Units of group algebras and automorphism groups

Florian Eisele

City, University of London

June 2021

Units in group rings

- R: commutative ring
- G: finite group

Question (Brauer)

To what extent does RG determine G?

A more precise version of this question: Isomorphism Problem (Higman)

Does $\mathbb{Z}G \cong \mathbb{Z}H$ imply $G \cong H$? *True for: G nilpotent, G metabelian, ...*

Unit groups: $\mathcal{U}(RG) = \{ \text{ units in } RG \}$

- $\mathcal{U}(RG)$ trivially contains G and $\mathcal{U}(R)$, but $\mathcal{U}(RG)$ is much bigger (for $R = \mathbb{Z}$ it is an arithmetic group).
- $\mathcal{U}(RG)$ is an invariant of the ring RG, and it is natural to consider it when trying to answer Brauer's question.

Zassenhaus made three strong conjectures on the finite subgroups of $\mathcal{U}(\mathbb{Z}G)$, which would allow us to recover G from $\mathcal{U}(\mathbb{Z}G)$.

What do we know about $\mathcal{U}(\mathbb{Z}G)$ for finite groups G?

- $\mathcal{U}(\mathbb{Z}G)$ is finitely presented.
- However, presentations are hard to come by, except in small examples. E.g.

$$\begin{array}{rcl} S_3 & = & \langle t, y \mid t^3 = 1,\ y^2 = 1,\ {}^y t = t^{-1} \rangle \\ \cap & & \\ \mathcal{U}(\mathbb{Z}S_3) & = & \langle t, y, v \mid t^3 = 1,\ y^2 = 1,\ {}^y t = t^{-1},\ {}^y v = v^{-1} \rangle \\ & \cong & (C_3 * C_\infty) \rtimes C_2 \quad (\text{“}*\text{”} = \text{free product}) \end{array}$$

  where $v = 1 + (1 - y) \cdot t \cdot (1 + y) \in \mathcal{U}(\mathbb{Z}S_3)$.
- Even finding generators is an impossible task in almost all cases. $\rightsquigarrow$ other methods required.
- There are units of finite order which are not conjugate to group elements (up to sign). In the above example: $v \cdot y$ has order two.

The Zassenhaus conjectures

How to get rid of units of R

- **Augmentation map:** $\varepsilon : RG \longrightarrow R : \sum_{g\in G} r_g \cdot g \mapsto \sum_{g\in G} r_g$,
- **Normalised units:** $V(RG) = \{u \in \mathcal{U}(RG) \mid \varepsilon(u) = 1\}$.

We get a decomposition

$$\mathcal{U}(RG) = V(RG) \times \mathcal{U}(R).$$

The conjectures

$$\begin{array}{ll}
\text{(IP):} & \mathbb{Z}G \cong \mathbb{Z}H \Longrightarrow G \cong H \\
\Uparrow & \\
\text{(ZC2):} & H \leqslant V(\mathbb{Z}G) \text{ and } |H| = |G| \Longrightarrow aHa^{-1} = G \text{ for some } a \in \mathcal{U}(\mathbb{Q}G) \\
\Uparrow & \\
\text{(ZC3):} & H \leqslant V(\mathbb{Z}G) \text{ finite} \Longrightarrow aHa^{-1} \subseteq G \text{ for some } a \in \mathcal{U}(\mathbb{Q}G) \\
\Downarrow & \\
\textbf{(ZC1):} & H \leqslant V(\mathbb{Z}G) \text{ finite and cyclic} \Longrightarrow aHa^{-1} \subseteq G \text{ for some } a \in \mathcal{U}(\mathbb{Q}G)
\end{array}$$

Roggenkamp & Scott: counterexample to (ZC2). Hertweck: counterexample to (IP). Hence, (IP), (ZC3) and (ZC2) are all **false in general**.

What about (ZC1), the first Zassenhaus conjecture?

(ZC1) reformulated

If $u \in \mathcal{U}(\mathbb{Z}G)$ has finite order, then $aua^{-1} = \pm g$ for some $g \in G$ and $a \in \mathcal{U}(\mathbb{Q}G)$.

Remark

(ZC1) is a conjecture about **individual units**.
The counterexamples to (ZC2) and (IP) are unexpected finite subgroups of $V(\mathbb{Z}G)$, but each element of these subgroups satisfies (ZC1).

The conjecture (ZC1) is true for a certain classes of groups G. But

Theorem (E-Margolis, 2018)

Let $n \in \mathbb{N}$ be arbitrary. There is a finite group

$$G = ((Z/p\mathbb{Z})^2 \times (\mathbb{Z}/q\mathbb{Z})^2) \rtimes A \quad \text{for primes } p, q \text{ and an abelian group } A$$

such that $\mathbb{Z}G$ has least n different $\mathcal{U}(\mathbb{Q}G)$-conjugacy classes of elements of order $p \cdot q$ not conjugate to an element of $\pm G$.

This contradicts (ZC1).

So there are more units than expected. What could still be true?

- All mentioned counter-examples (not only to (ZC1), but also (ZC2) and (IP)) involve units whose order is divisible by at least two primes.
- What about units in $\mathbb{Z}G$ of p-power order?
  Is any finite p-subgroup of $V(\mathbb{Z}G)$ isomorphic to a subgroup of G?
- We can replace $\mathbb{Z}$ by the p-adic integers $\mathbb{Z}_p$ and ask the same.
  Is any finite p-subgroup of $V(\mathbb{Z}_pG)$ isomorphic to a subgroup of G? (this is obviously false for non-p-subgroups)
- Subgroups $H \leqslant V(RG)$ correspond to certain $R(G \times H)$-modules (later).
  For a p-local ring R, e.g. $R = \mathbb{Z}_p$, are these modules trivial source?

In modular representation theory we replace RG by a "block" and Sylow p-subgroups of G by "defect groups", and the following is very interesting:

Scott's defect group problem (1990)

Let B and C be blocks of $\mathbb{Z}_pG$ and $\mathbb{Z}_pH$ for finite groups G and H. If $B \cong C$, does a suitably normalised isomorphism

$$B \xrightarrow{\sim} C$$

take the defect groups of B to conjugates of those of C?

So what next?

- We should look at p-subgroups and/or p-local coefficient rings.
- I will talk about the latter, that is, p-local coefficient rings.
- I will talk about more recent problems surrounding automorphism groups of group algebras.
- These problems are related to (ZC2), but also to a theorem of Weiss which settled (IP) for p-groups.
- These problems also have applications to the modular representation theory of finite groups.

Automorphism groups and Picard groups

General fact: (bi)modules and homomorphisms $H \longrightarrow \mathcal{U}(RG)$

Let G and H be finite groups, R any commutative ring. There is a bijection

$$\mathrm{Hom}(H,\mathcal{U}(RG))/\mathrm{conj.} \longleftrightarrow \{\ R(G\times H)\text{-modules } M \text{ s.t. } M|_G \cong RG\ \}/\mathrm{iso.}$$

- We also think of $R(G \times H)$-modules as RG-RH-bimodules.
- The **outer automorphism group** of the R-algebra RG is

$$\mathrm{Out}_R(RG) = \mathrm{Aut}_R(RG)/\mathrm{Inn}(RG),$$

which corresponds to

$$\{\ R(G\times G)\text{-modules } M \text{ s.t. } M|_{G\times 1} \text{ and } M|_{1\times G} \text{ both free of rank one }\}.$$

- Composition of automorphisms corresponds to a tensor product "$-\otimes_{RG}=$".
- The **Picard group** of RG consists of

$$\{\ \text{invertible } RG\text{-}RG\text{-bimodules } M\ \}.$$

- We also have a group Outcent(RG) of outer automorphisms trivial on $Z(RG)$, as well as a group Picent(RG).

Automorphisms and (ZC2)

We saw that "(ZC2)" would imply "(IP)". The opposite implication relies on the following:

The property (AUT) (conjecture disproved by Roggenkamp and Scott)

We say a finite group G satisfies (AUT) if

$$\mathrm{Aut}(\mathbb{Z}G) \subseteq \mathrm{Aut}(G) \cdot \mathrm{Inn}(\mathbb{Q}G).$$

This constrains the structure of $\mathrm{Out}(\mathbb{Z}G)$.

(IP) + (AUT) $\Longrightarrow$ (ZC2)

If a finite group G satisfies (AUT) and it satisfies (IP), i.e.

$$\mathbb{Z}G \cong \mathbb{Z}H \Longrightarrow G \cong H, \text{ for any finite group } H,$$

then G satisfies (ZC2), i.e.

$$H \leqslant V(\mathbb{Z}G) \text{ with } |H| = |G| \implies G \text{ and } H \text{ are conjugate in } \mathcal{U}(\mathbb{Q}G).$$

But we know that some finite groups fail to satisfy (IP), (ZC2) and/or (AUT).
So: In what other ways can we constrain outer automorphism groups?

Working over p-local rings

By $\mathbb{Z}_p$ we denote the p-adic integers (for any prime $p > 0$).

Local-glocal approach

- The elements of $\mathrm{Pic}(\mathbb{Z}G)$ and $\mathrm{Out}(\mathbb{Z}G)$ correspond to certain $\mathbb{Z}(G \times G)$-modules. As with (ZC1), (ZC2), ..., we can look at $\mathbb{Z}_p(G \times G)$-modules first.
- A partial "local-global principle" in this case is given by Fröhlich's localisation sequence:

$$1 \longrightarrow \mathrm{Picent}(Z(\mathbb{Z}G)) \longrightarrow \mathrm{Picent}(\mathbb{Z}G) \longrightarrow \prod_p \mathrm{Picent}(\mathbb{Z}_p G) \longrightarrow 1$$

So it makes sense to consider outer automorphism groups, Picard groups etc. over $\mathbb{Z}_p$ for different p. But also over $\mathcal{O}$:

Definition

Fix a prime $p > 0$. By $\mathcal{O}$ we denote a complete discrete valuation ring such that

- $\mathcal{O}$ has characteristic zero,
- $F = \mathcal{O}/p\mathcal{O}$ is algebraically closed of characteristic p.

Note that $\mathcal{O} \supseteq \mathbb{Z}_p$. This coefficient ring is used in modular representation theory.

Questions about $\mathrm{Out}_{\mathcal{O}}(\mathcal{O}G)$ and Picard groups

- For any finite group G we have

$$\mathrm{Picent}(\mathcal{O}G) = \mathrm{Outcent}(\mathcal{O}G) \leqslant \mathrm{Out}_{\mathcal{O}}(\mathcal{O}G) \leqslant \mathrm{Pic}_{\mathcal{O}}(\mathcal{O}G).$$

  All of these inclusions are of finite index.
  But: **the structure of these groups is/was unclear**.
- If we replace $\mathcal{O}$ by $\mathbb{Z}_p$, all of the above groups are finite (Jordan-Zassenhaus).

Questions (Boltje-Kessar-Linckelmann 2018)

- Is every element of $\mathrm{Pic}_{\mathcal{O}}(\mathcal{O}G)$ represented by a $\mathcal{O}(G \times G)$-module with endo-permutation source? We can ask this for $\mathbb{Z}_p$ instead of $\mathcal{O}$ as well.
- Is $\mathrm{Pic}_{\mathcal{O}}(\mathcal{O}G)$ finite? This would be trivial over $\mathbb{Z}_p$, and would be implied by a positive answer to the first question.

Reformulation of the second question in terms of unit groups

Are there only finitely many conjugacy classes of embeddings $G \hookrightarrow \mathcal{U}(\mathcal{O}G)$?

Motivation

- These questions have applications in modular representation theory, in particular to the classification of blocks and Donovan's conjecture.
- The first question might have implications for (ZC2).

What do $\mathcal{O}$ and $\mathbb{Z}_p$ look like?

Let F be any perfect field of characteristic $p > 0$.

Witt vectors

Define

$$W(F) = \prod_{\mathbb{Z}_{\geqslant 0}} F \quad \text{(called the ring of Witt vectors)}$$

There are polynomials $\sigma_i, \mu_i \in F[x_0, \ldots, x_i, y_0, \ldots y_i]$ for $i \in \mathbb{Z}_{\geqslant 0}$ such that setting

$$(v + w)_i := \sigma_i(v_0, \ldots, v_i, w_0, \ldots, w_i) \text{ and } (v \cdot w)_i := \mu_i(v_0, \ldots, v_i, w_0, \ldots, w_i)$$

turn $W(F)$ into a complete discrete valuation ring of char. 0 with $W(F)/pW(F) = F$.

Example: $W(\mathbb{F}_p) \cong \mathbb{Z}_p$ (the ring of p-adic integers). We can pick $\mathcal{O} = W(\bar{\mathbb{F}}_p)$.

Easy consequences

- $W(F)/p^n W(F)$ is isomorphic to the projection of $W(F)$ to the first n components (i.e. F^n, also called "truncated Witt vectors"). The ring operations are still given by polynomials.
- $\mathrm{GL}_r(\mathcal{O}/p^n\mathcal{O})$ is an affine algebraic group ($r, n \in \mathbb{N}$).
- $\mathrm{Aut}_{\mathcal{O}}(\mathcal{O}G/p^n\mathcal{O}G)$ and $\mathrm{Out}_{\mathcal{O}}(\mathcal{O}G/p^n\mathcal{O}G)$ are affine algebraic groups over F (same is true for arbitrary "$\mathcal{O}$-orders", not just $\mathcal{O}G$).

The structure of $\mathrm{Out}_{\mathcal{O}}(\mathcal{O}G)$

A corollary of Maranda's theorem

$\mathrm{Out}_{\mathcal{O}}(\mathcal{O}G)$ embeds into $\mathrm{Out}_{\mathcal{O}}(\mathcal{O}G/p^n\mathcal{O}G)$ for n big enough.

A variation of a theorem of Higman

Assume n is big enough. If an automorphism of $\mathcal{O}G/p^{n+1}\mathcal{O}G$ lifts to an automorphism of $\mathcal{O}G/p^{2n+1}\mathcal{O}G$, then it lifts to an automorphism of $\mathcal{O}G$.

Theorem (E 2018)

For n big enough we have

$$\mathrm{Out}_{\mathcal{O}}(\mathcal{O}G) \cong \mathrm{Im}(\mathrm{Out}_{\mathcal{O}}(\mathcal{O}G/p^{2n+1}\mathcal{O}G) \longrightarrow \mathrm{Out}_{\mathcal{O}}(\mathcal{O}G/p^{n+1}\mathcal{O}G))$$

Corollary (E 2018)

$\mathrm{Pic}_{\mathcal{O}}(\mathcal{O}G)$ and $\mathrm{Out}_{\mathcal{O}}(\mathcal{O}G)$ are affine algebraic groups over $F = \mathcal{O}/p\mathcal{O}$.

Everything on this slide works if we replace $\mathcal{O}G$ by an *$\mathcal{O}$-order in a semisimple algebra*. But for $\mathcal{O}G$ an even stronger assertion should be true.

What about the finiteness question?

The situation over a field $F = \bar{F}$

For a finite-dimensional F-algebra A

- $\mathrm{Out}_F(A)$ is an algebraic group.
- We have an embedding

$$\mathrm{Lie}(\mathrm{Out}_F(A)) \hookrightarrow HH^1(A)$$

Hence the dimension of $\mathrm{Out}_F(A)$ is bounded by the dimension of $HH^1(A)$.

We know that in general that

$$HH^1(\mathcal{O}G) = 0$$

for any finite group G.
The analogous statement for FG is wrong, and $\mathrm{Out}_F(FG)$ is usually an algebraic group of dimension > 0.

Idea

If the Lie algebra of $\mathrm{Out}_{\mathcal{O}}(\mathcal{O}G)$ and $HH^1(\mathcal{O}G)$ are related in a similar way, then $\mathrm{Out}_{\mathcal{O}}(\mathcal{O}G)$ should be finite.

A finiteness theorem

The idea from the previous slide leads to the following:

Theorem (E 2019)

$\mathrm{Pic}_{\mathcal{O}}(\mathcal{O}G)$ and $\mathrm{Out}_{\mathcal{O}}(\mathcal{O}G)$ are finite groups.

Reformulation in terms of unit groups

There are only finitely many conjugacy classes of embeddings $G \hookrightarrow \mathcal{U}(\mathcal{O}G)$. Or:

$$[N_{\mathcal{U}(KG)}(\mathcal{U}(\mathcal{O}G)) \ : \ \mathcal{U}(\mathcal{O}G)] < \infty$$

- In general, the theorem above is the strongest statement known at the moment.
- If G has a normal Sylow p-subgroup, then a theorem of Weiss implies that the elements of $\mathrm{Outcent}(\mathcal{O}G)$ are represented by trivial source modules.
- In that case $\mathrm{Pic}_{\mathcal{O}}(\mathcal{O}G)$ is automatically finite, and this was already observed by Boltje, Kessar and Linckelmann.
- For some groups with normal Sylow p-subgroups (or blocks with normal defect group) we know that $\mathrm{Pic}_{\mathcal{O}}(\mathcal{O}G)$ consists of elements represented by linear source bimodules (Livesey-Marchi).

Future research

Question (from earlier, still open)

Are all elements of $\mathrm{Out}_{\mathcal{O}}(\mathcal{O}G)$ and $\mathrm{Pic}_{\mathcal{O}}(\mathcal{O}G)$ represented by elements of endo-permutation source?

This is non-trivial even if we replace $\mathcal{O}$ by $\mathbb{Z}_p$.

- This question pops up in modular representation theory, in particular in the context of Donovan's conjecture.
- A lot of the work by Cliff, Weiss, Roggenkamp and Scott related to the Zassenhaus conjectures applies to this problem.
- We can ask in the context of the Zassenhaus conjectures: Counterexamples correspond to certain $\mathbb{Z}(G \times H)$-modules, where G and H depend on which Zassenhaus conjecture we are looking at. Do these modules become endo-permutation or even trivial source modules over $\mathbb{Z}_p$?
- For small groups one can determine all lattices with a given character computationally. Can one construct units or automorphisms violating the questions above?

Thank you for your attention!