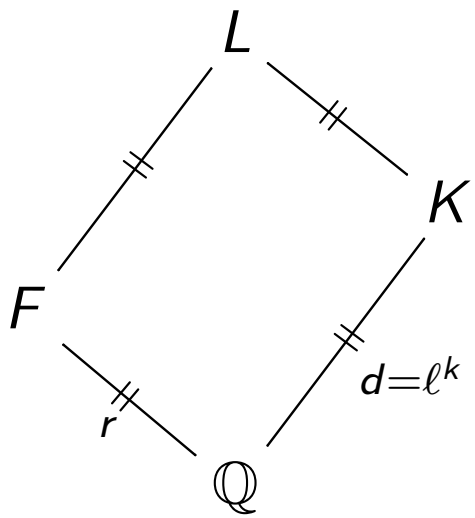
Let us denote f and m the conductors of F and K, respectively. We further assume

- ℓ does not ramify in L (so $\ell \nmid fm$),
- $\gcd(m, f) = 1$ (so fm is the conductor of L).

Problem: Can we obtain still more annihilators in a systematic way? Yes, we can do so under certain asumptions on L:

- L is cyclic, i.e. $G = \mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$,
- ℓ is an odd prime dividing the degree $[L\colon \mathbb{Q}]$.

It follows, that L is the compositum of a real cyclic field K of ℓ-power degree and an imaginary cyclic field F, $\ell \nmid [F\colon \mathbb{Q}]$.



Let us denote f and m the conductors of F and K, respectively. We further assume

- ℓ does not ramify in L (so $\ell \nmid fm$),
- $\gcd(m, f) = 1$ (so fm is the conductor of L).

Root extraction of a Gauss sum

Root extraction of a Gauss sum

The conductor m is a product of distinct prime numbers $p_1, p_2, \ldots, p_t$.

Root extraction of a Gauss sum

The conductor m is a product of distinct prime numbers $p_1, p_2, \ldots, p_t$.
$I = \{1, 2, \ldots, t\}$

Root extraction of a Gauss sum

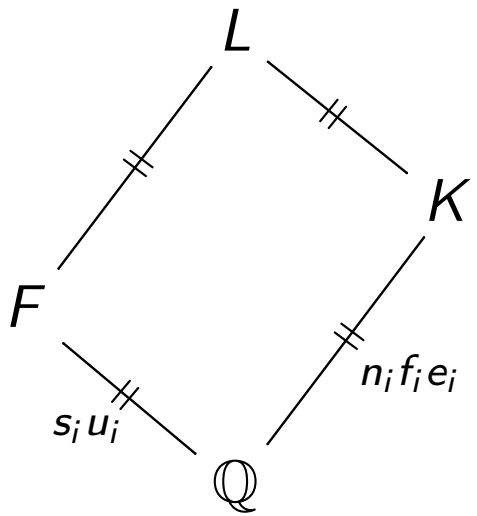
The conductor m is a product of distinct prime numbers $p_1, p_2, \ldots, p_t$.
$I = \{1, 2, \ldots, t\}$
e_i = the ramification index of p_i in K
f_i = the degree of inertia of p_i in K
n_i = number of distinct prime ideals of K dividing p_i

Root extraction of a Gauss sum

The conductor m is a product of distinct prime numbers $p_1, p_2, \ldots, p_t$.
$I = \{1, 2, \ldots, t\}$
e_i = the ramification index of p_i in K
f_i = the degree of inertia of p_i in K
n_i = number of distinct prime ideals of K dividing p_i
s_i = the degree of inertia of p_i in F
u_i = number of distinct prime ideals of F dividing p_i

Root extraction of a Gauss sum

The conductor m is a product of distinct prime numbers $p_1, p_2, \ldots, p_t$.
$I = \{1, 2, \ldots, t\}$
e_i = the ramification index of p_i in K
f_i = the degree of inertia of p_i in K
n_i = number of distinct prime ideals of K dividing p_i
s_i = the degree of inertia of p_i in F
u_i = number of distinct prime ideals of F dividing p_i
For each $i \in I$ we have



For each $i \in I$ we set

$$h_i(X) = X^{n_i u_i} - 1$$

For each $i \in I$ we set

$$h_i(X) = X^{n_i u_i} - 1$$

and for $i = t + 1$ we set

$$h_{t+1}(X) = X - 1.$$

For each $i \in I$ we set

$$h_i(X) = X^{n_i u_i} - 1$$

and for $i = t + 1$ we set

$$h_{t+1}(X) = X - 1.$$

Now define $h(X) \in \mathbb{Z}[X]$ as the least common multiple of polynomials h_i.

For each $i \in I$ we set

$$h_i(X) = X^{n_i u_i} - 1$$

and for $i = t + 1$ we set

$$h_{t+1}(X) = X - 1.$$

Now define $h(X) \in \mathbb{Z}[X]$ as the least common multiple of polynomials h_i. We fix an odd prime p that splits completely in $\mathbb{Q}_{fm}$, together with a prime ideal $\mathfrak{p}|p$.

For each $i \in I$ we set

$$h_i(X) = X^{n_i u_i} - 1$$

and for $i = t + 1$ we set

$$h_{t+1}(X) = X - 1.$$

Now define $h(X) \in \mathbb{Z}[X]$ as the least common multiple of polynomials h_i. We fix an odd prime p that splits completely in $\mathbb{Q}_{fm}$, together with a prime ideal $\mathfrak{p}|p$. Let g be the Gauss sum given by p and $\mathbb{Q}_{fm}$.

For each $i \in I$ we set

$$h_i(X) = X^{n_i u_i} - 1$$

and for $i = t + 1$ we set

$$h_{t+1}(X) = X - 1.$$

Now define $h(X) \in \mathbb{Z}[X]$ as the least common multiple of polynomials h_i. We fix an odd prime p that splits completely in $\mathbb{Q}_{fm}$, together with a prime ideal $\mathfrak{p}|p$. Let g be the Gauss sum given by p and $\mathbb{Q}_{fm}$.

Proposition

Let $\delta = H(\gamma)$, where

$$H(X) = \frac{\prod_{i=1}^{t+1} h_i(X)}{h(X)}.$$

Then there is $\beta \in L$ such that $\mathrm{N}_{\mathbb{Q}_{fm}/L}\left(g^{fm(1-\tau)}\right)^{2f} = \beta^{\delta}$.

The element β from the previous proposition is supported only on conjugates of $\mathfrak{p}$.

The element β from the previous proposition is supported only on conjugates of $\mathfrak{p}$. Therefore there is $\xi_L \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\beta \cdot \mathcal{O}_L = \mathfrak{p}^{\xi_L}.$$

The element β from the previous proposition is supported only on conjugates of $\mathfrak{p}$. Therefore there is $\xi_L \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\beta \cdot \mathcal{O}_L = \mathfrak{p}^{\xi_L}.$$

On the other hand we have

$$\mathrm{N}_{\mathbb{Q}_{fm}/L}\left(g^{fm(1-\tau)}\right)^{2f} \cdot \mathcal{O}_L = \mathfrak{p}^{\varkappa_L},$$

The element β from the previous proposition is supported only on conjugates of $\mathfrak{p}$. Therefore there is $\xi_L \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\beta \cdot \mathcal{O}_L = \mathfrak{p}^{\xi_L}.$$

On the other hand we have

$$\mathrm{N}_{\mathbb{Q}_{fm}/L}\left(g^{fm(1-\tau)}\right)^{2f} \cdot \mathcal{O}_L = \mathfrak{p}^{\varkappa_L},$$

where

$$\varkappa_L = 2f^2 m \cdot (1 - \gamma^{r\ell^k/2}) \cdot \mathrm{res}_{\mathbb{Q}_{fm}/L}\theta_{fm} \in \mathbb{Z}[\langle\gamma\rangle].$$

The element β from the previous proposition is supported only on conjugates of $\mathfrak{p}$. Therefore there is $\xi_L \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\beta \cdot \mathcal{O}_L = \mathfrak{p}^{\xi_L}.$$

On the other hand we have

$$\mathrm{N}_{\mathbb{Q}_{fm}/L}\left(g^{fm(1-\tau)}\right)^{2f} \cdot \mathcal{O}_L = \mathfrak{p}^{\varkappa_L},$$

where

$$\varkappa_L = 2f^2 m \cdot (1-\gamma^{r\ell^k/2}) \cdot \mathrm{res}_{\mathbb{Q}_{fm}/L}\theta_{fm} \in \mathbb{Z}[\langle\gamma\rangle].$$

Comparing exponents on both sides of $\mathrm{N}_{\mathbb{Q}_{fm}/L}\left(g^{fm(1-\tau)}\right)^{2f} = \beta^{\delta}$ gives

$$\varkappa_L = \xi_L \cdot \delta.$$

The element β from the previous proposition is supported only on conjugates of $\mathfrak{p}$. Therefore there is $\xi_L \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\beta \cdot \mathcal{O}_L = \mathfrak{p}^{\xi_L}.$$

On the other hand we have

$$\mathrm{N}_{\mathbb{Q}_{fm}/L}\left(g^{fm(1-\tau)}\right)^{2f} \cdot \mathcal{O}_L = \mathfrak{p}^{\varkappa_L},$$

where

$$\varkappa_L = 2f^2 m \cdot (1 - \gamma^{r\ell^k/2}) \cdot \mathrm{res}_{\mathbb{Q}_{fm}/L}\theta_{fm} \in \mathbb{Z}[\langle\gamma\rangle].$$

Comparing exponents on both sides of $\mathrm{N}_{\mathbb{Q}_{fm}/L}\left(g^{fm(1-\tau)}\right)^{2f} = \beta^{\delta}$ gives

$$\varkappa_L = \xi_L \cdot \delta.$$

The polynomial $H(X)$ can be written uniquely in the form

$$\prod_{j|rd} \Phi_j(X)^{a_j}$$

for suitable nonnegative integers a_j.

The element β from the previous proposition is supported only on conjugates of $\mathfrak{p}$. Therefore there is $\xi_L \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\beta \cdot \mathcal{O}_L = \mathfrak{p}^{\xi_L}.$$

On the other hand we have

$$\mathrm{N}_{\mathbb{Q}_{fm}/L}\left(g^{fm(1-\tau)}\right)^{2f} \cdot \mathcal{O}_L = \mathfrak{p}^{\varkappa_L},$$

where

$$\varkappa_L = 2f^2 m \cdot (1 - \gamma^{r\ell^k/2}) \cdot \mathrm{res}_{\mathbb{Q}_{fm}/L}\theta_{fm} \in \mathbb{Z}[\langle\gamma\rangle].$$

Comparing exponents on both sides of $\mathrm{N}_{\mathbb{Q}_{fm}/L}\left(g^{fm(1-\tau)}\right)^{2f} = \beta^{\delta}$ gives

$$\varkappa_L = \xi_L \cdot \delta.$$

The polynomial $H(X)$ can be written uniquely in the form

$$\prod_{j|rd} \Phi_j(X)^{a_j}$$

for suitable nonnegative integers a_j.

Therefore we have

$$\delta = \prod_{j|rd} \Phi_j(\gamma)^{a_j}.$$

Therefore we have

$$\delta = \prod_{j|rd} \Phi_j(\gamma)^{a_j}.$$

For each positive divisor j of rd let

$$\Delta_j = \sum_{i=1}^{(rd/j)-1} i\gamma^{ij}.$$

Therefore we have

$$\delta = \prod_{j|rd} \Phi_j(\gamma)^{a_j}.$$

For each positive divisor j of rd let

$$\Delta_j = \sum_{i=1}^{(rd/j)-1} i\gamma^{ij}.$$

Lemma

The element ξ_L is determined uniquely, in fact

$$\xi_L = \prod_{j|rd} \Big(\frac{j}{rd} \Delta_j \prod_{\substack{i|j \\ i \neq j}} \Phi_i(\gamma) \Big)^{a_j} \varkappa_L.$$

Therefore we have

$$\delta = \prod_{j|rd} \Phi_j(\gamma)^{a_j}.$$

For each positive divisor j of rd let

$$\Delta_j = \sum_{i=1}^{(rd/j)-1} i\gamma^{ij}.$$

Lemma

The element ξ_L is determined uniquely, in fact

$$\xi_L = \prod_{j|rd} \Big(\frac{j}{rd} \Delta_j \prod_{\substack{i|j \\ i \neq j}} \Phi_i(\gamma) \Big)^{a_j} \varkappa_L.$$

Theorem

The element $\xi_L \in \mathbb{Z}[\langle\gamma\rangle]$ is an annihilator of A_ℓ^-.

Let $\mathcal{L}$ be a poset consisting of the subfields M of L which are imaginary and satisfy $M = \mathbb{Q}_n \cap L$ for suitable positive integer n.

Let $\mathcal{L}$ be a poset consisting of the subfields M of L which are imaginary and satisfy $M = \mathbb{Q}_n \cap L$ for suitable positive integer n.

$\mathcal{I} =$ an ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by $\mathrm{cor}_{L/M} \varkappa_M$ for all $M \in \mathcal{L}$

Let $\mathcal{L}$ be a poset consisting of the subfields M of L which are imaginary and satisfy $M = \mathbb{Q}_n \cap L$ for suitable positive integer n.

$\mathcal{I} =$ an ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by $\mathrm{cor}_{L/M}\varkappa_M$ for all $M \in \mathcal{L}$
$\mathcal{J} =$ an ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by $\mathrm{cor}_{L/M}\xi_M$ for all $M \in \mathcal{L}$

Let $\mathcal{L}$ be a poset consisting of the subfields M of L which are imaginary and satisfy $M = \mathbb{Q}_n \cap L$ for suitable positive integer n.

$\mathcal{I}$ = an ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by $\mathrm{cor}_{L/M}\varkappa_M$ for all $M \in \mathcal{L}$
$\mathcal{J}$ = an ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by $\mathrm{cor}_{L/M}\xi_M$ for all $M \in \mathcal{L}$
S_L = Sinnott's Stickelberger ideal for L

Let $\mathcal{L}$ be a poset consisting of the subfields M of L which are imaginary and satisfy $M = \mathbb{Q}_n \cap L$ for suitable positive integer n.

$\mathcal{I} =$ an ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by $\mathrm{cor}_{L/M}\varkappa_M$ for all $M \in \mathcal{L}$
$\mathcal{J} =$ an ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by $\mathrm{cor}_{L/M}\xi_M$ for all $M \in \mathcal{L}$
$S_L =$ Sinnott's Stickelberger ideal for L

Since $\ell \nmid fm$ we have

$$\mathcal{I} \cdot \mathbb{Z}_\ell[\langle\gamma\rangle] = e^- S_L \cdot \mathbb{Z}_\ell[\langle\gamma\rangle].$$

Let $\mathcal{L}$ be a poset consisting of the subfields M of L which are imaginary and satisfy $M = \mathbb{Q}_n \cap L$ for suitable positive integer n.

$\mathcal{I}$ = an ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by $\mathrm{cor}_{L/M}\varkappa_M$ for all $M \in \mathcal{L}$
$\mathcal{J}$ = an ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by $\mathrm{cor}_{L/M}\xi_M$ for all $M \in \mathcal{L}$
S_L = Sinnott's Stickelberger ideal for L

Since $\ell \nmid fm$ we have

$$\mathcal{I} \cdot \mathbb{Z}_\ell[\langle\gamma\rangle] = e^- S_L \cdot \mathbb{Z}_\ell[\langle\gamma\rangle].$$

Therefore if $\ell \mid [\mathcal{J} : \mathcal{I}]$, then $\mathcal{J}$ contains annihilators not belonging to S_L.

Let $\mathcal{L}$ be a poset consisting of the subfields M of L which are imaginary and satisfy $M = \mathbb{Q}_n \cap L$ for suitable positive integer n.

$\mathcal{I}$ = an ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by $\mathrm{cor}_{L/M}\varkappa_M$ for all $M \in \mathcal{L}$
$\mathcal{J}$ = an ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by $\mathrm{cor}_{L/M}\xi_M$ for all $M \in \mathcal{L}$
S_L = Sinnott's Stickelberger ideal for L

Since $\ell \nmid fm$ we have

$$\mathcal{I} \cdot \mathbb{Z}_\ell[\langle\gamma\rangle] = e^- S_L \cdot \mathbb{Z}_\ell[\langle\gamma\rangle].$$

Therefore if $\ell \mid [\mathcal{J} : \mathcal{I}]$, then $\mathcal{J}$ contains annihilators not belonging to S_L.

Moreover $\mathrm{ord}_\ell\big([\mathcal{J} : \mathcal{I}]\big)$ divides the relative class number of L.

Computing the index $[\mathcal{J} : \mathcal{I}]$

Computing the index $[\mathcal{J} : \mathcal{I}]$

Special case: Suppose that $[F : \mathbb{Q}] = 2^u$, $u \in \mathbb{N}$.

Computing the index $[\mathcal{J} : \mathcal{I}]$

Special case: Suppose that $[F : \mathbb{Q}] = 2^u$, $u \in \mathbb{N}$. For each $i = 0, 1, \ldots k$ let L_i be the unique subfield of L of degree $[L_i : \mathbb{Q}] = 2^u \ell^i$.

Computing the index $[\mathcal{J} : \mathcal{I}]$

Special case: Suppose that $[F : \mathbb{Q}] = 2^u$, $u \in \mathbb{N}$. For each $i = 0, 1, \ldots k$ let L_i be the unique subfield of L of degree $[L_i : \mathbb{Q}] = 2^u \ell^i$. The poset $\mathcal{L}$ is the following string

$$F = L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_k = L.$$

Computing the index $[\mathcal{J} : \mathcal{I}]$

Special case: Suppose that $[F : \mathbb{Q}] = 2^u$, $u \in \mathbb{N}$. For each $i = 0, 1, \ldots k$ let L_i be the unique subfield of L of degree $[L_i : \mathbb{Q}] = 2^u \ell^i$. The poset $\mathcal{L}$ is the following string

$$F = L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_k = L.$$

Let s_i be the number of ramified primes in L_i that split completely in F.

Computing the index $[\mathcal{J} : \mathcal{I}]$

Special case: Suppose that $[F : \mathbb{Q}] = 2^u$, $u \in \mathbb{N}$. For each $i = 0, 1, \ldots k$ let L_i be the unique subfield of L of degree $[L_i : \mathbb{Q}] = 2^u \ell^i$. The poset $\mathcal{L}$ is the following string

$$F = L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_k = L.$$

Let s_i be the number of ramified primes in L_i that split completely in F.

Theorem

The index $[\mathcal{J} : \mathcal{I}]$ is given by

$$[\mathcal{J} : \mathcal{I}] = \prod_{i=0}^{k} \prod_{j=0}^{i-1} \ell^{2^{u-1} \cdot \varphi(\ell^j) \cdot c_i},$$

where $c_i = \max\{s_i - 1, 0\}$.

Computing the index $[\mathcal{J} : \mathcal{I}]$

Special case: Suppose that $[F : \mathbb{Q}] = 2^u$, $u \in \mathbb{N}$. For each $i = 0, 1, \ldots k$ let L_i be the unique subfield of L of degree $[L_i : \mathbb{Q}] = 2^u \ell^i$. The poset $\mathcal{L}$ is the following string

$$F = L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_k = L.$$

Let s_i be the number of ramified primes in L_i that split completely in F.

Theorem

The index $[\mathcal{J} : \mathcal{I}]$ is given by

$$[\mathcal{J} : \mathcal{I}] = \prod_{i=0}^{k} \prod_{j=0}^{i-1} \ell^{2^{u-1} \cdot \varphi(\ell^j) \cdot c_i},$$

where $c_i = \max\{s_i - 1, 0\}$.

Remark: If $s_k \geq 2$, then our new (explicitly computed) annihilators lie outside of the Stickelberger ideal S_L!

Example

We set $F = \mathbb{Q}(i) = \mathbb{Q}_4$.

Example

We set $F = \mathbb{Q}(i) = \mathbb{Q}_4$. We further set K to be the field belonging to $\chi_1\chi_2$, where χ_1 and χ_2 are characters of order 3 of conductor 13 and 37, respectively.

Example

We set $F = \mathbb{Q}(i) = \mathbb{Q}_4$. We further set K to be the field belonging to $\chi_1\chi_2$, where χ_1 and χ_2 are characters of order 3 of conductor 13 and 37, respectively. Let L be the compositum of F and K, $\mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$.

Example

We set $F = \mathbb{Q}(i) = \mathbb{Q}_4$. We further set K to be the field belonging to $\chi_1\chi_2$, where χ_1 and χ_2 are characters of order 3 of conductor 13 and 37, respectively. Let L be the compositum of F and K, $\mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$. We can compute that

$$(1-\gamma^3)\mathrm{res}_{\mathbb{Q}_{1924}/L}\theta_{1924} = 6\gamma^5 - 6\gamma^3 - 6\gamma^2 + 6,$$

Example

We set $F = \mathbb{Q}(i) = \mathbb{Q}_4$. We further set K to be the field belonging to $\chi_1\chi_2$, where χ_1 and χ_2 are characters of order 3 of conductor 13 and 37, respectively. Let L be the compositum of F and K, $\mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$. We can compute that

$$(1-\gamma^3)\mathrm{res}_{\mathbb{Q}_{1924}/L}\theta_{1924} = 6\gamma^5 - 6\gamma^3 - 6\gamma^2 + 6,$$

therefore

$$\varkappa_L = 2^6 \cdot 3 \cdot 13 \cdot 37 \cdot (\gamma^5 - \gamma^3 - \gamma^2 + 1).$$

Example

We set $F = \mathbb{Q}(i) = \mathbb{Q}_4$. We further set K to be the field belonging to $\chi_1\chi_2$, where χ_1 and χ_2 are characters of order 3 of conductor 13 and 37, respectively. Let L be the compositum of F and K, $\mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$. We can compute that

$$(1-\gamma^3)\mathrm{res}_{\mathbb{Q}_{1924}/L}\theta_{1924} = 6\gamma^5 - 6\gamma^3 - 6\gamma^2 + 6,$$

therefore

$$\varkappa_L = 2^6 \cdot 3 \cdot 13 \cdot 37 \cdot (\gamma^5 - \gamma^3 - \gamma^2 + 1).$$

Since both 13 and 37 split completely in F, we have

$$H(X) = \frac{(X^2-1)^2(X-1)}{(X^2-1)} = (X^2-1)(X-1) = \Phi_1(X)^2\Phi_2(X).$$

Therefore we just need to compute Δ_1 and Δ_2:

Therefore we just need to compute Δ_1 and Δ_2:

$$\Delta_1 = \sum_{i=1}^{5} = i\gamma^i = \gamma + 2\gamma^2 + 3\gamma^3 + 4\gamma^4 + 5\gamma^5$$

$$\Delta_2 = \gamma^2 + 2\gamma^4.$$

Therefore we just need to compute Δ_1 and Δ_2:

$$\Delta_1 = \sum_{i=1}^{5} = i\gamma^i = \gamma + 2\gamma^2 + 3\gamma^3 + 4\gamma^4 + 5\gamma^5$$

$$\Delta_2 = \gamma^2 + 2\gamma^4.$$

Then we have

$$\begin{aligned}\xi_L &= \left(\frac{1}{6}\Delta_1\right)^2 \cdot \left(\frac{1}{3}\Delta_2(\gamma - 1)\right) \varkappa_L \\ &= 2^6 \cdot 13 \cdot 37 \cdot (-\gamma^5 - 2\gamma^4 - \gamma^3 + \gamma^2 + 2\gamma + 1).\end{aligned}$$

Thank you for your attention!