How quaternion algebras shape the structure of square power classes over biquadratic extensions

Andrew Schultz

May 29, 2023

Wellesley College

In collaboration with...

John Swallow

Frank Chemotti

Ján Mináč

Tung T. Nguyen

Nguyen Duy Tan

The next 25 minutes of your life

Here's what we'll be doing

- Introduce a Galois module of interest
- Review what is known about it
- Reinterpret module-theoretic info arithmetically
- Compute some examples

Motivation and Background

Big picture goal

Problem under consideration

If K/F is a biquadratic extension and $\mathrm{char}(F) \neq 2$, decompose $K^\times/K^{\times 2}$ as module over $\mathbb{F}_2[\mathrm{Gal}(K/F)]$.

Big picture goal

Problem under consideration

If K/F is a biquadratic extension and $\mathrm{char}(F) \neq 2$, decompose $K^\times/K^{\times 2}$ as module over $\mathbb{F}_2[\mathrm{Gal}(K/F)]$.

Why should we care?

Big picture goal

Problem under consideration

If K/F is a biquadratic extension and $\mathrm{char}(F) \neq 2$, decompose $K^\times/K^{\times 2}$ as module over $\mathbb{F}_2[\mathrm{Gal}(K/F)]$.

Why should we care?

If decomposition is "special" for any K/F, this means absolute Galois groups are "special" too

Big picture goal

Problem under consideration

If K/F is a biquadratic extension and $\text{char}(F) \neq 2$, decompose $K^\times/K^{\times 2}$ as module over $\mathbb{F}_2[\text{Gal}(K/F)]$.

Why should we care?

If decomposition is "special" for any K/F, this means absolute Galois groups are "special" too

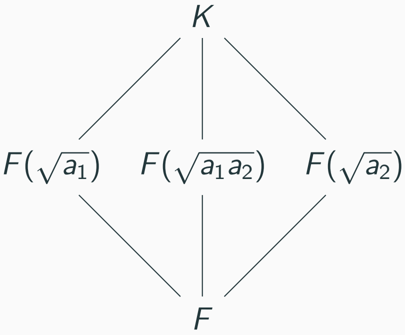
(Spoiler alert: this module has been decomposed, and its "special" for any choice of K/F)

Notation

$K = F(\sqrt{a_1}, \sqrt{a_2})$

$\sigma_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}\sqrt{a_j}$

$G = \mathrm{Gal}(K/F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

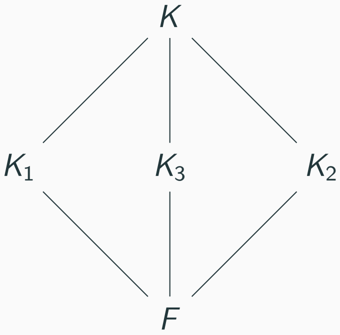


Notation

$K = F(\sqrt{a_1}, \sqrt{a_2})$

$\sigma_i(\sqrt{a_j}) = (-1)^{\delta_{ij}} \sqrt{a_j}$

$G = \mathrm{Gal}(K/F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$



Notation

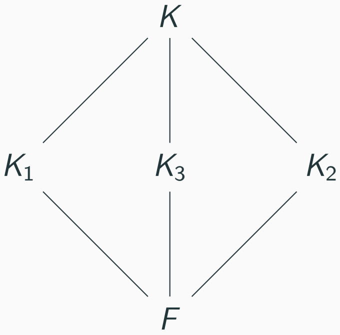
$K = F(\sqrt{a_1}, \sqrt{a_2})$

$\sigma_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}\sqrt{a_j}$

$G = \mathrm{Gal}(K/F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

$[\gamma] \in K^\times/K^{\times 2}$ is class of
$\gamma \in K^\times$

$[\gamma]_i \in K_i^\times/K_i^{\times 2}$ is class of $\gamma \in K_i$



Notation

$K = F(\sqrt{a_1}, \sqrt{a_2})$

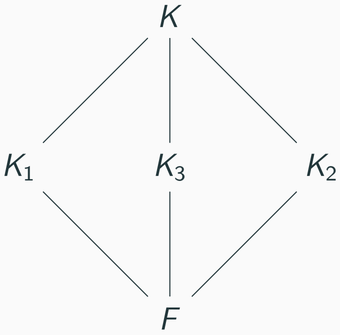
$\sigma_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}\sqrt{a_j}$

$G = \mathrm{Gal}(K/F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

$[\gamma] \in K^\times/K^{\times 2}$ is class of
$\gamma \in K^\times$

$[\gamma]_i \in K_i^\times/K_i^{\times 2}$ is class of $\gamma \in K_i$

$H_i = \mathrm{Gal}(G/K_i)$



Warning: graphic content

Key operators: $1 + \sigma_1$ and $1 + \sigma_2$

Warning: graphic content

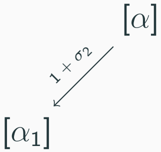
Key operators: $1 + \sigma_1$ and $1 + \sigma_2$

We will view module information with pictures

Warning: graphic content

Key operators: $1 + \sigma_1$ and $1 + \sigma_2$

We will view module information with pictures

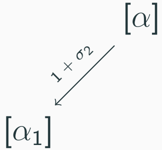


$$[\alpha_1] = [\alpha]^{1+\sigma_2}$$

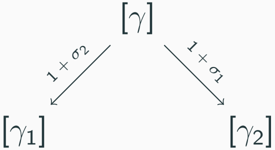
Warning: graphic content

Key operators: $1+\sigma_1$ and $1+\sigma_2$

We will view module information with pictures



$$[\alpha_1] = [\alpha]^{1+\sigma_2}$$

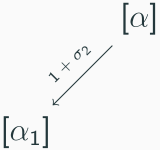


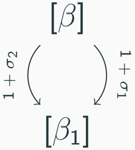
$$\begin{aligned}[\gamma_1] &= [\gamma]^{1+\sigma_2}\\ [\gamma_2] &= [\gamma]^{1+\sigma_1}\end{aligned}$$

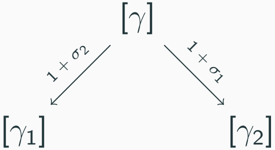
Warning: graphic content

Key operators: $1+\sigma_1$ and $1+\sigma_2$

We will view module information with pictures







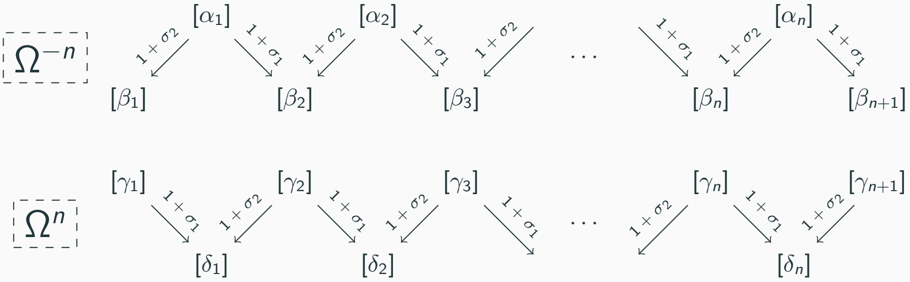
$$[\alpha_1] = [\alpha]^{1+\sigma_2}$$

$$\begin{aligned} [\beta_1] &= [\beta]^{1+\sigma_2} \\ &= [\beta]^{1+\sigma_2} \end{aligned}$$

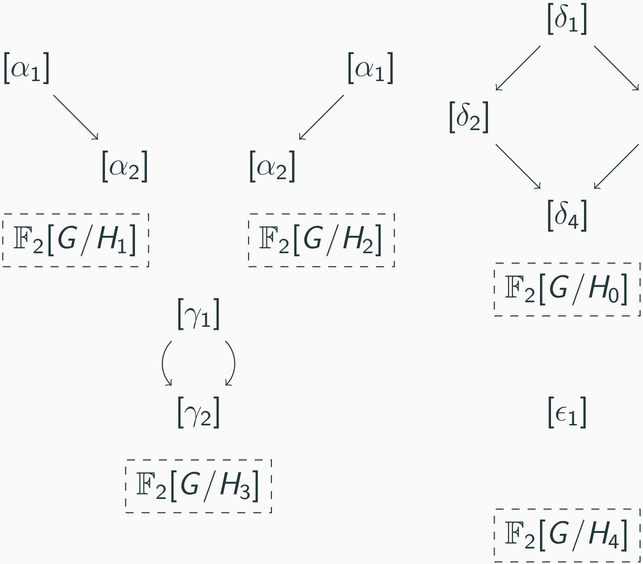
$$\begin{aligned} [\gamma_1] &= [\gamma]^{1+\sigma_2} \\ [\gamma_2] &= [\gamma]^{1+\sigma_1} \end{aligned}$$

A sample of $\mathbb{F}_2[\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}]$-indecomposables

For $n > 1$, there are 2 indecomposables of dimension $2n+1$



A sample of $\mathbb{F}_2[\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}]$-indecomposables



Our module decomposition

Theorem [Chemotti, Mináč, S-, Swallow]

Suppose char$(K) \neq 2$ and $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Then

$$K^\times/K^{\times 2} \simeq O_1 \oplus O_2 \oplus Q_0 \oplus Q_1 \oplus Q_2 \oplus Q_3 \oplus Q_4 \oplus X,$$

where

- for each $i \in \{1, 2\}$, the summand O_i is a direct sum of modules isomorphic to Ω^i; and
- for each $i \in \{0, 1, 2, 3, 4\}$, the summand Q_i is a direct sum of modules isomorphic to $\mathbb{F}_2[G/H_i]$; and
- X is isomorphic to one of the following: $\{0\}, \mathbb{F}_2, \mathbb{F}_2 \oplus \mathbb{F}_2, \Omega^{-1}, \Omega^{-2}$, or $\Omega^{-1} \oplus \Omega^{-1}$.

Our module decomposition

Theorem [Chemotti, Mináč, S-, Swallow]

Suppose char$(K) \neq 2$ and $\mathrm{Gal}(K/F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Then

$$K^\times/K^{\times 2} \simeq \underbrace{O_1 \oplus O_2 \oplus Q_0 \oplus Q_1 \oplus Q_2 \oplus Q_3 \oplus Q_4}_{\text{“unexceptional summand” } Y} \oplus X,$$

where

- for each $i \in \{1, 2\}$, the summand O_i is a direct sum of modules isomorphic to Ω^i; and
- for each $i \in \{0, 1, 2, 3, 4\}$, the summand Q_i is a direct sum of modules isomorphic to $\mathbb{F}_2[G/H_i]$; and
- X is isomorphic to one of the following: $\{0\}, \mathbb{F}_2, \mathbb{F}_2 \oplus \mathbb{F}_2, \Omega^{-1}, \Omega^{-2}$, or $\Omega^{-1} \oplus \Omega^{-1}$.

Motivation and Background

How the decomposition works

Basic strategy

Lemma (Exclusion lemma)

If $U, V \subseteq W$ are $\mathbb{F}_2[G]$-modules, then

$$U \cap V = \{0\} \iff U^G \cap V^G = \{0\}$$

Basic strategy

Lemma (Exclusion lemma)

If $U, V \subseteq W$ are $\mathbb{F}_2[G]$-modules, then

$$U \cap V = \{0\} \iff U^G \cap V^G = \{0\}$$

Strategy:

I: Build a big module Y with $Y^G = [F^\times] \subseteq (K^\times / K^{\times 2})^G$

Basic strategy

Lemma (Exclusion lemma)

If $U, V \subseteq W$ are $\mathbb{F}_2[G]$-modules, then

$$U \cap V = \{0\} \iff U^G \cap V^G = \{0\}$$

Strategy:

I: Build a big module Y with $Y^G = [F^\times] \subseteq (K^\times / K^{\times 2})^G$

II: Build a small module X "over" a complement to $[F^\times]$

Basic strategy

Lemma (Exclusion lemma)

If $U, V \subseteq W$ are $\mathbb{F}_2[G]$-modules, then

$$U \cap V = \{0\} \iff U^G \cap V^G = \{0\}$$

Strategy:

I: Build a big module Y with $Y^G = [F^\times] \subseteq (K^\times / K^{\times 2})^G$

II: Build a small module X "over" a complement to $[F^\times]$

III: Show $X + Y$ spans

Basic strategy

Lemma (Exclusion lemma)

If $U, V \subseteq W$ are $\mathbb{F}_2[G]$-modules, then

$$U \cap V = \{0\} \iff U^G \cap V^G = \{0\}$$

Strategy:

I: Build a big module Y with $Y^G = [F^\times] \subseteq (K^\times / K^{\times 2})^G$

II: Build a small module X "over" a complement to $[F^\times]$

III: Show $X + Y$ spans

How do we build Y?

Guiding principle

If $[f] \in [F^\times]$ is in the image of a norm map in $K^\times/K^{\times 2}$, make sure it's in the image of that norm map in Y.

How do we build Y?

Guiding principle

If $[f] \in [F^\times]$ is in the image of a norm map in $K^\times/K^{\times 2}$, make sure it's in the image of that norm map in Y.

How do we build Y?

Guiding principle

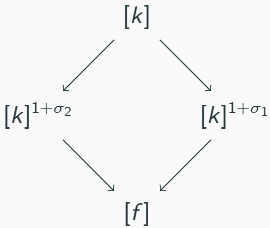
If $[f] \in [F^\times]$ is in the image of a norm map in $K^\times/K^{\times 2}$, make sure it's in the image of that norm map in Y.

Introducing the norms

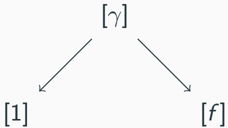
$$\begin{array}{ccc} & [k] & \\ \swarrow & & \searrow \\ [k]^{1+\sigma_2} & & [k]^{1+\sigma_1} \\ \searrow & & \swarrow \\ & [f] & \end{array}$$

$$\mathscr{A} = \{[f] : \exists [k] \ni \dots\}$$

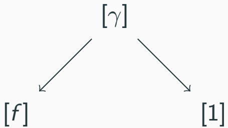
Introducing the norms



$$\mathscr{A} = \{[f] : \exists [k] \ni \dots\}$$



$$\mathscr{B} = \{[f] : \exists [\gamma] \ni \dots\}$$



$$\mathscr{C} = \{[f] : \exists [\gamma] \ni \dots\}$$

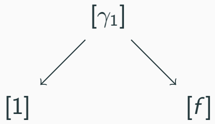
$$\mathscr{D} = \{[f] : \exists [\gamma] \ni \dots\}$$

Tension!

But what if $[f] \in \mathscr{B} \cap \mathscr{C}$?

Tension!

But what if $[f] \in \mathscr{B} \cap \mathscr{C}$?



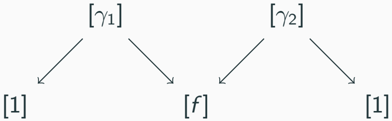
Tension!

But what if $[f] \in \mathscr{B} \cap \mathscr{C}$?

$$[f] \longleftarrow [\gamma_2] \longrightarrow [1]$$

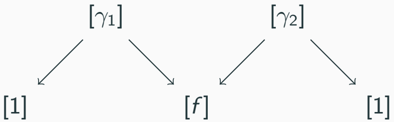
Tension!

But what if $[f] \in \mathscr{B} \cap \mathscr{C}$?



Tension!

But what if $[f] \in \mathscr{B} \cap \mathscr{C}$?



$$\mathscr{V} = \{[f] : \exists [\gamma_1], [\gamma_2] \ni \dots\}$$

To be greedy, we want $\mathscr{V}$ more than $\mathscr{B}$ or $\mathscr{C}$

One final issue

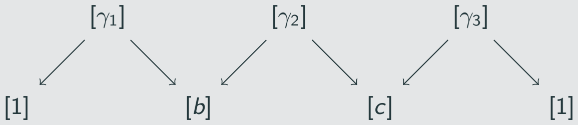
What about $(\mathscr{B} + \mathscr{C}) \cap \mathscr{D}$?

One final issue

What about $(\mathscr{B} + \mathscr{C}) \cap \mathscr{D}$?

Lemma [Tracking norm interactions]

$[b][c] \in (\mathscr{B} + \mathscr{C}) \cap \mathscr{D}$ if and only if there is a solution to



Define $\mathscr{W} = \{([b],[c]) : \exists [\gamma_1], [\gamma_2], [\gamma_3] \ni \ldots\}$.

Building the unexceptional piece

Proposition

There exists a submodule Y whose fixed part is $[F^\times]$, and which is a direct sum of modules isomorphic to

- $\mathbb{F}_2[G/H_i]$ for $i \in \{0, 1, 2, 3, 4\}$
- Ω^k for $k \in \{1, 2\}$

Building the unexceptional piece

Proposition

There exists a submodule Y whose fixed part is $[F^\times]$, and which is a direct sum of modules isomorphic to

- $\mathbb{F}_2[G/H_i]$ for $i \in \{0, 1, 2, 3, 4\}$
- Ω^k for $k \in \{1, 2\}$

Proof sketch:

Building the unexceptional piece

Proposition

There exists a submodule Y whose fixed part is $[F^\times]$, and which is a direct sum of modules isomorphic to

- $\mathbb{F}_2[G/H_i]$ for $i \in \{0, 1, 2, 3, 4\}$
- Ω^k for $k \in \{1, 2\}$

Proof sketch:

Move through subspaces in order $(\mathscr{A}, \mathscr{V}, \mathscr{W}, \mathscr{B}, \mathscr{C}, \mathscr{D}, [F^\times])$

Building the unexceptional piece

Proposition

There exists a submodule Y whose fixed part is $[F^\times]$, and which is a direct sum of modules isomorphic to

- $\mathbb{F}_2[G/H_i]$ for $i \in \{0, 1, 2, 3, 4\}$
- Ω^k for $k \in \{1, 2\}$

Proof sketch:

Move through subspaces in order $(\mathscr{A}, \mathscr{V}, \mathscr{W}, \mathscr{B}, \mathscr{C}, \mathscr{D}, [F^\times])$

$\rightsquigarrow$ Make module "above" your element for given diagram

Building the unexceptional piece

Proposition

There exists a submodule Y whose fixed part is $[F^\times]$, and which is a direct sum of modules isomorphic to

- $\mathbb{F}_2[G/H_i]$ for $i \in \{0, 1, 2, 3, 4\}$
- Ω^k for $k \in \{1, 2\}$

Proof sketch:

Move through subspaces in order $(\mathscr{A}, \mathscr{V}, \mathscr{W}, \mathscr{B}, \mathscr{C}, \mathscr{D}, [F^\times])$

$\rightsquigarrow$ Make module “above” your element for given diagram

$\rightsquigarrow$ Be sure to avoid what you’ve already captured!

Reinterpreting the construction of Y

Arithmetic interpretation for solvability

Original argument views Y in terms of solvability of diagrams, but gives no indication of how we determine solvability

Arithmetic interpretation for solvability

Original argument views Y in terms of solvability of diagrams, but gives no indication of how we determine solvability

Theorem [Diagram solvability and $\mathrm{Br}(F)$]

Let $\mathcal{S} = \langle (a_1, a_1), (a_1, a_2), (a_2, a_2) \rangle \subseteq \mathrm{Br}(F)$. For $f, g \in F^\times$, we have $(a_1, f)(a_2, g) \in \mathcal{S}$ iff there exists $\gamma \in K^\times$ with

$$[g] \xleftarrow{1+\sigma_2} [\gamma] \xrightarrow{1+\sigma_1} [f]$$

Arithmetic interpretation for solvability

Original argument views Y in terms of solvability of diagrams, but gives no indication of how we determine solvability

Theorem [Diagram solvability and $\mathrm{Br}(F)$]

Let $\mathcal{S} = \langle (a_1, a_1), (a_1, a_2), (a_2, a_2) \rangle \subseteq \mathrm{Br}(F)$. For $f, g \in F^\times$, we have $(a_1, f)(a_2, g) \in \mathcal{S}$ iff there exists $\gamma \in K^\times$ with

$$[g] \xleftarrow{1+\sigma_2} [\gamma] \xrightarrow{1+\sigma_1} [f]$$

Sketch of proof: solvability of Galois embedding problems

Thinking rationally

Great news: if $F = \mathbb{Q}$, then local-global principle makes computing elements of $\mathrm{Br}(\mathbb{Q})$ nicely explicit:
$(a, b) = (c, d) \in \mathrm{Br}(\mathbb{Q})$ iff for all $v \in \{2, 3, 5, 7, \cdots, \infty\}$ we have $(a, b)_v = (c, d)_v$

Thinking rationally

Great news: if $F = \mathbb{Q}$, then local-global principle makes computing elements of $\mathrm{Br}(\mathbb{Q})$ nicely explicit:
$(a, b) = (c, d) \in \mathrm{Br}(\mathbb{Q})$ iff for all $v \in \{2, 3, 5, 7, \cdots, \infty\}$ we have $(a, b)_v = (c, d)_v$

- if $p = \infty$ and $a, b \in \mathbb{Z}$ then

$$(a, b)_\infty = -1 \text{ if } a, b < 0, \qquad (a, b)_\infty = 1 \text{ else}$$

- if p odd prime then for $\gcd(a, p) = \gcd(b, p) = 1$ we get

$$(a, b)_p = 1, \qquad (a, p)_p = \left(\frac{a}{p}\right), \qquad (p, p)_p = \left(\frac{-1}{p}\right)$$

- if $p = 2$ and $a, b \in 2\mathbb{Z} + 1$ then

$$(a, b)_2 = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}, \quad (a, 2)_p = (-1)^{\frac{a^2-1}{8}}, \quad (2, 2)_2 = 1$$

Application: hunting for summands

$$\mathscr{V} = \left\{ [f] : \exists [\gamma_1], [\gamma_2] \text{ with } \begin{array}{ccccccc} & & [\gamma_1] & & [\gamma_2] & & \\ & \swarrow & & \searrow \; \swarrow & & \searrow & \\ [1] & & & [f] & & & [1] \end{array} \right\}$$

Application: hunting for summands

$$\mathscr{V} = \left\{ [f] : \exists [\gamma_1], [\gamma_2] \text{ with } \begin{array}{ccccccc} & [\gamma_1] & & & [\gamma_2] & & \\ \swarrow & & \searrow & \swarrow & & \searrow & \\ [1] & & & [f] & & & [1] \end{array} \right\}$$

$$= \{[f] : (a_1, f)(a_2, 1) \in \mathcal{S} \text{ and } (a_1, 1)(a_2, f) \in \mathcal{S}\}$$

Application: hunting for summands

$$\mathscr{V} = \left\{ [f] : \exists [\gamma_1], [\gamma_2] \text{ with } \begin{array}{ccccccc} & [\gamma_1] & & & [\gamma_2] & & \\ \swarrow & & \searrow & \swarrow & & \searrow & \\ [1] & & & [f] & & & [1] \end{array} \right\}$$

$$= \{[f] : (a_1, f)(a_2, 1) \in \mathcal{S} \text{ and } (a_1, 1)(a_2, f) \in \mathcal{S}\}$$

Application: hunting for summands

$$\mathscr{V} = \left\{ [f] : \exists [\gamma_1], [\gamma_2] \text{ with } [1] \leftarrow [\gamma_1] \rightarrow [f] \leftarrow [\gamma_2] \rightarrow [1] \right\}$$

$$= \{[f] : (a_1, f)(a_2, 1) \in \mathcal{S} \text{ and } (a_1, 1)(a_2, f) \in \mathcal{S}\}$$

$$= \{[f] : (a_1, f) \in \mathcal{S} \text{ and } (a_2, f) \in \mathcal{S}\}$$

Application: hunting for summands

$$\mathscr{V} = \left\{ [f] : \exists[\gamma_1],[\gamma_2] \text{ with } \begin{array}{ccccccccc} & & [\gamma_1] & & & & [\gamma_2] & & \\ & \swarrow & & \searrow & & \swarrow & & \searrow & \\ [1] & & & & [f] & & & & [1] \end{array} \right\}$$

$$= \{[f] : (a_1, f)(a_2, 1) \in \mathcal{S} \text{ and } (a_1, 1)(a_2, f) \in \mathcal{S}\}$$

$$= \{[f] : (a_1, f) \in \mathcal{S} \text{ and } (a_2, f) \in \mathcal{S}\}$$

Corollary

Ω^1 summands of $K^\times/K^{\times 2}$ exist if there exists f so that $(a_1, f), (a_2, f) \in \mathcal{S} \setminus \{0\}$.

Finding Ω^1 summands in the wild

Let $K/F = \mathbb{Q}(\sqrt{7}, \sqrt{-5})/\mathbb{Q}$

$$\mathcal{S} = \langle (7,7), (7,-5), (-5,-5) \rangle$$

Finding Ω^1 summands in the wild

Let $K/F = \mathbb{Q}(\sqrt{7}, \sqrt{-5})/\mathbb{Q}$

$$\mathcal{S} = \langle (7,7), (7,-5), (-5,-5) \rangle$$

Goal: show $K^\times / K^{\times 2}$ has Ω^1 summands

$\rightsquigarrow$ enough to find $f \in \mathbb{Q}$ so $(-5, f), (7, f) \in \mathcal{S} \setminus \{0\}$

Finding Ω^1 summands in the wild

Let $K/F = \mathbb{Q}(\sqrt{7}, \sqrt{-5})/\mathbb{Q}$

$$\mathcal{S} = \langle (7,7), (7,-5), (-5,-5) \rangle$$

Goal: show $K^\times / K^{\times 2}$ has Ω^1 summands

$\rightsquigarrow$ enough to find $f \in \mathbb{Q}$ so $(-5, f), (7, f) \in \mathcal{S} \setminus \{0\}$

Strategy: find prime p with $(-5, -p) = (-5, -5)$ and $(7, -p) = (7, 7)$

Finding our prime, part I: $(-5,-5)=(-5,-p)$

Fact: $(-5,-5)_v = -1$ iff $v = 2, \infty$

Finding our prime, part I: $(-5,-5) = (-5,-p)$

Fact: $(-5,-5)_v = -1$ iff $v = 2, \infty$

$$(-5,-p)_v = (-1,-1)_v(5,-1)_v(-1,p)_v(5,p)_v$$

Finding our prime, part I: $(-5,-5) = (-5,-p)$

Fact: $(-5,-5)_v = -1$ iff $v = 2, \infty$

$$(-5,-p)_v = (-1,-1)_v (5,-1)_v (-1,p)_v (5,p)_v$$
$$= \begin{cases} & \text{if } v = \infty \\ & \text{if } v = 2 \\ & \text{if } v = 5 \\ & \text{if } v = p. \end{cases}$$

Finding our prime, part I: $(-5,-5) = (-5,-p)$

Fact: $(-5,-5)_v = -1$ iff $v = 2, \infty$

$$(-5,-p)_v = (-1,-1)_v(5,-1)_v(-1,p)_v(5,p)_v$$

$$= \begin{cases} -1, & \text{if } v = \infty \\ & \text{if } v = 2 \\ & \text{if } v = 5 \\ & \text{if } v = p. \end{cases}$$

Finding our prime, part I: $(-5,-5)=(-5,-p)$

Fact: $(-5,-5)_v = -1$ iff $v = 2, \infty$

$$
\begin{aligned}
(-5,-p)_v &= (-1,-1)_v(5,-1)_v(-1,p)_v(5,p)_v \\
&= \begin{cases}
-1, & \text{if } v=\infty \\
-1\cdot 1\cdot(-1)^{\frac{p-1}{2}}\cdot 1, & \text{if } v=2 \\
 & \text{if } v=5 \\
 & \text{if } v=p.
\end{cases}
\end{aligned}
$$

Finding our prime, part I: $(-5,-5) = (-5,-p)$

Fact: $(-5,-5)_v = -1$ iff $v = 2, \infty$

$$(-5,-p)_v = (-1,-1)_v(5,-1)_v(-1,p)_v(5,p)_v$$
$$= \begin{cases} -1, & \text{if } v = \infty \\ -1 \cdot 1 \cdot (-1)^{\frac{p-1}{2}} \cdot 1, & \text{if } v = 2 \\ 1 \cdot \left(\frac{-1}{5}\right) \cdot 1 \cdot \left(\frac{p}{5}\right), & \text{if } v = 5 \\ & \text{if } v = p. \end{cases}$$

Finding our prime, part I: $(-5,-5)=(-5,-p)$

Fact: $(-5,-5)_v = -1$ iff $v = 2, \infty$

$$(-5,-p)_v = (-1,-1)_v(5,-1)_v(-1,p)_v(5,p)_v$$
$$= \begin{cases} -1, & \text{if } v=\infty \\ -1\cdot 1\cdot(-1)^{\frac{p-1}{2}}\cdot 1, & \text{if } v=2 \\ 1\cdot\left(\frac{-1}{5}\right)\cdot 1\cdot\left(\frac{p}{5}\right), & \text{if } v=5 \\ 1\cdot 1\cdot\left(\frac{-1}{p}\right)\cdot\left(\frac{5}{p}\right), & \text{if } v=p. \end{cases}$$

Finding our prime, part I: $(-5,-5) = (-5,-p)$

Fact: $(-5,-5)_v = -1$ iff $v = 2, \infty$

$$(-5,-p)_v = (-1,-1)_v(5,-1)_v(-1,p)_v(5,p)_v$$
$$= \begin{cases} -1, & \text{if } v = \infty \\ -1 \cdot 1 \cdot (-1)^{\frac{p-1}{2}} \cdot 1, & \text{if } v = 2 \\ 1 \cdot \left(\frac{-1}{5}\right) \cdot 1 \cdot \left(\frac{p}{5}\right), & \text{if } v = 5 \\ 1 \cdot 1 \cdot \left(\frac{-1}{p}\right) \cdot \left(\frac{5}{p}\right), & \text{if } v = p. \end{cases}$$

So we want $p \equiv 1 \pmod 4$ and $p \equiv 1, 4 \pmod 5$

Finding our prime, part II: $(7,7) = (7,-p)$

Fact: $(7,7)_v = -1$ iff $v = 2, 7$

Finding our prime, part II: $(7,7) = (7,-p)$

Fact: $(7,7)_v = -1$ iff $v = 2, 7$

$$
\begin{aligned}
(7,-p)_v &= (7,-1)_v (7,p)_v \\
&= \begin{cases} 1, & \text{if } v = \infty \\ -1 \cdot (-1)^{\frac{p-1}{2}}, & \text{if } v = 2 \\ \left(\frac{-1}{7}\right) \cdot \left(\frac{p}{7}\right), & \text{if } v = 7 \\ 1 \cdot \left(\frac{7}{p}\right), & \text{if } v = p. \end{cases}
\end{aligned}
$$

Finding our prime, part II: $(7,7) = (7,-p)$

Fact: $(7,7)_v = -1$ iff $v = 2, 7$

$$
\begin{aligned}
(7,-p)_v &= (7,-1)_v (7,p)_v \\
&= \begin{cases}
1, & \text{if } v = \infty \\
-1 \cdot (-1)^{\frac{p-1}{2}}, & \text{if } v = 2 \\
\left(\frac{-1}{7}\right) \cdot \left(\frac{p}{7}\right), & \text{if } v = 7 \\
1 \cdot \left(\frac{7}{p}\right), & \text{if } v = p.
\end{cases}
\end{aligned}
$$

So we need $p \equiv 1 \pmod 4$ and $p \equiv 1, 2, 4 \pmod 7$

Finding our prime, part II: $(7,7) = (7,-p)$

Fact: $(7,7)_v = -1$ iff $v = 2, 7$

$$\begin{aligned}(7,-p)_v &= (7,-1)_v (7,p)_v \\ &= \begin{cases} 1, & \text{if } v = \infty \\ -1 \cdot (-1)^{\frac{p-1}{2}}, & \text{if } v = 2 \\ \left(\frac{-1}{7}\right) \cdot \left(\frac{p}{7}\right), & \text{if } v = 7 \\ 1 \cdot \left(\frac{7}{p}\right), & \text{if } v = p. \end{cases}\end{aligned}$$

So we need $p \equiv 1 \pmod 4$ and $p \equiv 1, 2, 4 \pmod 7$

Summary: any prime p with $p \equiv 1 \pmod 4$, $p \equiv 1, 4 \pmod 5$, and $p \equiv 1, 2, 4 \pmod 7$ works.

Finding our prime, part II: $(7,7) = (7,-p)$

Fact: $(7,7)_v = -1$ iff $v = 2, 7$

$$
\begin{aligned}
(7,-p)_v &= (7,-1)_v(7,p)_v \\
&= \begin{cases} 1, & \text{if } v = \infty \\ -1 \cdot (-1)^{\frac{p-1}{2}}, & \text{if } v = 2 \\ \left(\frac{-1}{7}\right) \cdot \left(\frac{p}{7}\right), & \text{if } v = 7 \\ 1 \cdot \left(\frac{7}{p}\right), & \text{if } v = p. \end{cases}
\end{aligned}
$$

So we need $p \equiv 1 \pmod 4$ and $p \equiv 1, 2, 4 \pmod 7$

Summary: any prime p with $p \equiv 1 \pmod 4$, $p \equiv 1, 4 \pmod 5$, and $p \equiv 1, 2, 4 \pmod 7$ works.

$\rightsquigarrow$ lots of Ω^1 summands in this module

What about Ω^2 summands?

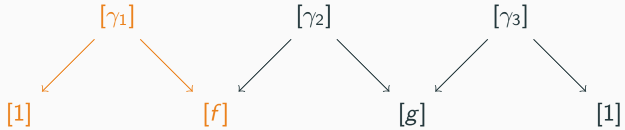
Ω^2 summands occurs for solutions to

$$\begin{array}{ccccccccccc} & & [\gamma_1] & & & & [\gamma_2] & & & & [\gamma_3] & & \\ & \swarrow & & \searrow & & \swarrow & & \searrow & & \swarrow & & \searrow & \\ [1] & & & & [f] & & & & [g] & & & & [1] \end{array}$$

AND we must have $[f], [g] \notin \mathscr{V}$

What about Ω^2 summands?

Ω^2 summands occurs for solutions to

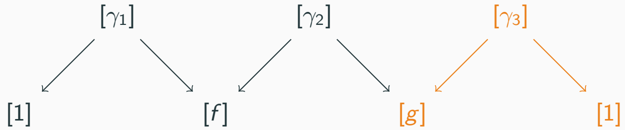


AND we must have $[f], [g] \notin \mathscr{V}$

So we need $(a_1, f), (a_2, g) \in \mathcal{S}$ and $(a_2, f)(a_1, g) \in \mathcal{S}$ but $(a_2, f), (a_1, g) \notin \mathcal{S}$

What about Ω^2 summands?

Ω^2 summands occurs for solutions to

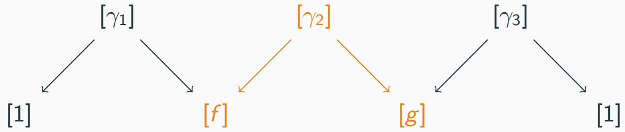


AND we must have $[f], [g] \notin \mathscr{V}$

So we need $(a_1, f), (a_2, g) \in \mathcal{S}$ and $(a_2, f)(a_1, g) \in \mathcal{S}$ but $(a_2, f), (a_1, g) \notin \mathcal{S}$

What about Ω^2 summands?

Ω^2 summands occurs for solutions to

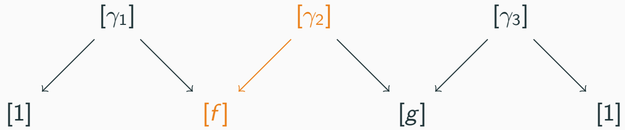


AND we must have $[f], [g] \notin \mathscr{V}$

So we need $(a_1, f), (a_2, g) \in \mathcal{S}$ and $(a_2, f)(a_1, g) \in \mathcal{S}$ but $(a_2, f), (a_1, g) \notin \mathcal{S}$

What about Ω^2 summands?

Ω^2 summands occurs for solutions to

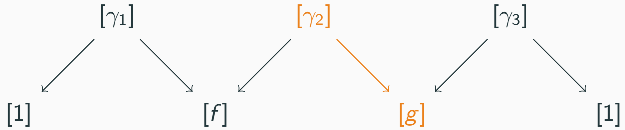


AND we must have $[f], [g] \notin \mathscr{V}$

So we need $(a_1, f), (a_2, g) \in \mathcal{S}$ and $(a_2, f)(a_1, g) \in \mathcal{S}$ but $(a_2, f), (a_1, g) \notin \mathcal{S}$

What about Ω^2 summands?

Ω^2 summands occurs for solutions to

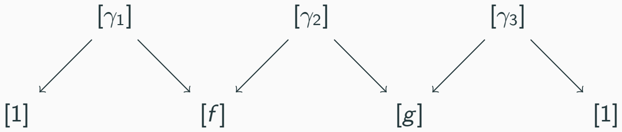


AND we must have $[f], [g] \notin \mathscr{V}$

So we need $(a_1, f), (a_2, g) \in \mathcal{S}$ and $(a_2, f)(a_1, g) \in \mathcal{S}$ but $(a_2, f), (a_1, g) \notin \mathcal{S}$

What about Ω^2 summands?

Ω^2 summands occurs for solutions to



AND we must have $[f], [g] \notin \mathscr{V}$

So we need $(a_1, f), (a_2, g) \in \mathcal{S}$ and $(a_2, f)(a_1, g) \in \mathcal{S}$ but $(a_2, f), (a_1, g) \notin \mathcal{S}$

Corollary

Ω^2 summands of $K^\times / K^{\times 2}$ exist if there exist f, g so that $(a_1, f), (a_2, g) \in \mathcal{S}$ and $(a_1, g) = (a_2, f) \notin \mathcal{S}$.

Finding Ω^2 summands in the wild

Let $K/F = \mathbb{Q}(\sqrt{33}, \sqrt{35})/\mathbb{Q}$

Finding Ω^2 summands in the wild

Let $K/F = \mathbb{Q}(\sqrt{33}, \sqrt{35})/\mathbb{Q}$

Goal: show $K^\times/K^{\times 2}$ has Ω^2 summands

$\rightsquigarrow$ enough to find f, g so that $(a_1, f), (a_2, g) \in \mathcal{S}$ and $(a_1, g) = (a_2, f) \notin \mathcal{S}$.

Finding Ω^2 summands in the wild

Let $K/F = \mathbb{Q}(\sqrt{33}, \sqrt{35})/\mathbb{Q}$

Goal: show $K^\times/K^{\times 2}$ has Ω^2 summands

$\rightsquigarrow$ enough to find f, g so that $(a_1, f), (a_2, g) \in \mathcal{S}$ and $(a_1, g) = (a_2, f) \notin \mathcal{S}$.

Strategy: find primes p, q with $(33, 3pq) = (33, 33)$ and $(35, 7pq) = (1, 1)$ and $(33, 7pq) = (35, 3pq) \notin \mathcal{S}$

Finding Ω^2 summands in the wild

Let $K/F = \mathbb{Q}(\sqrt{33}, \sqrt{35})/\mathbb{Q}$

Goal: show $K^\times/K^{\times 2}$ has Ω^2 summands

$\rightsquigarrow$ enough to find f, g so that $(a_1, f), (a_2, g) \in \mathcal{S}$ and $(a_1, g) = (a_2, f) \notin \mathcal{S}$.

Strategy: find primes p, q with $(33, 3pq) = (33, 33)$ and $(35, 7pq) = (1, 1)$ and $(33, 7pq) = (35, 3pq) \notin \mathcal{S}$

$\rightsquigarrow$ Choose p so $p \not\equiv \square \pmod 3$, $p \not\equiv \square \pmod 4$, $p \not\equiv \square \pmod 5$, $p \equiv \square \pmod 7$, and $p \not\equiv \square \pmod{11}$

$\rightsquigarrow$ Choose q so $q \equiv \square \pmod 3$, $q \equiv \square \pmod 4$, $q \equiv \square \pmod 5$, $q \equiv \square \pmod 7$, and $q \equiv \square \pmod{11}$

Lather, rinse, repeat

This same strategy provides methods for realizing other "unexceptional" summand types over well-chosen rational biquadratic extensions

Lather, rinse, repeat

This same strategy provides methods for realizing other "unexceptional" summand types over well-chosen rational biquadratic extensions

The structure of the X summand also has new interpretation in this lens (but less exciting since it was originally interpretable in terms of Galois embeddings)

Thanks!