# Brauer relations and large class groups

Jean Gillibert (joint with Pierre Gillibert)

International Conference on Class Groups of Number Fields and Related Topics 2022, KSoM
November 21, 2022

# The general framework

- $K/\mathbb{Q}$: a Galois extension
- $G = \mathrm{Gal}(K/\mathbb{Q})$
- $\mathrm{Cl}(K)$: the ideal class group
- $h(K)$: the order of $\mathrm{Cl}(K)$

# The general framework

- $K/\mathbb{Q}$: a Galois extension
- $G = \mathrm{Gal}(K/\mathbb{Q})$
- $\mathrm{Cl}(K)$: the ideal class group
- $h(K)$: the order of $\mathrm{Cl}(K)$

**Basic fact:** $\mathrm{Cl}(K)$ has a natural action of $G$, which endows it with a $\mathbb{Z}[G]$-module structure.

## The general framework

- $K/\mathbb{Q}$: a Galois extension
- $G = \mathrm{Gal}(K/\mathbb{Q})$
- $\mathrm{Cl}(K)$: the ideal class group
- $h(K)$: the order of $\mathrm{Cl}(K)$

**Basic fact:** $\mathrm{Cl}(K)$ has a natural action of $G$, which endows it with a $\mathbb{Z}[G]$-module structure.

**Today's topic:** what kind of information about $\mathrm{Cl}(K)$ does this structure give?

# An example: dihedral extensions

Assume that $G = \mathrm{Gal}(K/\mathbb{Q})$ is the dihedral group of order $2p$, where $p$ is an odd prime. Write $G = \langle \sigma, \tau \rangle$ with relations $\sigma^p = 1 = \tau^2$, and $\sigma\tau = \tau\sigma^{-1}$.

It was proved by Halter-Koch in 1977 that

$$\frac{h(K)}{h(K^\sigma)h(K^\tau)^2} = \frac{[\mathcal{O}_K^\times : \mathcal{O}_{K^\sigma}^\times \mathcal{O}_{K^\tau}^\times \mathcal{O}_{K^{\sigma\tau}}^\times]}{p^{1+\epsilon}}$$

where $K^\mu$ denotes the subfield fixed by $\mu$, and $\epsilon$ is 0 (resp. 1) if $K^\sigma$ is imaginary (resp. real).

This is a special, explicit case of Brauer's class number relation.

## Dihedral extensions, continued

We have seen that $h(K) = h(K^\sigma)h(K^\tau)^2$ up to a power of $p$.

One may ask if there is some underlying isomorphism between (prime-to-$p$ parts) of the class groups. This was conjectured by Nehrkorn, and proved by Walter in 1979 using integral representation theory.

More precisely, the map induced by the norms

$$\mathrm{Cl}(K) \to \mathrm{Cl}(K^\sigma) \oplus \mathrm{Cl}(K^\tau) \oplus \mathrm{Cl}(K^{\sigma\tau})$$

has $p$-torsion kernel and cokernel. Note that $K^{\sigma\tau} \simeq K^\tau$.

## Remark on the $m$-rank of class groups

**Definition:** if $m > 1$ is an integer and $A$ is a finite abelian group, we denote by $\operatorname{rank}_m A$ the largest integer $r$ such that $A$ contains $(\mathbb{Z}/m\mathbb{Z})^r$ as a subgroup.

According to the previous discussion, if $p \nmid m$ then we have

$$\operatorname{rank}_m \operatorname{Cl}(K) = \operatorname{rank}_m \operatorname{Cl}(K^\sigma) + 2 \operatorname{rank}_m \operatorname{Cl}(K^\tau).$$

This is of particular interest in the quest for number fields whose class group has large $m$-rank.

## The case $D_6$ $(= \mathfrak{S}_3)$

In our previous work, we constucted a family of fields $K/\mathbb{Q}$ with Galois group $D_6$ such that

$$\operatorname{rank}_m \operatorname{Cl}(K^\sigma) \geq 1 \quad \text{and} \quad \operatorname{rank}_m \operatorname{Cl}(K^\tau) \geq 2.$$

Therefore, if $3 \nmid m$ we obtain

$$\operatorname{rank}_m \operatorname{Cl}(K) \geq 5.$$

In fact, our result holds for all $m$, and its proof does not require the use of the above formula.

The lower bound obtained is better than Nakano's one for general degree $n$ extensions, which is $\lfloor \frac{n}{2} \rfloor + 1$.

# A natural question

What kind of lower bound (on the $m$-rank of the class group) is it possible to obtain for fields $K/\mathbb{Q}$ with Galois group $\mathfrak{S}_n$?

According to Nakano, one can construct (non-Galois) fields $L/\mathbb{Q}$ of degree $n$ whose class group has $m$-rank $\lfloor \frac{n}{2} \rfloor + 1$. What if we take $K$ to be the Galois closure of $L$?

(Reminder: fields of degree $n$ have generically Galois closure with Galois group $\mathfrak{S}_n$).

# Brauer relations

Going back to the dihedral case, the relation between the class group of $K$ and those of its subfields can be explained by integral representation theory.

More precisely, we have the following Brauer relation in the dihedral group $G = D_{2p}$

$$\{1\} + 2D_{2p} = \langle\sigma\rangle + 2\langle\tau\rangle,$$

which means that we have an isomorphism of $\mathbb{Q}[G]$-modules

$$\mathbb{Q}[G] \oplus \mathbb{Q}^2 \simeq \mathbb{Q}[G/\langle\sigma\rangle] \oplus \mathbb{Q}[G/\langle\tau\rangle]^2.$$

# Integral version of the above isomorphism

One can check that the $\mathbb{Z}[G]$-module map

$$\begin{aligned} \varphi : \mathbb{Z}[G] \oplus \mathbb{Z}^2 &\longrightarrow \mathbb{Z}[G/\langle\sigma\rangle] \oplus \mathbb{Z}[G/\langle\tau\rangle] \oplus \mathbb{Z}[G/\langle\sigma\tau\rangle] \\ (m,0,0) &\longmapsto (m\langle\sigma\rangle, m\langle\tau\rangle, m\langle\sigma\tau\rangle) \\ (0,a,b) &\longmapsto (0, a\Sigma_{G/\langle\tau\rangle}, b\Sigma_{G/\langle\sigma\tau\rangle}) \end{aligned}$$

is injective, and has cokernel of order $p$.

In fact, one can construct a map $\varphi'$ in the other direction such that $\varphi \circ \varphi' = p$ and $\varphi' \circ \varphi = p$ (multiplication-by-$p$ map).

The map $m \mapsto m\langle\sigma\rangle$ is a "reduction map". There is a "lifting map" $\mathbb{Z}[G/\langle\sigma\rangle] \to \mathbb{Z}[G]$ defined by $g\langle\sigma\rangle \mapsto \sum_{i=0}^{p-1} g\sigma^i$. These two operations are the building blocks for maps between such modules.

# What is a permutation module?

A $\mathbb{Z}[G]$-Permutation module is a $\mathbb{Z}[G]$-module of the form $\mathbb{Z}[X]$, where $X$ is a finite set on which $G$ acts.

Such an $X$ can be written as a union of orbits. Each orbit is of the form $G/H$ (set of left cosets $gH$), where $H$ is some stabiliser.

So, any permutation module is a direct sum of modules of the form $\mathbb{Z}[G/H]$, where $H$ runs through subgroups of $G$.

Integral representation theory can be seen as the study of permutation modules.

# How is this related to class groups?

The assignement

$$F : \{\mathbb{Z}[G]\text{-Permutation modules}\} \longrightarrow \{\text{Abelian groups}\}$$
$$\mathbb{Z}[G/H] \longmapsto \mathrm{Cl}(K^H)$$

is an additive functor.

In particular, any relation between permutations modules yields a relation between class groups of subfields of $K$.

The "reduction map" $\mathbb{Z}[G] \to \mathbb{Z}[G/H]$ corresponds to the norm map $\mathrm{Cl}(K) \to \mathrm{Cl}(K^H)$. The "lifting map" $\mathbb{Z}[G/H] \to \mathbb{Z}[G]$ corresponds to the natural map $\mathrm{Cl}(K^H) \to \mathrm{Cl}(K)$.

# Functors are helpful

Going back to the dihedral case, the image of our permutation modules by the functor $F$ are

$$\mathbb{Z}[G] \oplus \mathbb{Z}^2 \longmapsto \mathrm{Cl}(K) \oplus \mathrm{Cl}(\mathbb{Q})^2$$

$$\mathbb{Z}[G/\langle\sigma\rangle] \oplus \mathbb{Z}[G/\langle\tau\rangle]^2 \longmapsto \mathrm{Cl}(K^\sigma) \oplus \mathrm{Cl}(K^\tau)^2$$

# Functors are helpful

Going back to the dihedral case, the image of our permutation modules by the functor $F$ are

$$\begin{array}{ccc} \mathbb{Z}[G] \oplus \mathbb{Z}^2 & \longmapsto & \mathrm{Cl}(K) \oplus \mathrm{Cl}(\mathbb{Q})^2 \\ \varphi \downarrow\uparrow \varphi' & & \\ \mathbb{Z}[G/\langle\sigma\rangle] \oplus \mathbb{Z}[G/\langle\tau\rangle]^2 & \longmapsto & \mathrm{Cl}(K^\sigma) \oplus \mathrm{Cl}(K^\tau)^2 \end{array}$$

In the source category, we have maps $\varphi$ and $\varphi'$ whose composite in both directions is multiplication by $p$.

# Functors are helpful

Going back to the dihedral case, the image of our permutation modules by the functor $F$ are

$$\begin{array}{ccc} \mathbb{Z}[G] \oplus \mathbb{Z}^2 & \longmapsto & \mathrm{Cl}(K) \oplus \mathrm{Cl}(\mathbb{Q})^2 \\ \varphi \downarrow\uparrow \varphi' & & F(\varphi) \downarrow\uparrow F(\varphi') \\ \mathbb{Z}[G/\langle\sigma\rangle] \oplus \mathbb{Z}[G/\langle\tau\rangle]^2 & \longmapsto & \mathrm{Cl}(K^\sigma) \oplus \mathrm{Cl}(K^\tau)^2 \end{array}$$

In the source category, we have maps $\varphi$ and $\varphi'$ whose composite in both directions is multiplication by $p$.

This yields maps $F(\varphi)$ and $F(\varphi')$ between (sums of) class groups which, by functoriality, have the same property. Hence, the kernel and cokernel of these maps are $p$-torsion groups.

## Revisiting Walter's proof

Walter's proof does not relies on functors, but on the following observation: for any subgroup $H$ of $G$, we have

$$\mathrm{Hom}_G(\mathbb{Z}[G/H], \mathrm{Cl}(K)) = \mathrm{Cl}(K)^H$$

and

$$\mathrm{Cl}(K)^H \otimes \mathbb{Z}\left[\frac{1}{2p}\right] = \mathrm{Cl}(K^H) \otimes \mathbb{Z}\left[\frac{1}{2p}\right]$$

The Brauer relation yields an isomorphism of $\mathbb{Z}\left[\frac{1}{2p}, G\right]$-modules, hence the result.

Gain from the functorial approach: finer control on primes one should invert ($p$ is enough), and information about the kernel and cokernel of the map (these are $p$-torsion).

# The Kani-Rosen decomposition theorem

Let $C$ be a smooth projective curve over a field $k$, and let $C$ be the Jacobian variety of $C$.

In 1989, Kani and Rosen proved that, if $G$ is a finite group of automorphisms of $C$, then certain Brauer relations in $G$ gives rise to a decomposition of the Jacobian $J(C)$ as the product of Jacobians of subcovers.

For example, if $D_{2p}$ acts on $C$ then we have

$$J(C) \times J(C/D_{2p})^2 \sim J(C/\langle\sigma\rangle) \times J(C/\langle\tau\rangle)^2,$$

where $\sim$ means the existence of an isogeny between these two abelian varieties.

# Revisiting the Kani-Rosen decomposition theorem

The assignement

$$F : \{\mathbb{Z}[G]\text{-Permutation modules}\} \longrightarrow \{\text{Abelian varieties}\}$$
$$\mathbb{Z}[G/H] \longmapsto J(C/H)$$

is an additive functor.

In particular, any relation between permutations modules yields a relation between Jacobians of subcovers of $C$.

One recovers the Kani-Rosen theorem, with a small refinement: in the dihedral case described above, there exists an isogeny whose kernel is $p$-torsion.

# Another use of Brauer relations: BSD conjecture

Let $E$ be an elliptic curve over $\mathbb{Q}$, and let $K/\mathbb{Q}$ with group $G$.

Like the class group, the Selmer group and the Tate-Shafarevich group of $E$ behave nicely with respect to subfields of $K$. The $L$-function behaves even better: its residue at $s = 1$ is multiplicative under Brauer relations. More precisely, the map

$$\begin{aligned} \{\mathbb{Q}[G]\text{-Permutation modules}\} &\longrightarrow (\mathbb{Q}^\times, \times) \\ \mathbb{Q}[G/H] &\longmapsto \mathrm{res}_{s=1} L(E/K^H, s) \end{aligned}$$

turns direct sums into products.

In 2009 and 2010, Tim and Vladimir Dokchitser used this to make progress towards the Birch and Swinnerton-Dyer conjecture.

# General strategy

Let $K/\mathbb{Q}$ be a Galois extensions with group $G$. In order to establish "nice" relations between the class group of $K$ and those of its subfields, we need two ingredients:

- a Brauer relation in $G$
- an integral version of this Brauer relation

# General strategy

Let $K/\mathbb{Q}$ be a Galois extensions with group $G$. In order to establish "nice" relations between the class group of $K$ and those of its subfields, we need two ingredients:

- a Brauer relation in $G$
- an integral version of this Brauer relation

What do we mean by "integral version"?

# Integral Brauer relations

A result of Maranda (1955): given a $\mathbb{Q}[G]$-isomorphism

$$\bigoplus_{i\in I} \mathbb{Q}[G/H_i] \simeq \bigoplus_{j\in J} \mathbb{Q}[G/K_j]$$

one can find a $\mathbb{Z}[G]$-morphism

$$\varphi : \bigoplus_{i\in I} \mathbb{Z}[G/H_i] \longrightarrow \bigoplus_{j\in J} \mathbb{Z}[G/K_j]$$

which becomes an isomorphism after tensoring by $\mathbb{Z}\left[\frac{1}{|G|}\right]$.

# Integral Brauer relations

A result of Maranda (1955): given a $\mathbb{Q}[G]$-isomorphism

$$\bigoplus_{i\in I} \mathbb{Q}[G/H_i] \simeq \bigoplus_{j\in J} \mathbb{Q}[G/K_j]$$

one can find a $\mathbb{Z}[G]$-morphism

$$\varphi : \bigoplus_{i\in I} \mathbb{Z}[G/H_i] \longrightarrow \bigoplus_{j\in J} \mathbb{Z}[G/K_j]$$

which becomes an isomorphism after tensoring by $\mathbb{Z}\left[\frac{1}{|G|}\right]$. Such a map is injective (for obvious reasons) and has $d$-torsion cokernel for some $d$ whose prime factors divide $|G|$. So, we have a map $\varphi'$ in the other direction satisfying $\varphi \circ \varphi' = d$ and $\varphi' \circ \varphi = d$. Thus, if $F$ is an additive functor, $F(\varphi)$ has $d$-torsion kernel and cokernel.

# Facts about Brauer relations

What kind of Brauer relations can one find in general?

- cyclic groups don't have Brauer relations.
- non-cyclic groups always do.
- in 2015, Bartel and Dokchitser gave a classification of all Brauer relations in all finite groups. These can be deduced from some explicit list of primitive relations.

# Symmetric groups

Let $L/\mathbb{Q}$ be an extension of degree $n$, whose Galois closure $K/\mathbb{Q}$ has Galois group $\mathfrak{S}_n$. Then $L$ has $n$ conjugates, corresponding to the $n$ stabilizers of one element in $\mathfrak{S}_n$. It is tempting to relate the class group of $K$ with that of these subfields.

The case of $\mathfrak{S}_3(= D_6)$ has been seen previously.

For $n \geq 4$, there is no Brauer relation in $\mathfrak{S}_n$ which allows to do this. This follows from the result of Bartel and Dokchitser.

# Symmetric groups

Let $L/\mathbb{Q}$ be an extension of degree $n$, whose Galois closure $K/\mathbb{Q}$ has Galois group $\mathfrak{S}_n$. Then $L$ has $n$ conjugates, corresponding to the $n$ stabilizers of one element in $\mathfrak{S}_n$. It is tempting to relate the class group of $K$ with that of these subfields.

The case of $\mathfrak{S}_3 (= D_6)$ has been seen previously.

For $n \geq 4$, there is no Brauer relation in $\mathfrak{S}_n$ which allows to do this. This follows from the result of Bartel and Dokchitser.

**Question:** does there exist a weaker relation that a Brauer one?

# A map in the symmetric case

**Theorem**

*Let $n > 1$ and let $G = \mathfrak{S}_n$ be the symmetric group over the set $\{0, \ldots, n-1\}$. We let $\sigma = (0 \ldots n-1)$ a cycle of length $n$, and for $i = 0, \ldots, n-1$ we denote by $H_i$ the stabilizer of $i$.*

*Then the morphism of $\mathbb{Z}[G]$-modules defined by*

$$\begin{aligned} \varphi : \mathbb{Z}[G] \oplus \mathbb{Z}^{n-1} &\longrightarrow \mathbb{Z}[G/\langle\sigma\rangle] \oplus \bigoplus_{i=1}^{n-1} \mathbb{Z}[G/H_i] \\ (m, (0)) &\longmapsto (m\langle\sigma\rangle, mH_1, \ldots, mH_{n-1}) \\ (0, (n_i)_{i=1}^{n-1}) &\longmapsto (0, (n_i \Sigma_{G/H_i})_{i=1}^{n-1}) \end{aligned}$$

*has cokernel a $n(n-2)!$-torsion group.*

# The map $\varphi'$ in the other direction

In order to derive information from $\varphi$, it would be nice to find a map $\varphi'$ in the other direction such that $\varphi \circ \varphi' = n(n-2)!$.

Unfortunately, the computations are intricate and it seems tricky to construct such a map $\varphi'$. In fact, it may not exist. Nevertheless, we prove the following

## Lemma

*Let $\varphi : M \to N$ be a morphism of $\mathbb{Z}[G]$-permutation modules, whose cokernel is $d$-torsion. Then there exists a morphism $\varphi' : N \to M$ such that $\varphi \circ \varphi' = d\,|G|$.*

This follows from the fact that short exact sequences of $\mathbb{Z}[G]$-modules split after multiplication by $|G|$.

# The relation we were looking for

By the Lemma, there exist $\varphi'$ such that $\varphi \circ \varphi' = n!n(n-2)!$.

It follows from the functorial machinery that, if $L/\mathbb{Q}$ is an extension of degree $n$ whose Galois closure $K/\mathbb{Q}$ has Galois group $\mathfrak{S}_n$, then there exist a map

$$\mathrm{Cl}(K) \longrightarrow \mathrm{Cl}(K^\sigma) \oplus \mathrm{Cl}(L)^{n-1}$$

whose cokernel is $n!n(n-2)!$-torsion (here, $\sigma$ denotes any cycle of length $n$). In particular, letting $d := n!n(n-2)!$ we have

$$\mathrm{rank}_m \mathrm{Cl}(K) \geq \mathrm{rank}_{dm} \mathrm{Cl}(K^\sigma) + (n-1)\,\mathrm{rank}_{dm} \mathrm{Cl}(L).$$

# A variant of Nakano's construction

Let $q_1, \ldots, q_d$ be pairwise distinct nonzero integers such that, for all $k \in \{1, \ldots, d\}$, $(q_k, 1 + (-1)^{d-1} \prod_{i \neq k} q_i^m) = 1$.

Let $\Delta_0$ be an integer such that all primes dividing one of the $q_i$, or $q_i^m - q_j^m$ for some $i \neq j$ also divide $\Delta_0$. Let $t \in \mathbb{Z}$, and let $x$ be an algebraic number satisfying the equation

$$x(1 + t\Delta_0)^m + \prod_{i=1}^{d} (x - q_i^m) = 0.$$

Then for $i \in \{1, \ldots, d\}$ the numbers $x - q_i^m$ are $m$-th powers of ideal classes in $\mathbb{Q}(x)$.

We let

$$q_i = \begin{cases} t_i t_{i+1} & \text{for } i = 1, \dots n-1 \\ t_{n-1} t_n t_1 & \text{for } i = n \end{cases} \quad \text{and} \quad \Delta_0 = \prod_{i<j} (q_i^m - q_j^m)$$

Then:

- the Galois extension of $\mathbb{Q}(t_0, t_1, \dots, t_n)$ obtained by splitting the polynomial in the variable $x$

$$x(1 + t_0 \Delta_0)^m + \prod_{i=1}^{n} (x - q_i^m)$$

  has Galois group the symmetric group $\mathfrak{S}_n$.
- for any specialization of $(t_1, \dots, t_n)$ in $\mathbb{Z}^n$, the assumptions of the previous slide are satisfied by the $q_i$ and $\Delta_0$.

Applying Hilbert's irreducibility theorem while controlling the signature of $\mathbb{Q}(x)$ yields the existence of infinitely many values of $(t_0, t_1, \ldots, t_n) \in \mathbb{Z}^{n+1}$ for which the class group of $\mathbb{Q}(x)$ has $m$-rank at least $\lfloor \frac{n}{2} \rfloor + 1$. Thus we obtain:

### Theorem

*Let $m > 1$ and $n > 1$ be two integers. Then there exists infinitely many, pairwise linearly disjoint, Galois extensions $K/\mathbb{Q}$ with* $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathfrak{S}_n$ *such that*

$$\mathrm{rank}_m \, \mathrm{Cl}(K) \geq (n-1) \times \left( \left\lfloor \frac{n}{2} \right\rfloor + 1 \right).$$

For $n = 3$ the lower bound is 4 (same as Nakano's), but using another family we achived 5 in our previous paper.

In general the bound above is smaller than Nakano's one ($\lfloor \frac{n!}{2} \rfloor + 1$), but the fields obtained are Galois extensions of $\mathbb{Q}$.

Thank you for your attention!