A counterexample to the first Zassenhaus Conjecture

Leo Margolis

jt. F. Eisele

Free University of Brussels

June 7th, 2021

The group ring

Denote by G a *finite* group, by R a commutative ring, by RG the *group ring* of G over R:

$$RG = \left\{ \sum_{g \in G} r_g g \mid r_g \in R \right\}$$

is the free R-module with basis G where multiplication is extended distributively from G.

Let $U(RG)$ be the unit group in RG.
Trivial units: $\{rg \mid r \in U(R), g \in G\}$

Guiding Question

How far are finite subgroups of $U(RG)$ from being trivial?

It began with Higman

Naturally $R = \mathbb{Z}$ is the most restrictive case, as $RG = R \otimes_{\mathbb{Z}} \mathbb{Z}G$.

G. Higman 1940

- If G abelian, then any finite subgroup of $U(\mathbb{Z}G)$ is trivial.
- This is not true for $G = S_3$.
- Is any finite subgroup of $U(\mathbb{Z}G)$ isomorphic to a subgroup of trivial units?

Hertweck 1998

No. There are non-isomorphic groups G and H of order $2^{21}97^{28}$ s.t. $\mathbb{Z}G \cong \mathbb{Z}H$.

Normalized Units

The *augmentation map* is

$$\varepsilon : RG \to R, \sum_{g \in G} r_g g \mapsto \sum_{g \in G} r_g.$$

Let $V(RG)$ the units of augmentation 1 aka *normalized units*.
$\rightsquigarrow$ $U(RG) \cong U(R) \times V(RG)$.

Basic facts:

- For $H \leq V(\mathbb{Z}G)$ finite, we have $|H| \mid |G|$.
- Exponents of G and $V(\mathbb{Z}G)$ coincide.

$\rightsquigarrow$ The arithmetic reflection of G in $U(\mathbb{Z}G)$ is captured much better by $V(\mathbb{Z}G)$.

The Zassenhaus Conjectures

We call $H, K \leq V(\mathbb{Z}G)$ *rationally conjugate* if there exists $u \in U(\mathbb{Q}G)$ such that $u^{-1}Hu = K$.

The Zassenhaus Conjectures, 1970's

(ZC1): Any $u \in V(\mathbb{Z}G)$ of finite order is rationally conjugate to a trivial unit.

(ZC2): Any $H \leq V(\mathbb{Z}G)$ s.t. $|H| = |G|$ is rationally conjugate to G.

(ZC3): Any $H \leq V(\mathbb{Z}G)$ of finite order is rationally conjugate to a trivial subgroup.

The Zassenhaus Conjectures

The Zassenhaus Conjectures, 1970's

(ZC1): Any $u \in V(\mathbb{Z}G)$ of finite order is rationally conjugate to a trivial unit.
(ZC2): Any $H \leq V(\mathbb{Z}G)$ s.t. $|H| = |G|$ is rationally conjugate to G.
(ZC3): Any $H \leq V(\mathbb{Z}G)$ of finite order is rationally conjugate to a trivial subgroup.

Results

- (ZC2) is true for G nilpotent, but wrong in general (Roggenkamp-Scott late 1980's)
- (ZC3) is true for G nilpotent (Weiss 1991)
- (ZC1) is true for G cyclic-by-abelian; Sylow-by-abelian; of order less than 160; isomorphic to $\mathrm{PSL}(2, q)$ for $q \leq 25$ or Fermat or Mersenne prime

The counterexample

Eisele-M' 2018

Let p and q primes, $N = C_{pq} \times C_{pq}$, d a divisor of $p-1$ and $q-1$, $A = C_{\frac{p^2-1}{d}} \times C_{q^2-1}$.

- For $p = 7$, $q = 19$, $d = 3$ there is $G = N \rtimes A$ s.t. $V(\mathbb{Z}G)$ contains a unit of order pq not rationally conjugate to any trivial unit.
- For any $m \in \mathbb{Z}_{>0}$ there are p and q big enough such that there is $G = N \rtimes A$ and m units of order pq in $V(\mathbb{Z}G)$ not rationally conjugate to a trivial unit or each other.

Still open - conjugation

(ZC3) for p-groups

Is (ZC3) true if H is a p-group?

Kimmerle Problem (KP)

Is any $u \in V(\mathbb{Z}G)$ of finite order conjugate in $V(\mathbb{Q}K)$ to a trivial unit, for some $G \leq K$?

(KP) can be formulated in a more approachable, but also more technical, way.

Still open - orders

Spectrum Problem (SP)

If there is $u \in V(\mathbb{Z}G)$ of order n, is there $g \in G$ of order n?

Prime Graph Question (PQ)

Let p and q primes. If there is $u \in V(\mathbb{Z}G)$ of order pq, is there $g \in G$ of order pq?

Kimmerle-Konovalov '13

(PQ) has a positive answer for G if it has a positive answer for all almost simple images of G.

$\rightsquigarrow$ Use Classification of Finite Simple Groups?

Caicedo-M' '20

If the Sylow p-subgroup of G has order p, then $V(\mathbb{Z}G)$ contains an element of order pq if and only if G does.

What we know today

	Abelian	Nilpotent	Metabelian	Supersol'	solvable	Any
(TU)	✓	✗	✗	✗	✗	✗
(ZC1)	✓	✓	✗	?	✗	✗
(KP)	✓	✓	✓	✓	?	?
(SP)	✓	✓	✓	✓	✓	?
(PQ)	✓	✓	✓	✓	✓	?

Reformulating (ZC1) - Partial augmentations

First Zassenhaus Conjecture (ZC1)

Any $u \in V(\mathbb{Z}G)$ of finite order is conjugate in $U(\mathbb{Q}G)$ to a trivial unit.

Let $u = \sum_{g \in G} r_g g \in U(RG)$ of order k and x^G a conjugacy class in G.

$$\varepsilon_x(u) = \sum_{g \in x^G} r_g$$

is the *partial augmentation* of u at x.

Marciniak-Ritter-Sehgal-Weiss/Luthar-Passi

$u \in V(\mathbb{Z}G)$ is rationally conjugate to a trivial unit if and only if $\varepsilon_x(u^d) \geq 0$ for all $x \in G, d \in \mathbb{Z}$.

The partial augmentations of units of finite order are a well-studied object.

Reformulating (ZC1) - Double action

Set $u^0 = \sum_{g \in G} r_g g^{-1}$ and $U = \langle c \rangle \cong C_k$.

Define the *double action module* ${}_u(RG)_G$: an $R(G \times U)$-module which is RG as R-module and

$$m \cdot (g, c^i) = (u^i)^0 mg \quad \text{for} \quad m \in {}_u(RG)_G, \ (g, c^i) \in G \times U$$

An $R(G \times U)$-module M is *G-regular* if $M|_{RG} \cong RG$, i.e. M is free of rank 1 as RG-module.

Reformulating (ZC1) - Double action

Define the *double action module* ${}_u(RG)_G$: an $R(G \times U)$-module which is RG as R-module and

$$m \cdot (g, c^i) = (u^i)^0 mg \quad \text{for} \quad m \in {}_u(RG)_G, \ (g, c^i) \in G \times U$$

An $R(G \times U)$-module M is *G-regular* if $M|_{RG} \cong RG$, i.e. M is free of rank 1 as RG-module.

Folklore/Weiss

- If M is G-regular, there is $u \in U(RG)$ s.t. $u^k = 1$ and $M \cong {}_u(RG)_G$.
- If $u, v \in U(RG)$ and $u^k = v^k = 1$, then u and v are conjugate in $U(RG)$ if and only if ${}_u(RG)_G \cong {}_v(RG)_G$.
- If θ is the character of ${}_u(RG)_G$, then $\theta(g, c^i) = |C_G(g)|\varepsilon_g(u^i)$.

$\rightsquigarrow$ **Goal:** Find G-regular $\mathbb{Z}(G \times U)$-module with "bad" character (as conjugation over $\mathbb{Q}$)

The strategy

For p a prime and π a set of primes denote

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus p\mathbb{Z} \right\} \text{ and } \mathbb{Z}_{(\pi)} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \pi\mathbb{Z} \right\}$$

the *localisations* at p and π.
For π the prime divisors of $|G|$ we construct $u \in V(\mathbb{Z}G)$ and its corresponding double-action module "stepwise":

$$\mathbb{Q}G \longleftarrow\!\!\shortmid\; \mathbb{Z}_{(p)}G \longleftarrow\!\!\shortmid\; \mathbb{Z}_{(\pi)}G \longleftarrow\!\!\shortmid\; \mathbb{Z}G$$

Rational – – – Local – – – Semi-local – – – Global

$\mathbb{Q}G$ - a question of characters

Let $g_1, ..., g_r \in G$ be representatives of conjugacy classes, $\varepsilon_{g_1}, ..., \varepsilon_{g_r} \in \mathbb{Z}$ s.t. $\varepsilon_{g_1} + ... + \varepsilon_{g_r} = 1$.
Set $[g_i] = \langle (g_i, c) \rangle \leq G \times U$ and $\mathbf{1}$ the trivial character.

Existence of rational unit

If

$$\chi = \sum_{i=1}^{r} \varepsilon_{g_i} \mathrm{ind}_{[g_i]}^{G \times U} \mathbf{1}$$

is a *proper* character of $G \times U$, then there is $u_{\mathbb{Q}} \in U(\mathbb{Q}G)$ s.t. $u^k = 1$ and $\varepsilon_{g_i}(u_{\mathbb{Q}}) = \varepsilon_{g_i}$.

χ is a proper character if and only if $\langle \chi, \psi \rangle \in \mathbb{Z}_{\geq 0}$ for any irreducible character ψ of $G \times U$.
$\rightsquigarrow$ This is a problem of solving linear integral inequalities.

$\mathbb{Z}_{(p)}G$ - characters and action

Let N abelian, $G = N \rtimes A$ and $\varepsilon_g = 0$ for $g \notin N$. Let p be any prime.

Existence of local unit

If $C_G(n_p) \cap C_G(n_{p'}^g) = N$ for all $g \in G$ and $n \in N$ with $\varepsilon_n \neq 0$ and

$$\chi|_{N\times U} = \sum_{n\in N_p} \xi_n \otimes \mathrm{ind}_{[n]_p}^{N_p\times U_p} \mathbf{1}$$

with all ξ_n proper characters of $N_{p'} \times U_{p'}$, then there is $u_{(p)} \in U(\mathbb{Z}_{(p)}G)$ s.t. $u^k = 1$ and $\varepsilon_{g_i}(u_{(p)}) = \varepsilon_{g_i}$.

$\rightsquigarrow$ Again this is a problem of solving linear integral inequalities and a (mild) condition on the action of A on N.

$\mathbb{Z}_{(\pi)}G$ - a well-known procedure

For each prime p dividing $|G|$ from the previous step we get $u_{(p)} \in \mathbb{Z}_{(p)}G$ with the needed properties and corresponding double-action modules M_p over $\mathbb{Z}_{(p)}(G \times U)$.

These modules can be intersected to give a $\mathbb{Z}_{(\pi)}(G \times U)$-module

$\rightsquigarrow$ We get $u_{(\pi)} \in U(\mathbb{Z}_{(\pi)}G)$ with the needed properties not adding any new conditions.

$\mathbb{Z}G$ - genus class group and eigenvalues

A $\mathbb{Z}G$-module M is *locally free* if $\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}} M$ is free for every prime p.

Two $\mathbb{Z}G$ modules M_1 and M_2 are *stably isomorphic* if $M_1 \oplus \mathbb{Z}G \cong M_2 \oplus \mathbb{Z}G$.

The stable isomorphism classes of locally free $\mathbb{Z}G$-modules form the *genus class group* by defining

$$[M_1] + [M_2] = [M_3] \quad \text{when} \quad M_1 \oplus M_2 \cong M_3 \oplus \mathbb{Z}G.$$

This object is well-studied and can also be described as the image of another group (Fröhlich).

The unit $u_{(\pi)}$ gives us a $\mathbb{Z}(G \times U)$-module M which is locally free as $\mathbb{Z}G$-module.
$\rightsquigarrow$ Can we "deform" M to become free as $\mathbb{Z}G$-module, i.e. G-regular, in particular trivial in the genus class group?

$\mathbb{Z}G$ - genus class group and eigenvalues

Let D be an ordinary representation of G.
$\rightsquigarrow$ D extends linearly to $\mathbb{Q}G$.
$\rightsquigarrow$ $D(u)^k = 1$, so $D(u)$ diagonisable with eigenvalues roots of unity.

The global unit

Assume $D(u_{(\pi)})$ has eigenvalue 1 for any irreducible representation D and G does not map surjectively onto certain groups. Then there is $u \in U(\mathbb{Z}G)$ s.t. $u^k = 1$ and $\varepsilon_{g_i}(u) = \varepsilon_{g_i}$

$\rightsquigarrow$ As eigenvalues of $D(u)$ follow from the partial augmentations, this is again a condition on the ε_{g_i} and a (mild) group-theoretical condition.

Putting things together

We have reduced the question of finding a counterexample, in a certain class of groups, to finding a group G and integers $\varepsilon_{g_1}, \ldots, \varepsilon_{g_r}$ with certain properties and such that some ε_{g_i} is negative.

$\rightsquigarrow$ For the groups from the theorem it remains to show that such numbers $\varepsilon_{g_1}, \ldots, \varepsilon_{g_r}$ exist. This is now an elementary (though long) calculation.

$\rightsquigarrow$ The Zassenhaus Conjecture does not hold.

Questions?