Galois Module Structure of Square Power Classes in Biquadratic Extensions

Andrew Schultz

September 27, 2020

Wellesley College

In collaboration with...

John Swallow

Frank Chemotti

Ján Mináč

Motivation and Background

Motivation

Inverse Galois Problem

If G is a group and K is a field, can we find/parameterize all G-extensions of K?

Kummer theory: if $\text{char}(K) \neq p$ and $\xi_p \in K$:

$$\left\{ \begin{array}{c} \text{Elementary } p\text{-abelian} \\ \text{extensions of K} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \mathbb{F}_p - \text{subspaces} \\ \text{of } \boxed{K^\times / K^{\times p}} \end{array} \right\}$$

Artin-Schreier theory: if $\text{char}(K) = p$:

$$\left\{ \begin{array}{c} \text{Elementary } p\text{-abelian} \\ \text{extensions of K} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \mathbb{F}_p - \text{subspaces} \\ \text{of } \boxed{K / \wp(K)} \end{array} \right\}$$

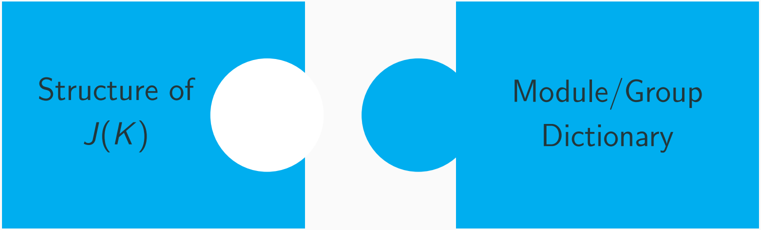
$J(K)$

More structure $\Longrightarrow$ more structure

Proposition (Waterhouse,S-)

If M is an $\mathbb{F}_p$-subspace of $J(K)$, and L/K its extension, then L/F Galois iff M is an $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-module.

In fact, $\mathrm{Gal}(L/F)$ can be computed in terms of module structure of M and some field-theoretic data.



What's been done

$\mathrm{Gal}(K/F)$	Module	Caveats
$\mathbb{Z}/p^n\mathbb{Z}$	$J(K)$	$\emptyset$
$\mathbb{Z}/p^n\mathbb{Z}$	$E^\times/E^{\times p^s}$	$\mathrm{char}(E) \neq p$
$\mathbb{Z}/p\mathbb{Z}$	$H^i(K, \mathbb{F}_p)$	$\xi_p \in K$
$\mathbb{Z}/p^n\mathbb{Z}$	$H^i(K, \mathbb{F}_p)$	$\xi_p \in K$ and embedibility
$\mathbb{Z}/p\mathbb{Z}$	$K_i(K)/p^s K_i(K)$	$\mathrm{char}(K) = p$

The general trend

Modules have far fewer classes of indecomposable modules than one would expect

Punchline: Maximal pro-p quotient of absolute Galois group isn't a generic pro-p group

Corollary

Let $p > 2$. Define $\nu(G, F)$ as number of G-extensions of F. Then $\nu(M_{p^3}, F)$ is

$$(p^2 - 1)\nu(H_{p^3}, F) + \underbrace{\left(\binom{\dim_{\mathbb{F}_p} J(F)}{1}_p - \binom{\dim_{\mathbb{F}_p} \mathfrak{N}}{1}_p\right)}_{\text{“non-embeddable” } \mathbb{Z}/p\mathbb{Z}\text{-extensions of } F} \frac{|J(F)|}{p^2}.$$

Moving away from cyclic extensions

How can we dip our toe into the non-cyclic cases?

Let G be as simple as possible $\rightsquigarrow$ $G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

Structure of $K^\times/K^{\times 2}$

Notation

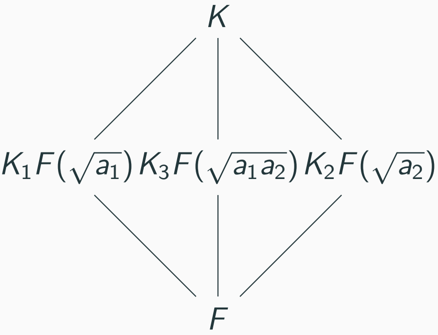
$K = F(\sqrt{a_1}, \sqrt{a_2})$

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

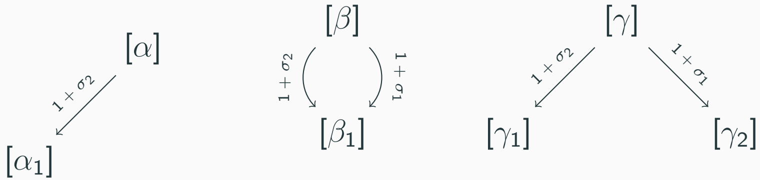
$G = \mathrm{Gal}(K/F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

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

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



Warning: graphic content



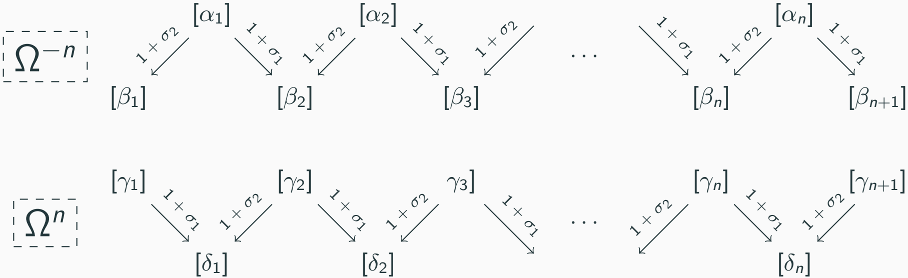
$$[\alpha_1] = [\alpha]^{1+\sigma_2}$$

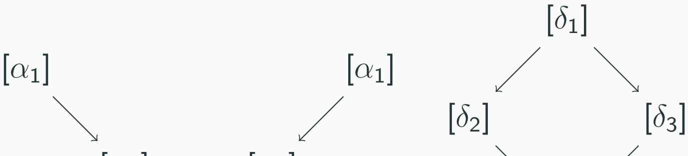
$$\begin{aligned}[\beta_1] &= [\beta]^{1+\sigma_2} \\ &= [\beta]^{1+\sigma_2}\end{aligned}$$

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

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

For $n > 0$, there are 2 indecomposables of dimension $2n + 1$





Our module decomposition

Theorem [Chemotti, Mináč, S-, Swallow]

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

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

where

- O_1 is a direct sum of modules isomorphic to Ω^1; 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 $\Omega^{-1} \oplus \Omega^{-1}$.

Sketch of proof

Playbill

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: Focus on $(K^\times/K^{\times 2})^G = [F^\times]+??$

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

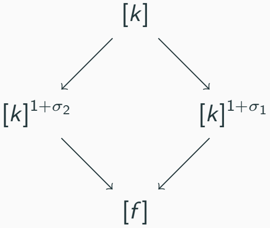
Act II: Build a big module X "over" a complement to $[F^\times]$

Act III: Show $X + Y$ spans

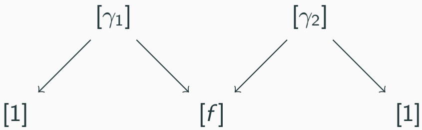
Sketch of proof

Act I: Building over $[F^\times]$

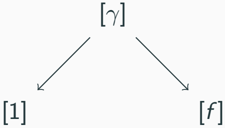
Act I: maximize preimages, minimize generators



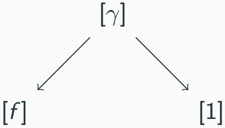
$\mathfrak{A} = \{[f] : \exists [k] \ni \dots\}$



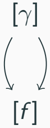
$\mathfrak{B} = \{[f] : \exists [\gamma_1], [\gamma_2] \ni \dots\}$



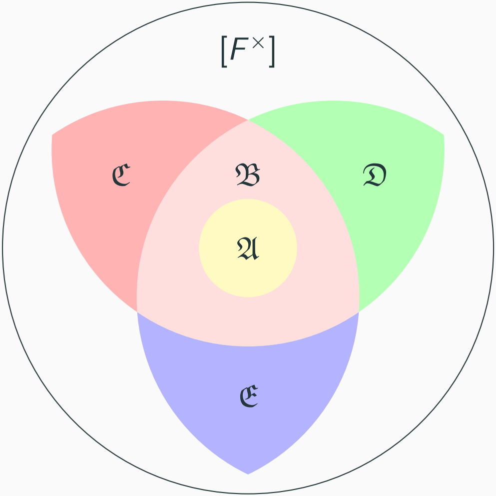
$\mathfrak{C} = \{[f] : \exists [\gamma] \ni \dots\}$



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



$\mathfrak{E} = \{[f] : \exists [\gamma] \ni \dots\}$


$[F^\times]$
$\mathfrak{C}$
$\mathfrak{B}$
$\mathfrak{D}$
$\mathfrak{A}$
$\mathfrak{E}$

Act I: Conclusion

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^1

Sketch of proof

Act II: Filling out $(K^\times/K^{\times 2})^G$

Act II: WTF

Lemma (Whether 'tis $[f]$)

For $[\gamma] \in (K^\times/K^{\times 2})^G$, the following are equivalent:

- $[\gamma] \in [F^\times]$
- $\mathrm{Gal}(K(\sqrt{\gamma})/F) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
- $[\gamma] \in \bigcap_{i=1}^{3} \ker \left(K^\times/K^{\times 2} \xrightarrow{N_{K/K_i}} K_i^\times/K_i^{\times 2} \right)$

Act II: How we build a complement

$[F^\times]$ is kernel of $T : J^G \to \bigoplus_{i=1}^3 (K_i^\times \cap K^{\times 2})/K_i^{\times 2}$ given by

$$T([\gamma]) = \big([N_{K/K_1}(\gamma)]_1, [N_{K/K_2}(\gamma)]_2, [N_{K/K_3}(\gamma)]_3\big)$$

Goal: Find "big" preimage for $\mathrm{im}(T)$ that has trivial intersection with $[F^\times]$

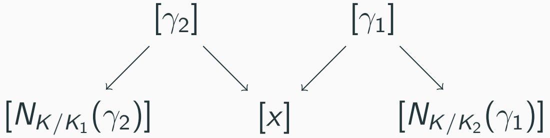
What we get depends on $\mathrm{im}(T)$

Act II: An example

Suppose $[x] \in \left([N_{K/K_1}(K^\times)] \cap [N_{K/K_2}(K^\times)] \cap J^G\right) \setminus \ker(T)$

$\rightsquigarrow$ exists $[\gamma_1], [\gamma_2]$ so that $[N_{K/K_i}(\gamma_i)] = [x]$

$\rightsquigarrow$ $\dim\left(T(\{[x], [N_{K/K_1}(\gamma_2)], [N_{K/K_2}(\gamma_1)]\})\right) = 3$



Ω^{-2}

Act II: Another example

Suppose that $\operatorname{im}(T) = \{([1]_1, [v]_2, [w]_3\}$

$\rightsquigarrow$ solvability of certain "small" Galois embedding problems

$\rightsquigarrow$ solvability of particular "large" Galois embedding problem

$\rightsquigarrow$ exists $[\gamma]$ so that $\mathrm{im}(T) = T\left(\{[N_{K/K_1}(\gamma)], [N_{K/K_2}(\gamma)]\}\right)$

$$[\gamma] \swarrow [N_{K/K_1}(\gamma)] \qquad [\gamma] \searrow [N_{K/K_2}(\gamma)]$$

Ω^{-1}

Act II: Constructing X

Proposition

Suppose $\{\mathrm{im}(T)\} \neq \{[1]_1, [1]_2, [1]_3\}$. Then there exists $X \in J(K)$ with $T(X^G) = \mathrm{im}(T)$, so that X is isomorphic to

$$\begin{cases} \mathbb{F}_2, & \text{if } \dim_{\mathbb{F}_2}(\mathrm{im}(T)) = 1 \\ \Omega^{-1}, & \text{if } \mathrm{im}(T) \text{ is a "coordinate plane"} \\ \mathbb{F}_2 \oplus \mathbb{F}_2, & \text{if } \mathrm{im}(T) \text{ is a "non-coordinate plane"} \\ \Omega^{-2}, & \text{if } T([N_{K/K_1}(K^\times)] \cap [N_{K/K_2}(K^\times)] \cap J^G) \text{ nontrivial} \\ \Omega^{-1} \oplus \Omega^{-1}, & \text{else.} \end{cases}$$

Note: in final case $\dim(X \cap [F^\times]) = 1$. Requires small Y tweak.

Sketch of proof

Act III: Putting it all together

Act III: Gotta catch 'em all

$X + Y = X \oplus Y$ by "exclusion lemma". Do they span?

Case 1: Suppose $\langle[\gamma]\rangle \simeq \mathbb{F}_2$

$\rightsquigarrow$ Can assume $T([\gamma]) = ([1]_1, [1]_2, [1]_3)$ by X

$\rightsquigarrow$ We picked up all of $[F^\times]$ in Y^G ✓

Act III: Still gotta catch 'em all

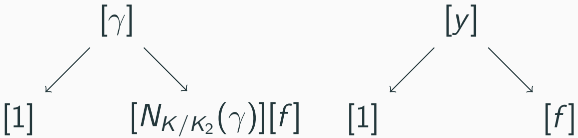
Case 2: Suppose $\langle[\gamma]\rangle \simeq \mathbb{F}_2[G/H_1]$.

$\rightsquigarrow$ Can prove $T([N_{K/K_2}(\gamma)]) = ([1]_1, [1]_2, [1]_3)$

$\rightsquigarrow$ $[N_{K/K_2}(\gamma)] = [f] \in \mathfrak{C}$

$\rightsquigarrow$ $\exists [y] \in Y$ with same images under $1 + \sigma_i$

$\rightsquigarrow$ $\langle[\gamma]/[y]\rangle \simeq \{[1]\}$ or $\langle[\gamma]/[y]\rangle \simeq \mathbb{F}_2$ ✓



Act III: Almost caught 'em all

Case 3: Suppose that $\langle[\gamma]\rangle \simeq \Omega^1$

$\rightsquigarrow$ Can assume $\langle[\gamma]\rangle^G \subseteq \ker(T)$ by X's construction

$\rightsquigarrow$ Lemma: $[F^\times] \cap [N_{K/K_1}(K^\times)] \subseteq \mathfrak{D} \cdot \mathfrak{E}$

$\rightsquigarrow$ Can "cut down" to a module type already checked

Act III: Cutting the module

$$
\begin{array}{ccccc}
[\gamma_{1,3}] & & [\gamma_{1,2}] & & [\gamma] \\
\curvearrowleft\ \curvearrowright & \swarrow & & \swarrow & \searrow \\
[f_{1,3}] & [f_{1,2}] & = [N_{K/K_1}(\gamma)] & & [N_{K/K_2}(\gamma)] \\
\in \mathfrak{E} & \in \mathfrak{D} & \in [F^\times] & &
\end{array}
$$

Then $([\gamma][\gamma_{1,3}][\gamma_{1,2}])^{1+\sigma_2} = [1]$

$\rightsquigarrow$ so $\langle [\gamma][\gamma_{1,3}][\gamma_{1,2}] \rangle$ is some previous case.

Thank you!