INTENSE AUTOMORPHISMS OF GROUPS

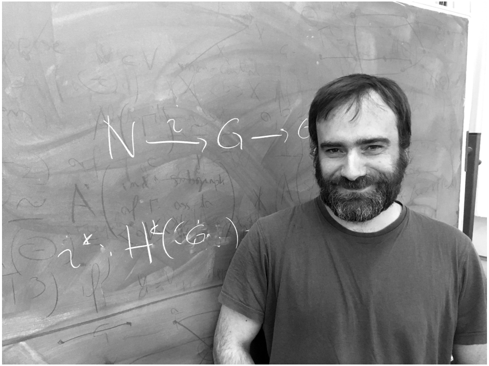
Mima Stanojkovski

FRAUEN IN DER MATHEMATIK
Konstanz, 24 January 2017

Joint work with

Hendrik Lenstra (UL)

Andrea Lucchini (UniPD)



Jon González Sánchez (EHU)

Groups and symmetries

Symmetries of objects

Symmetries of objects

Let X be an object and let $\mathrm{Sym}(X)$ be the group of its symmetries.

- S_n

Symmetries of objects

Let X be an object and let $\mathrm{Sym}(X)$ be the group of its symmetries.

- S_n
- D_{2n}

Symmetries of objects

Let X be an object and let $\mathrm{Sym}(X)$ be the group of its symmetries.

- S_n
- D_{2n}
- $\mathrm{GL}(V)$

Symmetries of objects

Let X be an object and let $\mathrm{Sym}(X)$ be the group of its symmetries.

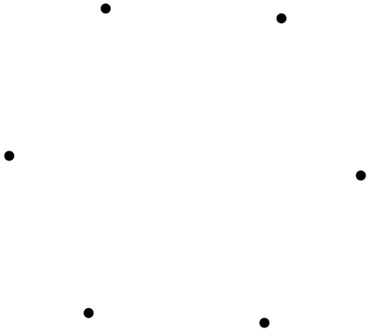
- S_n
- D_{2n}
- $\mathrm{GL}(V)$
- $\mathrm{Gal}(\ell/k)$

Symmetries of objects

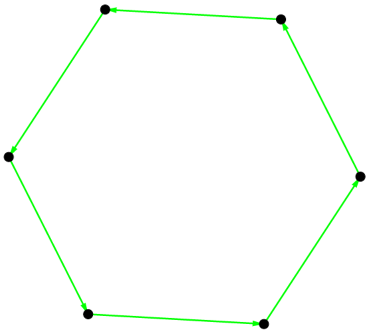
Let X be an object and let $\mathrm{Sym}(X)$ be the group of its symmetries.

- S_n
- D_{2n}
- $\mathrm{GL}(V)$
- $\mathrm{Gal}(\ell/k)$
- $\mathrm{Aut}(G)$

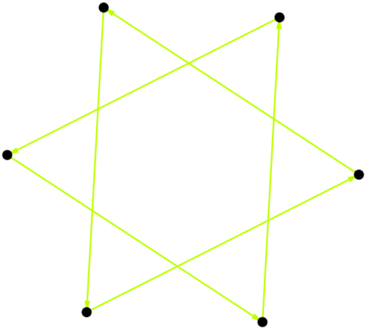
Permutation of points



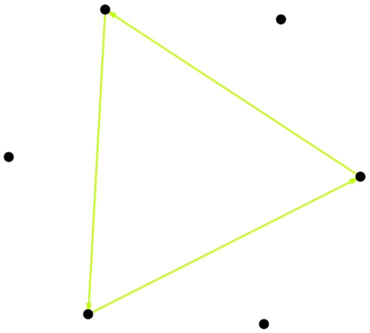
Permutation of points



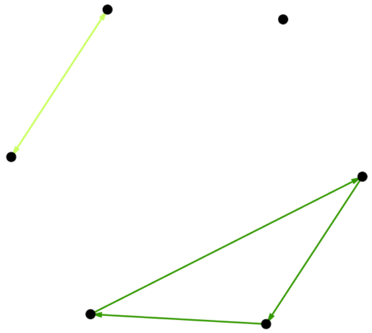
Permutation of points



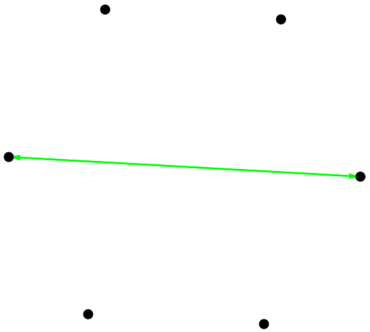
Permutation of points



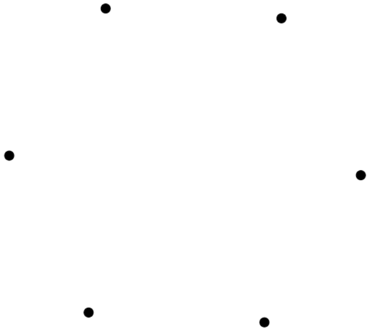
Permutation of points



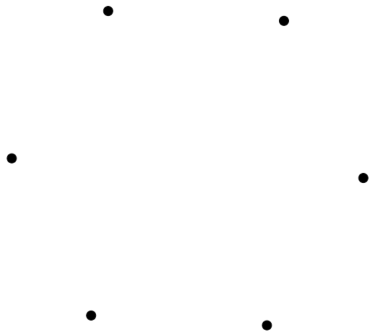
Permutation of points



Permutation of points

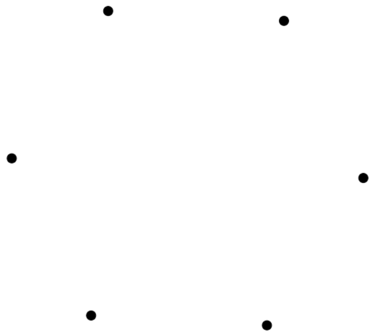


Permutation of points



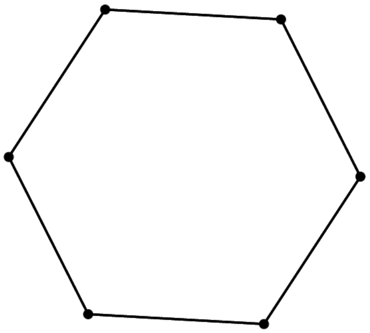
The group of symmetries is $\mathrm{Sym}(X) = S_6$

Permutation of points

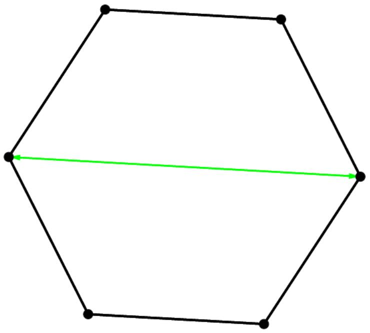


The group of symmetries is $\mathrm{Sym}(X) = S_6$ which has 720 elements.

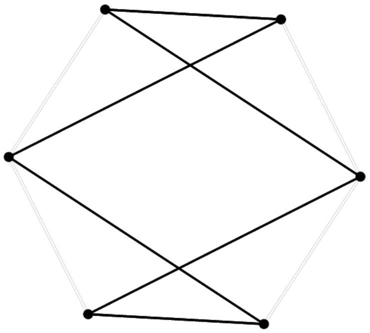
Symmetries of a regular polygon



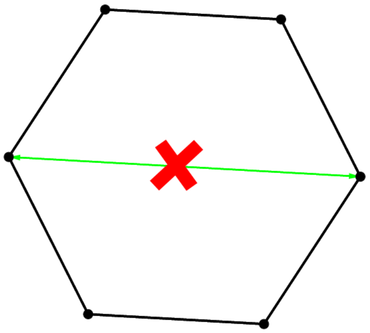
Symmetries of a regular polygon



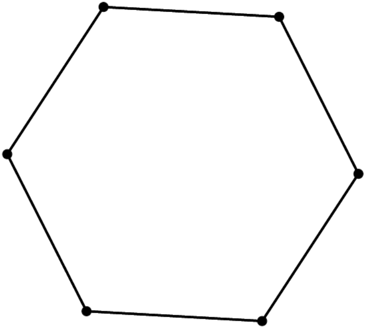
Symmetries of a regular polygon



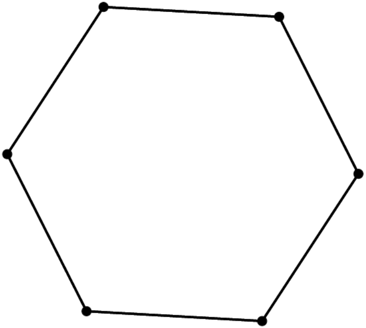
Symmetries of a regular polygon



Symmetries of a regular polygon

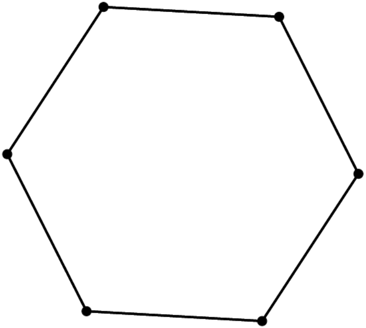


Symmetries of a regular polygon



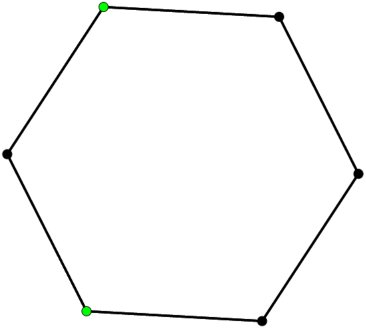
The group of symmetries is $\mathrm{Sym}(X) = \mathrm{D}_{12}$

Symmetries of a regular polygon

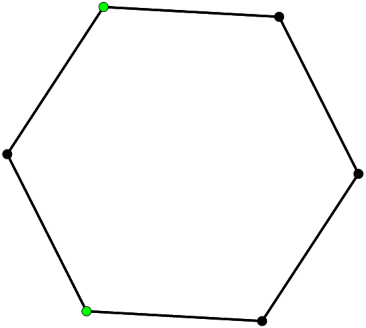


The group of symmetries is $\mathrm{Sym}(X) = \mathrm{D}_{12}$ which has 12 elements.

Symmetries of a coloured polygon

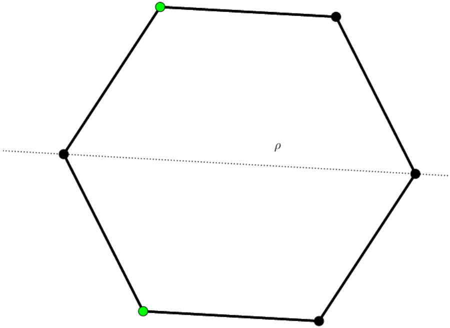


Symmetries of a coloured polygon



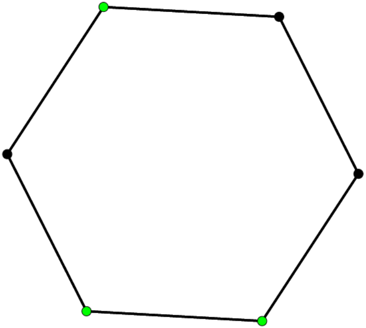
The group of symmetries is $\mathrm{Sym}(X) = \{\mathrm{id}_X, \rho\}$.

Symmetries of a coloured polygon

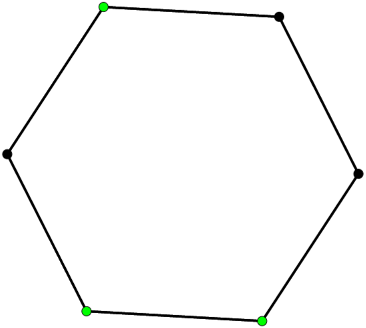


The group of symmetries is $\mathrm{Sym}(X) = \{\mathrm{id}_X, \rho\}$.

Symmetries of a coloured polygon



Symmetries of a coloured polygon



The group of symmetries is $\mathrm{Sym}(X) = \{\mathrm{id}_X\}$.

Symmetries of a vector space

Let k be a field and let V be a vector space over k.

Symmetries of a vector space

Let k be a field and let V be a vector space over k.

Then $\mathrm{Sym}(V) = \mathrm{GL}_k(V)$ is the collection of maps $\alpha : V \to V$ such that:

- for all $u, v \in V$, one has $\alpha(u + v) = \alpha(u) + \alpha(v)$;

Symmetries of a vector space

Let k be a field and let V be a vector space over k.

Then $\mathrm{Sym}(V) = \mathrm{GL}_k(V)$ is the collection of maps $\alpha : V \to V$ such that:

- for all $u, v \in V$, one has $\alpha(u+v) = \alpha(u) + \alpha(v)$;
- for all $\lambda \in k$ and $v \in V$, one has $\alpha(\lambda v) = \lambda\alpha(v)$;

Symmetries of a vector space

Let k be a field and let V be a vector space over k.

Then $\mathrm{Sym}(V) = \mathrm{GL}_k(V)$ is the collection of maps $\alpha : V \to V$ such that:

- for all $u, v \in V$, one has $\alpha(u + v) = \alpha(u) + \alpha(v)$;
- for all $\lambda \in k$ and $v \in V$, one has $\alpha(\lambda v) = \lambda\alpha(v)$;
- the map α is bijective.

Symmetries of a vector space

Let k be a field and let V be a vector space over k.

Then $\mathrm{Sym}(V) = \mathrm{GL}_k(V)$ is the collection of maps $\alpha : V \to V$ such that:

- for all $u, v \in V$, one has $\alpha(u + v) = \alpha(u) + \alpha(v)$;
- for all $\lambda \in k$ and $v \in V$, one has $\alpha(\lambda v) = \lambda\alpha(v)$;
- the map α is bijective.

If V has finite dimension n over k, then $GL_k(V) \cong \mathrm{GL}_n(k)$.

Symmetries of field extensions

Let ℓ/k be an extension of fields.

Symmetries of field extensions

Let ℓ/k be an extension of fields.

Then $\mathsf{Sym}(\ell/k) = \mathsf{Aut}_k(\ell)$ is the collection of maps $\alpha : \ell \to \ell$ such that:

- $\alpha \in \mathsf{GL}_k(\ell)$;

Symmetries of field extensions

Let ℓ/k be an extension of fields.

Then $\mathrm{Sym}(\ell/k) = \mathrm{Aut}_k(\ell)$ is the collection of maps $\alpha : \ell \to \ell$ such that:

- $\alpha \in \mathrm{GL}_k(\ell)$;
- for all $x, y \in \ell$, one has $\alpha(xy) = \alpha(x)\alpha(y)$.

Symmetries of field extensions

Let ℓ/k be an extension of fields.

Then $\mathrm{Sym}(\ell/k) = \mathrm{Aut}_k(\ell)$ is the collection of maps $\alpha : \ell \to \ell$ such that:

- $\alpha \in \mathrm{GL}_k(\ell)$;
- for all $x, y \in \ell$, one has $\alpha(xy) = \alpha(x)\alpha(y)$.

($\Rightarrow$ for all $x \in k$, one has $\alpha(x) = x$)

Symmetries of field extensions

Let ℓ/k be an extension of fields.

Then $\mathrm{Sym}(\ell/k) = \mathrm{Aut}_k(\ell)$ is the collection of maps $\alpha : \ell \to \ell$ such that:

- $\alpha \in \mathrm{GL}_k(\ell)$;
- for all $x, y \in \ell$, one has $\alpha(xy) = \alpha(x)\alpha(y)$.

($\Rightarrow$ for all $x \in k$, one has $\alpha(x) = x$)

Symmetries of field extensions

Let ℓ/k be an extension of fields.

Then $\mathrm{Sym}(\ell/k) = \mathrm{Aut}_k(\ell)$ is the collection of maps $\alpha : \ell \to \ell$ such that:

- $\alpha \in \mathrm{GL}_k(\ell)$;
- for all $x, y \in \ell$, one has $\alpha(xy) = \alpha(x)\alpha(y)$.

($\Rightarrow$ for all $x \in k$, one has $\alpha(x) = x$)

If the extension ℓ/k is Galois, then $\mathrm{Gal}(\ell/k) = \mathrm{Aut}_k(\ell)$.

Symmetries of groups

Let G be a group. Then $\mathrm{Sym}(G) = \mathrm{Aut}(G)$ consists of all maps $\alpha : G \to G$ such that:

- for all $g, h \in G$, one has $\alpha(gh) = \alpha(g)\alpha(h)$;

Symmetries of groups

Let G be a group. Then $\mathrm{Sym}(G) = \mathrm{Aut}(G)$ consists of all maps $\alpha : G \to G$ such that:

- for all $g, h \in G$, one has $\alpha(gh) = \alpha(g)\alpha(h)$;
- the map α is bijective.

Symmetries of groups

Let G be a group. Then $\mathrm{Sym}(G) = \mathrm{Aut}(G)$ consists of all maps $\alpha : G \to G$ such that:

- for all $g, h \in G$, one has $\alpha(gh) = \alpha(g)\alpha(h)$;
- the map α is bijective.

Example:

- $\mathrm{Aut}(\{1\}) = \{\mathrm{id}\}$;
- $\mathrm{Aut}(\mathbb{Z}) = \{\pm\,\mathrm{id}\}$;
- $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

From the symmetries to the group

Example 1

Let G be a group. Then

$$\mathrm{Aut}(G) = 1 \quad \Rightarrow$$

Example 1

Let G be a group. Then

$$\mathrm{Aut}(G) = 1 \quad \Rightarrow \quad \#G = 1 \text{ or } \#G = 2.$$

Example 2

Let G be a group. Then

$$\mathrm{Aut}(G) \text{ is cyclic} \quad \Rightarrow$$

Example 2

Let G be a group. Then

$$\mathrm{Aut}(G) \text{ is cyclic} \quad \Rightarrow \quad G \text{ is abelian.}$$

Example 2

Let G be a finitely generated group. Then

$$\mathrm{Aut}(G) \text{ is cyclic} \quad \Rightarrow \quad G \text{ is cyclic.}$$

Example 2

Let G be a finitely generated group. Then

$\mathrm{Aut}(G)$ is cyclic $\Rightarrow$ G is one between

- $\mathbb{Z}/2\mathbb{Z}$;
- $\mathbb{Z}/4\mathbb{Z}$;
- $\mathbb{Z}/p^k\mathbb{Z}$, for p odd and $k \geq 0$;
- $\mathbb{Z}$.

Example 3

Let G be a group and assume that

- G has cardinality $729 = 3^6$.
- G is 2-generated.
- $\mathrm{Aut}(G)$ has cardinality 104976.

Then G is unique up to isomorphism.

Non-Example 3

Let G be a group and assume that

- G has cardinality $729 = 3^6$.
- G is 2-generated.
- ~~$\mathrm{Aut}(G)$ has cardinality 104976~~.

Then there are 100 possible isomorphism classes for G.

General idea

Conditions on the structure of $\mathrm{Aut}(G)$

General idea

Conditions on the structure of $\mathrm{Aut}(G)$

$$\downarrow$$

Restrictions to the structure of G

General idea

Conditions on the structure of $\mathrm{Aut}(G)$

$\downarrow$

Restrictions to the structure of G

$\downarrow$

PB: Does G even exist?

Intense automorphisms of groups

Intense automorphisms

Let G be a finite group. An automorphism α of G is **intense** if for all $H \leq G$ there exists $g \in G$ such that $\alpha(H) = gHg^{-1}$. Write $\alpha \in \mathrm{Int}(G)$.

Intense automorphisms

Let G be a finite group. An automorphism α of G is **intense** if for all $H \leq G$ there exists $g \in G$ such that $\alpha(H) = gHg^{-1}$. Write $\alpha \in \mathrm{Int}(G)$.

Motivation: Intense automorphisms appear naturally as solutions to a certain cohomological problem. They (surprisingly!) give rise to a very rich theory.

Example:

- Every automorphism of a cyclic group is intense.
- Inner automorphisms are intense.

Intensity

Let p be a prime number and let G be a finite p-group.

Intensity

Let p be a prime number and let G be a finite p-group. Then

$$\mathrm{Int}(G) \cong P \rtimes C$$

where

- P is a p-group.
- C is a subgroup of $\mathbb{F}_p^*$.

Intensity

Let p be a prime number and let G be a finite p-group. Then

$$\mathrm{Int}(G) \cong P \rtimes C$$

where

- P is a p-group.
- C is a subgroup of $\mathbb{F}_p^*$.

The **intensity** of G is $\mathrm{int}(G) = \#C$.

The problem

Can we classify all p-groups G satisfying $\mathrm{int}(G) > 1$?

The problem

Can we classify all p-groups G satisfying $\mathrm{int}(G) > 1$?

YES!

Intense triples

An **intense triple** is a triple (p, G, α) such that

- p is a prime number.
- G is a finite p-group.
- $\alpha \neq 1$ belongs to C (or to a conjugate).

Intense triples

An **intense triple** is a triple (p, G, α) such that

- p is a prime number.
- G is a finite p-group.
- $\alpha \neq 1$ belongs to C (or to a conjugate).

Intense triples are quite rare: if a group occurs in an intense triple, then its structure is almost uniquely determined by p and its *class*.

Intense triples

An **intense triple** is a triple (p, G, α) such that

- p is a prime number.
- G is a finite p-group.
- $\alpha \neq 1$ belongs to C (or to a conjugate).

Intense triples are quite rare: if a group occurs in an intense triple, then its structure is almost uniquely determined by p and its *class*.

There are no intense triples with $p = 2$.

Equivalent triples

Example:

Let p be an odd prime and let $n \in \mathbb{Z}_{>0}$.
For all $\alpha \in \mathbb{F}_p^* \setminus \{1\}$, the triple $(p, \mathbb{F}_p^n, \alpha)$ is intense.

Equivalent triples

Example:

Let p be an odd prime and let $n \in \mathbb{Z}_{>0}$.
For all $\alpha \in \mathbb{F}_p^* \setminus \{1\}$, the triple $(p, \mathbb{F}_p^n, \alpha)$ is intense.

Two intense triples (p, G, α) and (q, G', β) are **equivalent** if there exists an isomorphism $\sigma : G \to G'$ such that $\beta = \sigma\alpha\sigma^{-1}$. It follows that $p = q$.

Let $\mathcal{T} = \{[p, G, \alpha] \mid p, G, \alpha \ldots\}$ denote the set of equivalence classes of intense triples.

Abelian groups

Let p be a prime number and let $\mathbb{Z}_p$ denote the ring of p-adic integers. Define $\omega(\mathbb{F}_p^*) = \{\alpha \in \mathbb{Z}_p^* \mid \alpha^{p-1} = 1\}$.

Note that $\omega(\mathbb{F}_p^*) \cong \mathbb{F}_p^*$ and that every abelian p-group has a natural structure of $\mathbb{Z}_p$-module.

Abelian groups

Let p be a prime number and let $\mathbb{Z}_p$ denote the ring of p-adic integers. Define $\omega(\mathbb{F}_p^*) = \{\alpha \in \mathbb{Z}_p^* \mid \alpha^{p-1} = 1\}$.

Note that $\omega(\mathbb{F}_p^*) \cong \mathbb{F}_p^*$ and that every abelian p-group has a natural structure of $\mathbb{Z}_p$-module.

Proposition

Assume that:

- *p is odd.*
- *$G \neq 1$ is a finite abelian p-group.*
- *$\alpha \in \omega(\mathbb{F}_p^*) \setminus \{1\}$. (Example: $\alpha = -1$)*

Then $[p, G, \alpha] \in \mathcal{T}$ *and* $\mathrm{int}(G) = p - 1$.

The lower central series

Let G be a finite group.

- If $x, y \in G$, then $[x, y] = xyx^{-1}y^{-1}$.
- If $H, K \leq G$, then $[H, K] = \langle [x, y] \mid x \in H, y \in K \rangle$.

The lower central series

Let G be a finite group.

- If $x, y \in G$, then $[x, y] = xyx^{-1}y^{-1}$.
- If $H, K \leq G$, then $[H, K] = \langle [x, y] \mid x \in H, y \in K \rangle$.

The **lower central series** of G is given by

- $G_1 = G$.
- $G_{i+1} = [G, G_i]$.

The lower central series

Let G be a finite group.

- If $x, y \in G$, then $[x, y] = xyx^{-1}y^{-1}$.
- If $H, K \leq G$, then $[H, K] = \langle [x, y] \mid x \in H, y \in K \rangle$.

The **lower central series** of G is given by

- $G_1 = G$.
- $G_{i+1} = [G, G_i]$.

If G is a p-group, there exists k such that $G_k = 1$ and the **(nilpotency) class** of G is

$$c = \#\{i \mid G_i \neq G_{i+1}\} = -1 + \min\{k \mid G_k = 1\}.$$

Strategy

For all $c \in \mathbb{Z}_{\geq 0}$, let $\mathcal{T}[c] = \{[p, G, \alpha] \in \mathcal{T} \mid G \text{ has class } c\}$.

Then:

- $\mathcal{T} = \bigsqcup_c \mathcal{T}[c]$.
- $\mathcal{T}[0] = \emptyset$.
- $\mathcal{T}[1] = \{[p, G, \alpha] \text{ as in the Proposition}\}$.
- $\mathcal{T}[c]$ for $c = 2$?
- $\mathcal{T}[c]$ for $c \geq 3$?

Class 2

Let p be an odd prime and let $n \in \mathbb{Z}_{>0}$. Define $(\mathrm{ES}(p,n), *)$ as

- $\mathrm{ES}(p,n) = \mathbb{F}_p \times \mathbb{F}_p^n \times \mathbb{F}_p^n$.
- $(z_1, y_1, x_1) * (z_2, y_2, x_2) = (z_1 + z_2 + x_1 \cdot y_2, y_1 + y_2, x_1 + x_2)$.

Class 2

Let p be an odd prime and let $n \in \mathbb{Z}_{>0}$. Define $(\mathrm{ES}(p,n),*)$ as

- $\mathrm{ES}(p,n) = \mathbb{F}_p \times \mathbb{F}_p^n \times \mathbb{F}_p^n$.
- $(z_1, y_1, x_1) * (z_2, y_2, x_2) = (z_1 + z_2 + x_1 \cdot y_2, y_1 + y_2, x_1 + x_2)$.

<u>*Exercise:*</u>

- $(\mathrm{ES}(p,n),*)$ has order p^{2n+1} and class 2.
- Let $\lambda \in \mathbb{F}_p^*$. Then $\alpha_\lambda : (z,y,x) \mapsto (\lambda^2 z, \lambda y, \lambda x)$ is an intense automorphism of $(\mathrm{ES}(p,n),*)$.

Class 2

Let p be an odd prime and let $n \in \mathbb{Z}_{>0}$. Define $(\mathrm{ES}(p,n),*)$ as

- $\mathrm{ES}(p,n) = \mathbb{F}_p \times \mathbb{F}_p^n \times \mathbb{F}_p^n$.
- $(z_1, y_1, x_1) * (z_2, y_2, x_2) = (z_1 + z_2 + x_1 \cdot y_2, y_1 + y_2, x_1 + x_2)$.

Exercise:

- $(\mathrm{ES}(p,n),*)$ has order p^{2n+1} and class 2.
- Let $\lambda \in \mathbb{F}_p^*$. Then $\alpha_\lambda : (z,y,x) \mapsto (\lambda^2 z, \lambda y, \lambda x)$ is an intense automorphism of $(\mathrm{ES}(p,n),*)$.

Proposition

$\mathcal{T}[2] = \{[p, (\mathrm{ES}(p,n),*), \alpha_\lambda] \mid p \textit{ is odd}, n \in \mathbb{Z}_{>0}, \lambda \in \mathbb{F}_p^* \setminus \{1\}\}$.

Class at least 3

Given a p-group G, let $(G_i)_{i\geq 1}$ be its lower central series. Let $(f_i)_{i\geq 1}$ be the sequence, with values in $\mathbb{Z}_{\geq 0}$, such that the order of G_i/G_{i+1} is equal to p^{f_i}.

Class at least 3

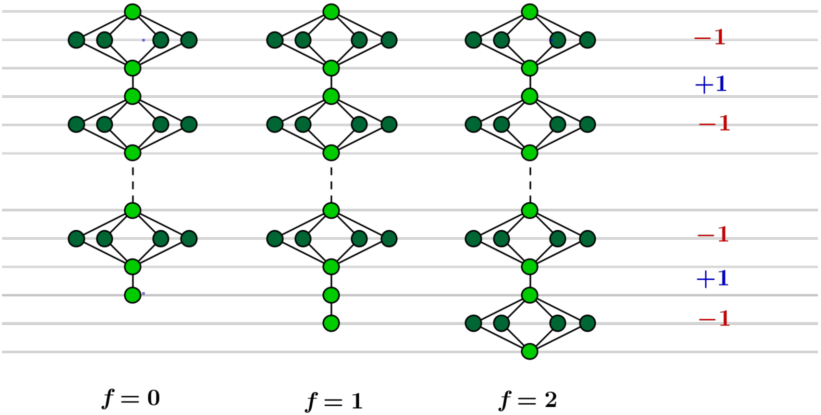
Given a p-group G, let $(G_i)_{i\geq 1}$ be its lower central series. Let $(f_i)_{i\geq 1}$ be the sequence, with values in $\mathbb{Z}_{\geq 0}$, such that the order of G_i/G_{i+1} is equal to p^{f_i}.

Proposition

Let $c \geq 3$ and assume $[p, G, \alpha] \in \mathcal{T}[c]$. The following hold.

- *The order of α is equal to 2 and* $\mathrm{int}(G) = 2$.
- *For all i, the quotient G_i/G_{i+1} is a vector space over $\mathbb{F}_p$ and α induces multiplication by $(-1)^i$ on it.*
- $(f_i)_{i\geq 1} = (2, 1, 2, 1, \dots, 2, 1, f, 0, 0, 0, \dots)$ *with* $f \in \{0, 1, 2\}$.

Normal subgroups structure



An intense graph

Fix p and define $\mathcal{T}_p = \{[p, G, \alpha] \mid G, \alpha, \dots\}$.

There is a well-defined sequence of sets

$$\dots \longrightarrow \mathcal{T}_p[c+1] \xrightarrow{\pi_{c+1}} \mathcal{T}_p[c] \xrightarrow{\pi_c} \mathcal{T}_p[c-1] \longrightarrow \dots$$

where, for all c, the map π_c is defined by

$$\pi_c : [p, G, \alpha] \mapsto [p, G/G_c, \overline{\alpha}].$$

An intense graph

Fix p and define $\mathcal{T}_p = \{[p, G, \alpha] \mid G, \alpha, \ldots\}$.

There is a well-defined sequence of sets

$$\ldots \longrightarrow \mathcal{T}_p[c+1] \xrightarrow{\pi_{c+1}} \mathcal{T}_p[c] \xrightarrow{\pi_c} \mathcal{T}_p[c-1] \longrightarrow \ldots$$

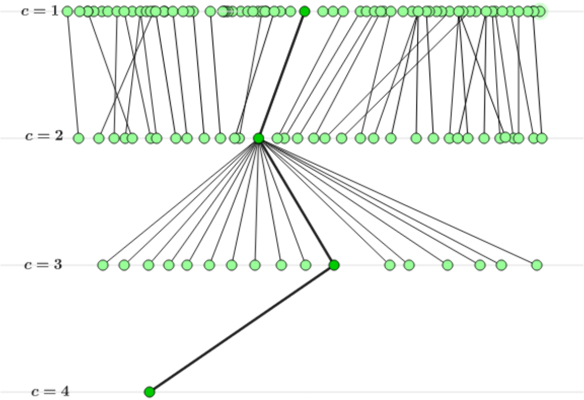
where, for all c, the map π_c is defined by

$$\pi_c : [p, G, \alpha] \mapsto [p, G/G_c, \overline{\alpha}].$$

We define a graph $\mathcal{G}_p = (E_p, V_p)$, where

- $V_p = \mathcal{T}_p$.
- $(v, w) \in E_p$ if there exists c such that $\pi_c(v) = w$.

The graph for $p = 3$



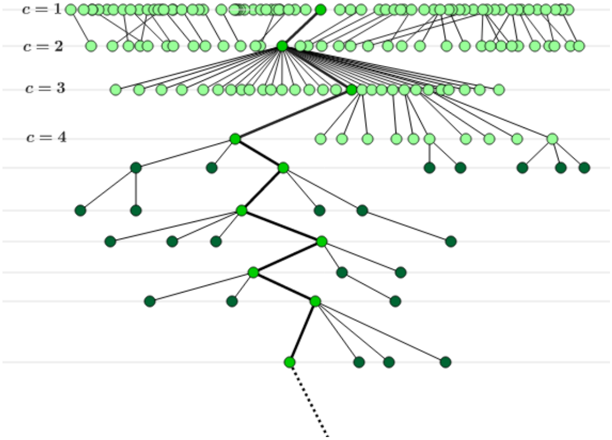
Example 3

Let G be a group. Assume that

- G has cardinality $729 = 3^6$.
- G is 2-generated.
- $\mathrm{Aut}(G)$ has cardinality 104976.

Then G is unique up to isomorphism.

The graph for $p > 3$



The infinite case

Theorem

Let p be an odd prime and let $c \in \mathbb{Z}_{>0}$. Then the following hold.

- *If $c \geq 3$, then $\mathcal{T}_p[c]$ is finite.*
- $\mathcal{T}_p[c] = \emptyset \iff p = 3$ *and* $c \geq 5$.
- *If $p > 3$, then $\# \varprojlim_{c} \mathcal{T}_p[c] = 1$.*

The infinite case

Theorem

Let p be an odd prime and let $c \in \mathbb{Z}_{>0}$. Then the following hold.

- *If $c \geq 3$, then $\mathcal{T}_p[c]$ is finite.*
- $\mathcal{T}_p[c] = \emptyset \iff p = 3$ *and* $c \geq 5$.
- *If $p > 3$, then $\# \varprojlim_{c} \mathcal{T}_p[c] = 1$.*

If $\varprojlim_{c} \mathcal{T}_p[c] = \{[p, G^{(c)}, \alpha^{(c)}]\}_{c>0}$, we want to determine the pro-p-group $G_{lim} = \varprojlim_{c} G^{(c)}$ and the automorphism α_{lim} of G_{lim} that is induced by the automorphisms $\alpha^{(c)}$.

A profinite example

Let $p > 3$ be a prime and let $t \in \mathbb{Z}_p$ satisfy $(\frac{t}{p}) = -1$. Set $\mathrm{A}_p = \mathbb{Z}_p + \mathbb{Z}_p\mathrm{i} + \mathbb{Z}_p\mathrm{j} + \mathbb{Z}_p\mathrm{ij}$ with defining relations $\mathrm{i}^2 = t$, $\mathrm{j}^2 = p$, and $\mathrm{ji} = -\mathrm{ij}$. Then A_p is a non-commutative local ring such that $\mathrm{A}_p/\mathrm{j}\mathrm{A}_p \cong \mathbb{F}_{p^2}$. The involution $\overline{\cdot} : \mathrm{A}_p \to \mathrm{A}_p$ is defined by

$$a = s + t\mathrm{i} + u\mathrm{j} + v\mathrm{ij} \;\mapsto\; \bar{a} = s - t\mathrm{i} - u\mathrm{j} - v\mathrm{ij}.$$

Let $G = \{a \in \mathrm{A}_p^* \mid a\bar{a} = 1 \text{ and } a \equiv 1 \bmod \mathrm{j}\mathrm{A}_p\}$ and, for all $a \in G$, define $\alpha(a) = \mathrm{i}a\mathrm{i}^{-1}$.

Theorem

G is a pro-p-group and α is topologically intense, i.e. for any closed subgroup H of G there exists $g \in G$ such that $\alpha(H) = gHg^{-1}$. Moreover, $(G, \alpha) \cong (G_{lim}, \alpha_{lim})$.

THANK YOU