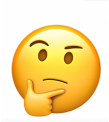
# The Galois module structure of integers in tame radical extensions.

Ilaria Del Corso
Università di Pisa

Hopf algebras & Galois module theory
University of Nebraska at Omaha
May 30, 2024

Motivation: I want to listen to Paul's talk! 

I needed a strategy . . .  . . .

I asked Paul to give a coordinate talk!

Consequences: I have to do my part... 

# Galois module structure

- $L/K$ finite Galois extension
- $G = Gal(L/K)$

$L$ is a left $K[G]$-module under the action

$$(\sum_{\sigma \in G} k_\sigma \sigma) \cdot x = \sum_{\sigma \in G} k_\sigma \sigma(x).$$

When we say that $L$ is a Galois module, we are referring to this action.

## Normal Basis Theorem

*$L$ is a free $K[G]$-module of rank 1, namely*

$$L = K[G]\omega$$

*for some $\omega \in L$. $\{\sigma(\omega)\}_{\sigma \in G}$ is a $K$-basis of $L$ called a normal basis.*

# The Number Theory side

If $L$ and $K$ are number fields (or $p$-adic fields), and denote by $\mathcal{O}_L$ and $\mathcal{O}_K$ their rings of integers.

$\mathcal{O}_L$ is a left $\mathcal{O}_K[G]$-module.

Question

*Is $\mathcal{O}_L$ free (of rank one) over $\mathcal{O}_K[G]$?*

In this case, $\mathcal{O}_L = \mathcal{O}_K[G]\omega$ and we call $\{\sigma(\omega)\}_{\sigma \in G}$ a *normal integral basis* (NIB) of $L/K$.

The general answer to this question is no.

- $\mathcal{O}_L$ might not be free over $\mathcal{O}_K$
- $\mathbb{Z}[i]$ is free over $\mathbb{Z}$, but not as a $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})]$-module

# General results

**Theorem (Noether's theorem)**
*$\mathcal{O}_L$ is $\mathcal{O}_K[G]$ locally-free $\iff L/K$ is tamely ramified.*

**Corollary**
*$\mathcal{O}_L$ free over $\mathcal{O}_K[G] \implies L/K$ is tamely ramified.*

**Theorem (Hilbert–Speiser's theorem)**
*$L/\mathbb{Q}$ abelian $L/\mathbb{Q}$ abelian $+$ tame $\Leftrightarrow L/\mathbb{Q}$ admits a NIB*
*(i.e. $\mathcal{O}_L$ is free over $\mathcal{O}_K[G]$)*

**Theorem (Greither, Reploge, Rubin, Srivastav 1999)**
*$\mathbb{Q}$ is the only number field satisfying the H–S's thm*

- Martinet 1971 First example of $L/\mathbb{Q}$ tame not admitting a NIB

Let $F = \mathbb{Q}(\sqrt{5}, \sqrt{21})$, and $m = \frac{5+\sqrt{5}}{2}\frac{21+\sqrt{21}}{2}$

$$L_1 = F(\sqrt{m}) \qquad L_2 = F(\sqrt{-3m})$$

$$L_i/\mathbb{Q} \text{ tame, } \mathrm{Gal}(L_i/\mathbb{Q}) \cong Q_8$$

$L_1/\mathbb{Q}$ admits a NIB $\qquad$ $L_2/\mathbb{Q}$ does **not** admit a NIB

This example was very important and motivated Fröhlich's work on the locally free class group.

Since the 70's many authors worked on this topic in many directions: proving that tame extensions of a certain kind have a NIB, explicitly finding generators or giving counter examples.

# A result for Kummer extensions

Gómez Ayala '94, idc+L. Rossi '10-'13

$K$ number field, $\zeta_m \in K$, $L/K$ finite Kummer extension
Case $L/K$ cyclic: $L = K(\alpha)$, $\alpha = \sqrt[m]{a}$, $a \in \mathcal{O}_K$

$$a\mathcal{O}_K = \prod_{P \subset \mathcal{O}_K} P^{\nu_P(a)}$$

For $0 \leq i < m$ let

$$\mathcal{B}_i = \mathcal{B}_i(a) = \prod_{P \subset \mathcal{O}_K} P^{\left\lfloor \frac{\nu_P(a^i)}{m} \right\rfloor}$$

$\mathcal{B}_i$ is a sort of $m$-th root of $a^i\mathcal{O}_K$

### Theorem

*Let $L/K$ be a tame cyclic Kummer extension of degree $m$.*
*$L/K$ has a NIB $\iff \exists \alpha \in \mathcal{O}_L$ such that $L = K(\alpha)$, $\alpha^m = a \in \mathcal{O}_K$, and the following conditions hold:*

1. *$\mathcal{B}_i$ is principal for all $i$;*
2. *the congruence $\displaystyle\sum_{i=0}^{m-1} \frac{\alpha^i}{b_i} \equiv 0 \pmod{m}$ holds for some $b_i \in \mathcal{O}_K$, with $\mathcal{B}_i = b_i\mathcal{O}_K$.*

*In this case, the integer $\omega = \frac{1}{m}\displaystyle\sum_{i=0}^{m-1} \frac{\alpha^i}{b_i}$ generates $\mathcal{O}_L$ over $\mathcal{O}_K[G]$.*

**

PROOF: $\Leftarrow$ It is clear that $\mathcal{O}_K[G]\omega \subseteq \mathcal{O}_L$. To prove equality we have to show that $disc_{L/K}(\mathcal{O}_K[G]\omega) = disc_{L/K}(\mathcal{O}_L)$.

Let $G = \langle\sigma\rangle$ and let $\hat{G} = \langle\chi\rangle$, with $\chi(\sigma) = \zeta_m$,

$$disc_{L/K}\mathcal{O}_K[G]\omega = \prod_{i=0}^{m-1}(\omega|\chi^i)^2 = \prod_{i=0}^{m-1}\frac{\alpha^{2i}}{b_i^2} = \frac{a^{m-1}}{(\prod b_i)^2}$$
$$= \frac{\prod_{\mathcal{P}\subset\mathcal{O}_K}\mathcal{P}^{(m-1)ord_{\mathcal{P}}a}}{\prod_{\mathcal{P}\subset\mathcal{O}_K}\mathcal{P}^{2\sum_i[i\, ord_{\mathcal{P}}a/m]}} = \prod_{\mathcal{P}\subset\mathcal{O}_K}\mathcal{P}^{m-(m,ord_{\mathcal{P}}a)}.$$

$disc_{L/K}(\mathcal{O}_K[G]\omega) = \prod_{\mathcal{P}\subset\mathcal{O}_K}\mathcal{P}^{m-(m,ord_{\mathcal{P}}a)}$.

$$disc(L/K) = \prod_{\mathcal{P}\subset\mathcal{O}_K}\mathcal{P}^{m-m/e_{\mathcal{P}}}$$

where $e_{\mathcal{P}}$ is the ramification index of $\mathcal{P}$ in $L/K$.

## Lemma

*Let $L = K(\sqrt[m]{a})$ with $a \in \mathcal{O}_K$. Then, for any prime $\mathcal{P} \subset \mathcal{O}_K$ tamely ramified in $\mathcal{O}_L$, we have*

$$e_{\mathcal{P}} = \frac{m}{(m, ord_{\mathcal{P}}(a))}.$$

$disc(L/K) = \prod_{\mathcal{P}\subset\mathcal{O}_K}\mathcal{P}^{m-(m,ord_{\mathcal{P}}a)}$.

$\Rightarrow$ Assume that $L/K$ has a NIB generated by $\omega$ and let $\alpha$ be any Kummer generator of $L/K$. Then

$$\omega = \sum_{i=0}^{m-1} c_i \alpha^i, \text{ where } c_i \in K.$$

Using that $disc_{L/K}(\mathcal{O}_K[G]\omega) = disc(L/K)$ we get that $\omega$ has the required form and that the $\mathcal{B}_i$ are principal.

**Remark**

- The criterion does not depend on the integral Kummer generator of the extension
- It is not always possible to satisfy condition *2* of the Theorem, even under condition *1*.

# General Kummer extensions

$L/K$ be a Kummer extension of exponent $m$ ($\zeta_m \in K$).

- $L = K(\alpha_1, \ldots, \alpha_r) = K(\boldsymbol{\alpha})$;
- $a_j = \alpha_j^m \in \mathcal{O}_K$ for $j = 1, \ldots, r$;
- $[L : K] = \prod_{j=1}^{r} [K(\alpha_j) : K] = N$;

For $\mathbf{i} \in \mathbb{Z}_m^r$ define $\mathbf{a}^{\mathbf{i}} = a_1^{i_1} \ldots a_r^{i_r}$ and

$$\mathcal{B}_{\mathbf{i}} = \prod_{P \subset \mathcal{O}_K} P^{\lfloor \frac{\nu_P(\mathbf{a}^{\mathbf{i}})}{m} \rfloor}$$

$\mathcal{B}_{\mathbf{i}}$ the smallest ideal $\mathcal{I} \subset \mathcal{O}_K$ such that $\mathbf{a}^{\mathbf{i}}\mathcal{I}^{-m}$ is an integral ideal in $\mathcal{O}_K$.

top

### Theorem (IDC, L. Rossi)

*Let $L/K$ tamely ramified Kummer extension of exponent $m$ and degree $N$.*
*$L/K$ has a NIB if and only if $\iff \exists \boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_r) \in \mathcal{O}_L^r$ s.t. $L = K(\boldsymbol{\alpha})$, and the following conditions hold:*

1. *$\mathcal{B}_{\mathbf{i}}$ is principal for any $\mathbf{i}$;*
2. *the congruence*
$$\sum_{\mathbf{i}} \frac{\boldsymbol{\alpha}^{\mathbf{i}}}{b_{\mathbf{i}}} \equiv 0 \pmod{N}$$
*holds for some $b_{\mathbf{i}} \in \mathcal{O}_K$, with $\mathcal{B}_{\mathbf{i}} = b_{\mathbf{i}}\mathcal{O}_K$.*

*In this case, the integer $\omega = \frac{1}{N} \sum_{\mathbf{i}} \frac{\boldsymbol{\alpha}^{\mathbf{i}}}{b_{\mathbf{i}}}$ generates $\mathcal{O}_L$ over $\mathcal{O}_K[G]$. Namely, $\mathcal{O}_L = \mathcal{O}_K[G]\omega$.*

# The Steintz class

Let $L/K$ be a number fields extension, let $v_1, \ldots, v_n$ be an $K$-basis of $L$ and let $\mathcal{I}$ be the fractional ideal of $\mathcal{O}_F$ such that

$$disc(L/K) = \mathcal{I}^2 disc_{K/F}(v_1, \ldots, v_n).$$

The *Steinitz class* of $L/K$ is the class of $\mathcal{I}$ in $Cl(K)$

- it is well defined
- $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module $\iff$ $[\mathcal{I}] = [\mathcal{O}_K]$
- Recall that if $\mathcal{O}_L$ is free over $\mathcal{O}_K[G]$, then it is also free over $\mathcal{O}_K$

## Proposition

*Let $L/K$ be a tame Kummer extension of exponent $m$, $\mathbf{a} \in \mathcal{O}_K^r$ such that $L = K(\sqrt[m]{\mathbf{a}})$.*
*Then the Steinitz class of $L/K$ is the ideal class of $(\prod_{\mathbf{i} \in \mathbb{Z}_m^r} \mathcal{B}_{\mathbf{i}})^{-1}$.*

*Namely, $\mathcal{O}_L$ is free over $\mathcal{O}_K$ $\iff$ $\prod_{\mathbf{i} \in \mathbb{Z}_m^r} \mathcal{B}_{\mathbf{i}}$ is principal.*

# The case $\mathbb{Q}(\zeta_m, \sqrt[m]{a_i} | i = 1, \ldots, n)$ with $a_i \in \mathbb{Q}$

Case $K = \mathbb{Q}(\zeta_m)$, $L = K(\sqrt[m]{a}_1, \ldots, \sqrt[m]{a}_r)$ where $a_i \in \mathbb{Q}$.
Explicit tameness condition. $a \in \mathbb{Z}$ and $m = p_1^{n_1} \cdots p_s^{n_s}$ is odd
$\mathbb{Q}(\zeta_m, \sqrt[m]{a})/\mathbb{Q}(\zeta_m)$ with $(a, m) = 1$ is tame $\iff$

$$a^{p_j - 1} \equiv 1 \pmod{p_j^{n_j+1}} \text{ for all } j.$$

Existence of integral basis over $\mathcal{O}_K$. If $L/K$ is tame then it admits an integral basis.

Existence of a NIB over $\mathcal{O}_K$. Kawamoto ('85), Ichimura (2010):
$L/K$ cyclic, $m$ sqr-free, $(a, m) = 1$, then $L/K$ tame $\iff$ NIB.
The same is no more true for non-cyclic extensions.

Example. $\mathbb{Q}(\zeta_3, \sqrt[3]{10}, \sqrt[3]{46})/\mathbb{Q}(\zeta_3)$ is tame but has no NIB.
If in addition $(a_i, a_j) = 1$ for all $i \neq j \Rightarrow \exists$ NIB.

Thank you!