On the minimal ramification problem for semiabelian groups

Danny Neftin
Joint with Hershy Kisilevsky and Jack Sonn

Department of Mathematics
University of Michigan
Ann Arbor, Michigan

Winter School on Galois Theory

Motivation

K- number field,
G- finite group.

Problems

- Let S be a finite set of primes,

Motivation

K- number field,
G- finite group.

Problems

- Let S be a finite set of primes,
  let K_S be the maximal extension of K unramified outside of S,

Motivation

K- number field,
G- finite group.

Problems

- Let S be a finite set of primes,
  let K_S be the maximal extension of K unramified outside of S,
  what is the structure of the Galois group $G_K(S) = \mathrm{Gal}(K_S/K)$?

Motivation

K- number field,
G- finite group.

Problems

- Let S be a finite set of primes,
  let K_S be the maximal extension of K unramified outside of S,
  what is the structure of the Galois group $G_K(S) = \mathrm{Gal}(K_S/K)$?
- Given G, what are the sets S for which G is a quotient of $G_K(S)$?

Motivation

K- number field,
G- finite group.

Problems

- Let S be a finite set of primes,
  let K_S be the maximal extension of K unramified outside of S,
  what is the structure of the Galois group $G_K(S) = \mathrm{Gal}(K_S/K)$?
- Given G, what are the sets S for which G is a quotient of $G_K(S)$?
- What is the minimal size of a set S for which G appears as a quotient of $G_K(S)$? In other words, what is the minimal number of ramified primes in a G-extension of K?

Motivation

K- number field,
G- finite group.

Problems

- Let S be a finite set of primes,
  let K_S be the maximal extension of K unramified outside of S,
  what is the structure of the Galois group $G_K(S) = \mathrm{Gal}(K_S/K)$?
- Given G, what are the sets S for which G is a quotient of $G_K(S)$?
- What is the minimal size of a set S for which G appears as a quotient of $G_K(S)$? In other words, what is the minimal number of ramified primes in a G-extension of K?

Example

$K = \mathbb{C}(t)$, $O_K = \mathbb{C}[t]$

- If $|S| = n$ then $G_K(S)$ is the free profinite group on $n-1$ generators (by Riemann's Existence Theorem).

Example

$K = \mathbb{C}(t)$, $O_K = \mathbb{C}[t]$

- If $|S| = n$ then $G_K(S)$ is the free profinite group on $n-1$ generators (by Riemann's Existence Theorem).
- Let $\mathrm{d}(G)$ denote the minimal number of generators of G. Then G is a quotient of $G_K(S)$ if and only if $|S| \geq \mathrm{d}(G) + 1$.

Example

$K = \mathbb{C}(t)$, $O_K = \mathbb{C}[t]$

- If $|S| = n$ then $G_K(S)$ is the free profinite group on $n-1$ generators (by Riemann's Existence Theorem).
- Let $\mathrm{d}(G)$ denote the minimal number of generators of G. Then G is a quotient of $G_K(S)$ if and only if $|S| \geq \mathrm{d}(G) + 1$.

Consequence

The minimal number of ramified primes in a G-extension of $\mathbb{C}(t)$ is $\mathrm{d}(G) + 1$.

Example

$K = \mathbb{C}(t)$, $O_K = \mathbb{C}[t]$

- If $|S| = n$ then $G_K(S)$ is the free profinite group on $n-1$ generators (by Riemann's Existence Theorem).
- Let $\mathrm{d}(G)$ denote the minimal number of generators of G. Then G is a quotient of $G_K(S)$ if and only if $|S| \geq \mathrm{d}(G) + 1$.

Consequence

The minimal number of ramified primes in a G-extension of $\mathbb{C}(t)$ is $\mathrm{d}(G) + 1$.

The Minimal Ramification Problem for $K = \mathbb{Q}$

Problem

Given a finite group G:

- What is the minimal number of ramified primes in a G-extension of $\mathbb{Q}$? (counting the infinite prime)

The Minimal Ramification Problem for $K = \mathbb{Q}$

Problem

Given a finite group G:

- What is the minimal number of ramified primes in a G-extension of $\mathbb{Q}$? (counting the infinite prime)
- The tame version: What is the minimal number of ramified primes in a *tame* G-extension of $\mathbb{Q}$?

The Minimal Ramification Problem for $K = \mathbb{Q}$

Problem

Given a finite group G:

- What is the minimal number of ramified primes in a G-extension of $\mathbb{Q}$? (counting the infinite prime)
- The tame version: What is the minimal number of ramified primes in a *tame* G-extension of $\mathbb{Q}$?

Open cases:

The Minimal Ramification Problem for $K = \mathbb{Q}$

Problem

Given a finite group G:

- What is the minimal number of ramified primes in a G-extension of $\mathbb{Q}$? (counting the infinite prime)
- The tame version: What is the minimal number of ramified primes in a *tame* G-extension of $\mathbb{Q}$?

Open cases:

- Nilpotent groups,

The Minimal Ramification Problem for $K = \mathbb{Q}$

Problem

Given a finite group G:

- What is the minimal number of ramified primes in a G-extension of $\mathbb{Q}$? (counting the infinite prime)
- The tame version: What is the minimal number of ramified primes in a *tame* G-extension of $\mathbb{Q}$?

Open cases:

- Nilpotent groups,
- Dihedral groups D_n,

The Minimal Ramification Problem for $K = \mathbb{Q}$

Problem

Given a finite group G:

- What is the minimal number of ramified primes in a G-extension of $\mathbb{Q}$? (counting the infinite prime)
- The tame version: What is the minimal number of ramified primes in a *tame* G-extension of $\mathbb{Q}$?

Open cases:

- Nilpotent groups,
- Dihedral groups D_n,
- Symmetric groups S_n.

The Minimal Ramification Problem for $K = \mathbb{Q}$

Problem

Given a finite group G:

- What is the minimal number of ramified primes in a G-extension of $\mathbb{Q}$? (counting the infinite prime)
- The tame version: What is the minimal number of ramified primes in a *tame* G-extension of $\mathbb{Q}$?

Open cases:

- Nilpotent groups,
- Dihedral groups D_n,
- Symmetric groups S_n.

Abelian groups

Cyclotomic fields

Let $G = C_{n_1} \times \ldots \times C_{n_r}$, where $n_1 | n_2 | \ldots | n_r$.

- Choose distinct primes $q_j \equiv 1 \pmod{n_j}$, $j = 1, \ldots, r$.

Abelian groups

Cyclotomic fields

Let $G = C_{n_1} \times \ldots \times C_{n_r}$, where $n_1|n_2|\ldots|n_r$.

- Choose distinct primes $q_j \equiv 1 \pmod{n_j}$, $j = 1, \ldots, r$.
- Let K_j be the subfield of $\mathbb{Q}(e^{\frac{2\pi i}{q_j}})$ for which $\mathrm{Gal}(K_j/\mathbb{Q}) \cong C_{n_j}$.

Abelian groups

Cyclotomic fields

Let $G = C_{n_1} \times \ldots \times C_{n_r}$, where $n_1 | n_2 | \ldots | n_r$.

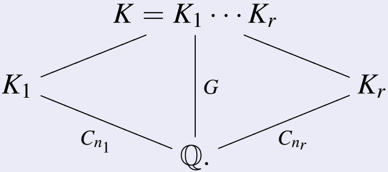
- Choose distinct primes $q_j \equiv 1 \pmod{n_j}$, $j = 1, \ldots, r$.
- Let K_j be the subfield of $\mathbb{Q}(e^{\frac{2\pi i}{q_j}})$ for which $\mathrm{Gal}(K_j/\mathbb{Q}) \cong C_{n_j}$.
- We have:

Abelian groups

Cyclotomic fields

Let $G = C_{n_1} \times \ldots \times C_{n_r}$, where $n_1 | n_2 | \ldots | n_r$.

- Choose distinct primes $q_j \equiv 1 \pmod{n_j}$, $j = 1, \ldots, r$.
- Let K_j be the subfield of $\mathbb{Q}(e^{\frac{2\pi i}{q_j}})$ for which $\mathrm{Gal}(K_j/\mathbb{Q}) \cong C_{n_j}$.
- We have:



Consequence

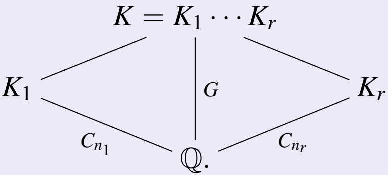
An abelian group of rank r can be (tamely) realized over $\mathbb{Q}$ with r ramified primes.

Abelian groups

Cyclotomic fields

Let $G = C_{n_1} \times \ldots \times C_{n_r}$, where $n_1 | n_2 | \ldots | n_r$.

- Choose distinct primes $q_j \equiv 1 \pmod{n_j}$, $j = 1, \ldots, r$.
- Let K_j be the subfield of $\mathbb{Q}(e^{\frac{2\pi i}{q_j}})$ for which $\mathrm{Gal}(K_j/\mathbb{Q}) \cong C_{n_j}$.
- We have:



Consequence

An abelian group of rank r can be (tamely) realized over $\mathbb{Q}$ with r ramified primes.

A lower bound

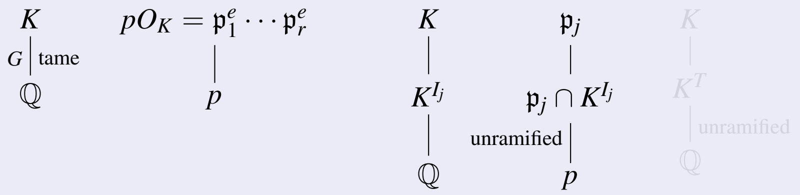
A consequence of Minkowski's Theorem

$$\begin{array}{c} K \\ G \Big| \text{ tame} \\ \mathbb{Q} \end{array} \qquad \begin{array}{c} pO_K = \mathfrak{p}_1^e \cdots \mathfrak{p}_r^e \\ \Big| \\ p \end{array} \qquad \begin{array}{c} K \\ \Big| \\ K^{I_j} \\ \Big| \\ \mathbb{Q} \end{array} \qquad \begin{array}{c} \mathfrak{p}_j \\ \Big| \\ \mathfrak{p}_j \cap K^{I_j} \\ \text{unramified} \Big| \\ p \end{array}$$

- I_j- the inertia group $I(\mathfrak{p}_j/p)$.
- The groups $I_1, \ldots, I_r$ are conjugates.
- Each I_j is cyclic.

A lower bound

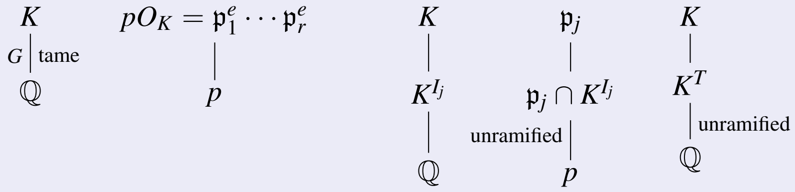
A consequence of Minkowski's Theorem



- I_j- the inertia group $I(\mathfrak{p}_j/p)$.
- The groups $I_1, \ldots, I_r$ are conjugates.
- Each I_j is cyclic.
- Let $T = \langle I(\mathfrak{p}/p) | \text{running over all rational primes } p \text{ and } \mathfrak{p}|p \rangle$.
- By Minkowski's Theorem $K^T = \mathbb{Q}$ and $T = G$. In other words, the inertia groups generate G.

A lower bound

A consequence of Minkowski's Theorem



- I_j- the inertia group $I(\mathfrak{p}_j/p)$.
- The groups $I_1, \ldots, I_r$ are conjugates.
- Each I_j is cyclic.
- Let $T = \langle I(\mathfrak{p}/p) |$running over all rational primes p and $\mathfrak{p}|p\rangle$.
- By Minkowski's Theorem $K^T = \mathbb{Q}$ and $T = G$. In other words, the inertia groups generate G.

A lower bound - Part II

Consequence

- If there are n ramified primes in $K/\mathbb{Q}$ then G is generated by n conjugacy classes.

A lower bound - Part II

Consequence

- If there are n ramified primes in $K/\mathbb{Q}$ then G is generated by n conjugacy classes.
- Let $c(G)$ be the minimal number of conjugacy classes that generate G.

A lower bound - Part II

Consequence

- If there are n ramified primes in $K/\mathbb{Q}$ then G is generated by n conjugacy classes.
- Let $c(G)$ be the minimal number of conjugacy classes that generate G.
- In every (tame) G-extension of $\mathbb{Q}$ there are at least $c(G)$ ramified primes.

A lower bound - Part II

Consequence

- If there are n ramified primes in $K/\mathbb{Q}$ then G is generated by n conjugacy classes.
- Let $c(G)$ be the minimal number of conjugacy classes that generate G.
- In every (tame) G-extension of $\mathbb{Q}$ there are at least $c(G)$ ramified primes.

Kaplan-Lev (2003)

Let $G \neq \{1\}$. Then:

$$c(G) := \begin{cases} \mathrm{d}(G^{ab}) & \text{if } G \neq [G,G] \\ 1 & \text{if } G = [G,G]. \end{cases}$$

A lower bound - Part II

Consequence

- If there are n ramified primes in $K/\mathbb{Q}$ then G is generated by n conjugacy classes.
- Let $c(G)$ be the minimal number of conjugacy classes that generate G.
- In every (tame) G-extension of $\mathbb{Q}$ there are at least $c(G)$ ramified primes.

Kaplan-Lev (2003)

Let $G \neq \{1\}$. Then:

$$c(G) := \begin{cases} \mathrm{d}(G^{ab}) & \text{if } G \neq [G,G] \\ 1 & \text{if } G = [G,G]. \end{cases}$$

Remark

If G is nilpotent then $c(G) = \mathrm{d}(G)$.

A lower bound - Part II

Consequence

- If there are n ramified primes in $K/\mathbb{Q}$ then G is generated by n conjugacy classes.
- Let $c(G)$ be the minimal number of conjugacy classes that generate G.
- In every (tame) G-extension of $\mathbb{Q}$ there are at least $c(G)$ ramified primes.

Kaplan-Lev (2003)

Let $G \neq \{1\}$. Then:

$$c(G) := \begin{cases} \mathrm{d}(G^{ab}) & \text{if } G \neq [G,G] \\ 1 & \text{if } G = [G,G]. \end{cases}$$

Remark

If G is nilpotent then $c(G) = \mathrm{d}(G)$.

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized with $c(G)$ ramified primes.

Evidence

The conjecture holds for:

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized with $c(G)$ ramified primes.

Evidence

The conjecture holds for:

- finite abelian groups,

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized with $c(G)$ ramified primes.

Evidence

The conjecture holds for:

- finite abelian groups,
- odd order groups of nilpotency class 2 (Plans 2004),

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized with $c(G)$ ramified primes.

Evidence

The conjecture holds for:

- finite abelian groups,
- odd order groups of nilpotency class 2 (Plans 2004),
- D_n for even n (Plans 2004),

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized with $c(G)$ ramified primes.

Evidence

The conjecture holds for:

- finite abelian groups,
- odd order groups of nilpotency class 2 (Plans 2004),
- D_n for even n (Plans 2004),
- 3-groups of order dividing 3^5 (Nomura 2008),

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized with $c(G)$ ramified primes.

Evidence

The conjecture holds for:

- finite abelian groups,
- odd order groups of nilpotency class 2 (Plans 2004),
- D_n for even n (Plans 2004),
- 3-groups of order dividing 3^5 (Nomura 2008),
- all groups of order at most 32 (Boston-Markin 2009),

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized with $c(G)$ ramified primes.

Evidence

The conjecture holds for:

- finite abelian groups,
- odd order groups of nilpotency class 2 (Plans 2004),
- D_n for even n (Plans 2004),
- 3-groups of order dividing 3^5 (Nomura 2008),
- all groups of order at most 32 (Boston-Markin 2009),
- S_n for small values of n (Jones-Roberts 2008, Rabayev 2009),

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized with $c(G)$ ramified primes.

Evidence

The conjecture holds for:

- finite abelian groups,
- odd order groups of nilpotency class 2 (Plans 2004),
- D_n for even n (Plans 2004),
- 3-groups of order dividing 3^5 (Nomura 2008),
- all groups of order at most 32 (Boston-Markin 2009),
- S_n for small values of n (Jones-Roberts 2008, Rabayev 2009),
- many other small order groups.

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized with $c(G)$ ramified primes.

Evidence

The conjecture holds for:

- finite abelian groups,
- odd order groups of nilpotency class 2 (Plans 2004),
- D_n for even n (Plans 2004),
- 3-groups of order dividing 3^5 (Nomura 2008),
- all groups of order at most 32 (Boston-Markin 2009),
- S_n for small values of n (Jones-Roberts 2008, Rabayev 2009),
- many other small order groups.

Semiabelian groups

Definition

The family of semiabelian groups $\mathcal{S}$ is the minimal family for which:

1. $\mathcal{S}$ contains all finite abelian groups;

Semiabelian groups

Definition

The family of semiabelian groups $\mathcal{S}$ is the minimal family for which:

1. $\mathcal{S}$ contains all finite abelian groups;
2. if $G \in \mathcal{S}$ and $G \twoheadrightarrow H$ then $H \in \mathcal{S}$.

Semiabelian groups

Definition

The family of semiabelian groups $\mathcal{S}$ is the minimal family for which:

1. $\mathcal{S}$ contains all finite abelian groups;
2. if $G \in \mathcal{S}$ and $G \twoheadrightarrow H$ then $H \in \mathcal{S}$.
3. if $H \in \mathcal{S}$ and A is an abelian group then any $A \rtimes H \in \mathcal{S}$;

Semiabelian groups

Definition

The family of semiabelian groups $\mathcal{S}$ is the minimal family for which:

1. $\mathcal{S}$ contains all finite abelian groups;
2. if $G \in \mathcal{S}$ and $G \twoheadrightarrow H$ then $H \in \mathcal{S}$.
3. if $H \in \mathcal{S}$ and A is an abelian group then any $A \rtimes H \in \mathcal{S}$;

Small orders (Dentzer)

All groups of order dividing p^4 or 2^5 are semiabelian.

Semiabelian groups

Definition

The family of semiabelian groups $\mathcal{S}$ is the minimal family for which:

1. $\mathcal{S}$ contains all finite abelian groups;
2. if $G \in \mathcal{S}$ and $G \twoheadrightarrow H$ then $H \in \mathcal{S}$.
3. if $H \in \mathcal{S}$ and A is an abelian group then any $A \rtimes H \in \mathcal{S}$;

Small orders (Dentzer)

All groups of order dividing p^4 or 2^5 are semiabelian.

Order	Total	Non-semiabelian
24	15	1
2^6	267	10
3^5	67	10

Semiabelian groups

Definition

The family of semiabelian groups $\mathcal{S}$ is the minimal family for which:

1. $\mathcal{S}$ contains all finite abelian groups;
2. if $G \in \mathcal{S}$ and $G \twoheadrightarrow H$ then $H \in \mathcal{S}$.
3. if $H \in \mathcal{S}$ and A is an abelian group then any $A \rtimes H \in \mathcal{S}$;

Small orders (Dentzer)

All groups of order dividing p^4 or 2^5 are semiabelian.

Order	Total	Non-semiabelian
24	15	1
2^6	267	10
3^5	67	10

Minimal ramification for semiabelian p-groups

A subfamily

The family $\mathcal{G}_p$ is the minimal family for which:

1. $\mathcal{G}_p$ contains all abelian p-groups;

Minimal ramification for semiabelian p-groups

A subfamily

The family $\mathcal{G}_p$ is the minimal family for which:

1. $\mathcal{G}_p$ contains all abelian p-groups;
2. if $H, G \in \mathcal{G}_p$ then $H \wr G = H^{|G|} \rtimes G \in \mathcal{G}_p$;

Minimal ramification for semiabelian p-groups

A subfamily

The family $\mathcal{G}_p$ is the minimal family for which:

1. $\mathcal{G}_p$ contains all abelian p-groups;
2. if $H, G \in \mathcal{G}_p$ then $H \wr G = H^{|G|} \rtimes G \in \mathcal{G}_p$;
3. if $G \in \mathcal{G}_p$ and $G \twoheadrightarrow H$ with $c(G) = c(H)$, then $H \in \mathcal{G}_p$.

Minimal ramification for semiabelian p-groups

A subfamily

The family $\mathcal{G}_p$ is the minimal family for which:

1. $\mathcal{G}_p$ contains all abelian p-groups;
2. if $H, G \in \mathcal{G}_p$ then $H \wr G = H^{|G|} \rtimes G \in \mathcal{G}_p$;
3. if $G \in \mathcal{G}_p$ and $G \twoheadrightarrow H$ with $c(G) = c(H)$, then $H \in \mathcal{G}_p$.

Theorem (Kisilevsky, Sonn)

Every $G \in \mathcal{G}_p$ can be tamely realized over $\mathbb{Q}$ with $c(G)$-ramified primes.

Minimal ramification for semiabelian p-groups

A subfamily

The family $\mathcal{G}_p$ is the minimal family for which:

1. $\mathcal{G}_p$ contains all abelian p-groups;
2. if $H, G \in \mathcal{G}_p$ then $H \wr G = H^{|G|} \rtimes G \in \mathcal{G}_p$;
3. if $G \in \mathcal{G}_p$ and $G \twoheadrightarrow H$ with $c(G) = c(H)$, then $H \in \mathcal{G}_p$.

Theorem (Kisilevsky, Sonn)

Every $G \in \mathcal{G}_p$ can be tamely realized over $\mathbb{Q}$ with $c(G)$-ramified primes.

Theorem (N)

$\mathcal{G}_p$ is the family of semiabelian p-groups.

Minimal ramification for semiabelian p-groups

A subfamily

The family $\mathcal{G}_p$ is the minimal family for which:

1. $\mathcal{G}_p$ contains all abelian p-groups;
2. if $H, G \in \mathcal{G}_p$ then $H \wr G = H^{|G|} \rtimes G \in \mathcal{G}_p$;
3. if $G \in \mathcal{G}_p$ and $G \twoheadrightarrow H$ with $c(G) = c(H)$, then $H \in \mathcal{G}_p$.

Theorem (Kisilevsky, Sonn)

Every $G \in \mathcal{G}_p$ can be tamely realized over $\mathbb{Q}$ with $c(G)$-ramified primes.

Theorem (N)

$\mathcal{G}_p$ is the family of semiabelian p-groups.

An upper bound for semiabelian groups

The wreath length

- A group G is semiabelian if and only if it is an epimorphic image of an iterated wreath product of cyclic groups $G_1, \ldots, G_r$:

$$G_1 \wr (G_2 \wr (\ldots \wr G_r) \ldots) \to G.$$

An upper bound for semiabelian groups

The wreath length

- A group G is semiabelian if and only if it is an epimorphic image of an iterated wreath product of cyclic groups $G_1, \ldots, G_r$:

$$G_1 \wr (G_2 \wr (\ldots \wr G_r) \ldots) \to G.$$

- Let $\mathrm{wl}(G)$ denote the minimal r for which such an epimorphism exists.

An upper bound for semiabelian groups

The wreath length

- A group G is semiabelian if and only if it is an epimorphic image of an iterated wreath product of cyclic groups $G_1, \ldots, G_r$:

$$G_1 \wr (G_2 \wr (\ldots \wr G_r) \ldots) \to G.$$

- Let $\mathrm{wl}(G)$ denote the minimal r for which such an epimorphism exists.

Theorem I(KNS)

Every semiabelian group G can be tamely realized with $\mathrm{wl}(G)$ ramified primes.

An upper bound for semiabelian groups

The wreath length

- A group G is semiabelian if and only if it is an epimorphic image of an iterated wreath product of cyclic groups $G_1, \ldots, G_r$:

$$G_1 \wr (G_2 \wr (\ldots \wr G_r) \ldots) \to G.$$

- Let $\mathrm{wl}(G)$ denote the minimal r for which such an epimorphism exists.

Theorem I(KNS)

Every semiabelian group G can be tamely realized with $\mathrm{wl}(G)$ ramified primes.

Theorem II (KNS)

For every **nilpotent** semiabelian group G, $\mathrm{wl}(G) = c(G)$.

An upper bound for semiabelian groups

The wreath length

- A group G is semiabelian if and only if it is an epimorphic image of an iterated wreath product of cyclic groups $G_1, \dots, G_r$:

$$G_1 \wr (G_2 \wr (\dots \wr G_r) \dots) \to G.$$

- Let $\mathrm{wl}(G)$ denote the minimal r for which such an epimorphism exists.

Theorem I(KNS)

Every semiabelian group G can be tamely realized with $\mathrm{wl}(G)$ ramified primes.

Theorem II (KNS)

For every **nilpotent** semiabelian group G, $\mathrm{wl}(G) = c(G)$.

Consequences

Corollary I - The Boston-Markin conjecture for nilpotent semiabelian groups

Every nilpotent semiabelian group G is tamely realizable over $\mathbb{Q}$ with $c(G)$ ramified primes.

Corollary II

Every group G of nilpotency class 2 is tamely realizable over $\mathbb{Q}$ with $c(G)$ ramified primes.

Consequences

Corollary I - The Boston-Markin conjecture for nilpotent semiabelian groups

Every nilpotent semiabelian group G is tamely realizable over $\mathbb{Q}$ with $c(G)$ ramified primes.

Corollary II

Every group G of nilpotency class 2 is tamely realizable over $\mathbb{Q}$ with $c(G)$ ramified primes.

Examples

Iterated wreath products of cyclic groups

Let $G = G_1 \wr (G_2 \wr \ldots \wr G_r)$ for non-trivial cyclic groups $G_1, \ldots, G_r$.

- $\mathrm{wl}(G) = r$.

Examples

Iterated wreath products of cyclic groups

Let $G = G_1 \wr (G_2 \wr \ldots \wr G_r)$ for non-trivial cyclic groups $G_1, \ldots, G_r$.

- $\mathrm{wl}(G) = r$.
- $c(G) = \mathrm{d}(G^{ab}) = \mathrm{d}(G_1 \times \cdots \times G_r)$.

Examples

Iterated wreath products of cyclic groups

Let $G = G_1 \wr (G_2 \wr \ldots \wr G_r)$ for non-trivial cyclic groups $G_1, \ldots, G_r$.

- $\mathrm{wl}(G) = r$.
- $c(G) = \mathrm{d}(G^{ab}) = \mathrm{d}(G_1 \times \cdots \times G_r)$.
- Therefore $\mathrm{wl}(G) = c(G)$ if and only if there is a prime p that divides the orders of $G_1, \ldots, G_r$.

Examples

Iterated wreath products of cyclic groups

Let $G = G_1 \wr (G_2 \wr \ldots \wr G_r)$ for non-trivial cyclic groups $G_1, \ldots, G_r$.

- $\mathrm{wl}(G) = r$.
- $c(G) = \mathrm{d}(G^{ab}) = \mathrm{d}(G_1 \times \cdots \times G_r)$.
- Therefore $\mathrm{wl}(G) = c(G)$ if and only if there is a prime p that divides the orders of $G_1, \ldots, G_r$.
- $G = C_3 \wr C_6$ can be realized with $\mathrm{wl}(G) = c(G) = 2$ ramified primes.

Examples

Iterated wreath products of cyclic groups

Let $G = G_1 \wr (G_2 \wr \ldots \wr G_r)$ for non-trivial cyclic groups $G_1, \ldots, G_r$.

- $\mathrm{wl}(G) = r$.
- $c(G) = \mathrm{d}(G^{ab}) = \mathrm{d}(G_1 \times \cdots \times G_r)$.
- Therefore $\mathrm{wl}(G) = c(G)$ if and only if there is a prime p that divides the orders of $G_1, \ldots, G_r$.
- $G = C_3 \wr C_6$ can be realized with $\mathrm{wl}(G) = c(G) = 2$ ramified primes.

Classical examples of iterated wreath products

Examples

Iterated wreath products of cyclic groups

Let $G = G_1 \wr (G_2 \wr \ldots \wr G_r)$ for non-trivial cyclic groups $G_1, \ldots, G_r$.

- $\mathrm{wl}(G) = r$.
- $c(G) = \mathrm{d}(G^{ab}) = \mathrm{d}(G_1 \times \cdots \times G_r)$.
- Therefore $\mathrm{wl}(G) = c(G)$ if and only if there is a prime p that divides the orders of $G_1, \ldots, G_r$.
- $G = C_3 \wr C_6$ can be realized with $\mathrm{wl}(G) = c(G) = 2$ ramified primes.

Classical examples of iterated wreath products

- The Sylow subgroups of S_n are direct products of iterated wreath products.

Examples

Iterated wreath products of cyclic groups

Let $G = G_1 \wr (G_2 \wr \ldots \wr G_r)$ for non-trivial cyclic groups $G_1, \ldots, G_r$.

- $\mathrm{wl}(G) = r$.
- $c(G) = \mathrm{d}(G^{ab}) = \mathrm{d}(G_1 \times \cdots \times G_r)$.
- Therefore $\mathrm{wl}(G) = c(G)$ if and only if there is a prime p that divides the orders of $G_1, \ldots, G_r$.
- $G = C_3 \wr C_6$ can be realized with $\mathrm{wl}(G) = c(G) = 2$ ramified primes.

Classical examples of iterated wreath products

- The Sylow subgroups of S_n are direct products of iterated wreath products.
- The p-Sylow subgroups of $GL_n(F_q)$, where q is a prime power and $(q,p) = 1$, are iterated wreath products.

Examples

Iterated wreath products of cyclic groups

Let $G = G_1 \wr (G_2 \wr \ldots \wr G_r)$ for non-trivial cyclic groups $G_1, \ldots, G_r$.

- $\mathrm{wl}(G) = r$.
- $c(G) = \mathrm{d}(G^{ab}) = \mathrm{d}(G_1 \times \cdots \times G_r)$.
- Therefore $\mathrm{wl}(G) = c(G)$ if and only if there is a prime p that divides the orders of $G_1, \ldots, G_r$.
- $G = C_3 \wr C_6$ can be realized with $\mathrm{wl}(G) = c(G) = 2$ ramified primes.

Classical examples of iterated wreath products

- The Sylow subgroups of S_n are direct products of iterated wreath products.
- The p-Sylow subgroups of $GL_n(F_q)$, where q is a prime power and $(q,p) = 1$, are iterated wreath products.

Other semiabelian groups

Open cases

- For n odd and $G = D_n$ the tame minimal ramification problem is equivalent to:

$$\begin{array}{c} K \\ C_n \Big| \text{-unramified} \\ M \\ 2 \Big| \text{-with prime discriminant} \\ \mathbb{Q} \end{array}$$

Other semiabelian groups

Open cases

- For n odd and $G = D_n$ the tame minimal ramification problem is equivalent to:

$$\begin{array}{c} K \\ C_n \Big| \text{ -unramified} \\ M \\ 2 \Big| \text{-with prime discriminant} \\ \mathbb{Q} \end{array}$$

- Let $p_1, \ldots, p_r$ be distinct primes. Can $G = C_{p_1} \wr \ldots \wr C_{p_r}$ be realized with 1 ramified prime?

Other semiabelian groups

Open cases

- For n odd and $G = D_n$ the tame minimal ramification problem is equivalent to:

$$\begin{array}{c} K \\ C_n \Big| \text{ -unramified} \\ M \\ 2 \Big| \text{ -with prime discriminant} \\ \mathbb{Q} \end{array}$$

- Let $p_1, \ldots, p_r$ be distinct primes. Can $G = C_{p_1} \wr \ldots \wr C_{p_r}$ be realized with 1 ramified prime?

Proof of Theorem I - by example

Recall: Theorem I

Every semiabelian group G can be tamely realized with $\mathrm{wl}(G)$ ramified primes.

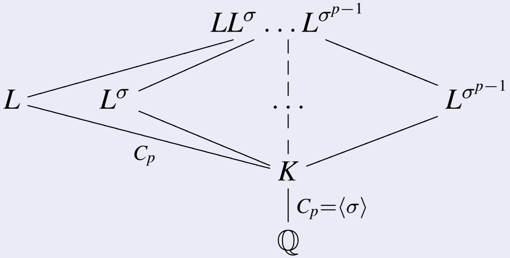
$G = C_p \wr C_p$ with two ramified primes

Proof of Theorem I - by example

Recall: Theorem I

Every semiabelian group G can be tamely realized with $\mathrm{wl}(G)$ ramified primes.

$G = C_p \wr C_p$ with two ramified primes



Splitting Lemma

Splitting Lemma, Kisilevsky-Sonn (2005)

Let K be a number field and r an integer. There is a number field $K_r \supseteq K$ such that for every prime $\mathfrak{p}$ of K that splits completely in K_r there is a C_{p^r}-extension of K that is ramified only at $\mathfrak{p}$ and is totally ramified there.

Remark

There are number fields $K_1, \ldots, K_m$ containing K such that there is a C_{p^r}-extension of K that is ramified only at $\mathfrak{p}$ and is totally ramified there if and only if $\mathfrak{p}$ splits completely in at least one of the fields $K_1, \ldots, K_m$.

Splitting Lemma

Splitting Lemma, Kisilevsky-Sonn (2005)

Let K be a number field and r an integer. There is a number field $K_r \supseteq K$ such that for every prime $\mathfrak{p}$ of K that splits completely in K_r there is a C_{p^r}-extension of K that is ramified only at $\mathfrak{p}$ and is totally ramified there.

Remark

There are number fields $K_1, \ldots, K_m$ containing K such that there is a C_{p^r}-extension of K that is ramified only at $\mathfrak{p}$ and is totally ramified there if and only if $\mathfrak{p}$ splits completely in at least one of the fields $K_1, \ldots, K_m$.

Proof of Theorem II - p-groups

Theorem II for p-groups (Recall)

Let G be a semiabelian p-group and $c := c(G)$. Then $wl(G) = c(G)$, i.e. there are cyclic groups $G_1, \ldots, G_c$ and an epimorphism $G_1 \wr (G_2 \wr \ldots \wr G_c) \to G$.

Equivalent formulation

There are cyclic p-groups $G_1, \ldots, G_r$ and a c-preserving epimorphism $G_1 \wr (G_2 \wr \ldots \wr G_r) \to G$.

Proof of Theorem II - p-groups

Theorem II for p-groups (Recall)

Let G be a semiabelian p-group and $c := c(G)$. Then $wl(G) = c(G)$, i.e. there are cyclic groups $G_1, \dots, G_c$ and an epimorphism $G_1 \wr (G_2 \wr \dots \wr G_c) \to G$.

Equivalent formulation

There are cyclic p-groups $G_1, \dots, G_r$ and a c-preserving epimorphism $G_1 \wr (G_2 \wr \dots \wr G_r) \to G$.

Proof of Theorem II, Step I, Decompositions

Lemma (Dentzer)

A non-trivial group G is semiabelian if and only if $G = AH$ for abelian $A \lhd G$ and a proper semiabelian subgroup $H < G$.

A Minimal Decomposition

Let G be a non-trivial semiabelian group. A minimal decomposition of G is a decomposition $G = AH$ such that:

Proof of Theorem II, Step I, Decompositions

Lemma (Dentzer)

A non-trivial group G is semiabelian if and only if $G = AH$ for abelian $A \lhd G$ and a proper semiabelian subgroup $H < G$.

A Minimal Decomposition

Let G be a non-trivial semiabelian group. A minimal decomposition of G is a decomposition $G = AH$ such that:

- $A \lhd G$ is a minimal normal subgroup for which there is a proper semiabelian subgroup $H_0 < G$ with $G = AH_0$,

Proof of Theorem II, Step I, Decompositions

Lemma (Dentzer)

A non-trivial group G is semiabelian if and only if $G = AH$ for abelian $A \lhd G$ and a proper semiabelian subgroup $H < G$.

A Minimal Decomposition

Let G be a non-trivial semiabelian group. A minimal decomposition of G is a decomposition $G = AH$ such that:

- $A \lhd G$ is a minimal normal subgroup for which there is a proper semiabelian subgroup $H_0 < G$ with $G = AH_0$,
- $H < G$ is a minimal subgroup for which $G = AH$.

Proof of Theorem II, Step I, Decompositions

Lemma (Dentzer)

A non-trivial group G is semiabelian if and only if $G = AH$ for abelian $A \lhd G$ and a proper semiabelian subgroup $H < G$.

A Minimal Decomposition

Let G be a non-trivial semiabelian group. A minimal decomposition of G is a decomposition $G = AH$ such that:

- $A \lhd G$ is a minimal normal subgroup for which there is a proper semiabelian subgroup $H_0 < G$ with $G = AH_0$,
- $H < G$ is a minimal subgroup for which $G = AH$.

Step I

Let G be a non-trivial semiabelian group and $G = AH$ a minimal decomposition. Then the induced epimorphism $A \rtimes H \to G = AH$ is c-preserving.

Proof of Theorem II, Step I, Decompositions

Lemma (Dentzer)

A non-trivial group G is semiabelian if and only if $G = AH$ for abelian $A \lhd G$ and a proper semiabelian subgroup $H < G$.

A Minimal Decomposition

Let G be a non-trivial semiabelian group. A minimal decomposition of G is a decomposition $G = AH$ such that:

- $A \lhd G$ is a minimal normal subgroup for which there is a proper semiabelian subgroup $H_0 < G$ with $G = AH_0$,
- $H < G$ is a minimal subgroup for which $G = AH$.

Step I

Let G be a non-trivial semiabelian group and $G = AH$ a minimal decomposition. Then the induced epimorphism $A \rtimes H \to G = AH$ is c-preserving.

Proof of Theorem II, Step II, Wreath Products

Step I

Let G be a non-trivial semiabelian group and $G = AH$ a minimal decomposition. Then the induced epimorphism $A \rtimes H \to G = AH$ is c-preserving.

Step II

There is an epimorphism $\pi : A \wr H = A^{|H|} \rtimes H \to A \rtimes H$. Let B be a minimal subgroup of A for which the restriction of π to $B \wr H$ is an epimorphism. Then $\pi : B \wr H \to A \rtimes H$ is c-preserving.

Proof of Theorem II, Step II, Wreath Products

Step I

Let G be a non-trivial semiabelian group and $G = AH$ a minimal decomposition. Then the induced epimorphism $A \rtimes H \to G = AH$ is c-preserving.

Step II

There is an epimorphism $\pi : A \wr H = A^{|H|} \rtimes H \to A \rtimes H$. Let B be a minimal subgroup of A for which the restriction of π to $B \wr H$ is an epimorphism. Then $\pi : B \wr H \to A \rtimes H$ is c-preserving.

Iterating

Take a minimal decomposition $H = A_2 H_2$ and obtain B_2 using Step II. We get a corresponding c-preserving epimorphism $B \wr (B_2 \wr H_2) \to G$.

Proof of Theorem II, Step II, Wreath Products

Step I

Let G be a non-trivial semiabelian group and $G = AH$ a minimal decomposition. Then the induced epimorphism $A \rtimes H \to G = AH$ is c-preserving.

Step II

There is an epimorphism $\pi : A \wr H = A^{|H|} \rtimes H \to A \rtimes H$. Let B be a minimal subgroup of A for which the restriction of π to $B \wr H$ is an epimorphism. Then $\pi : B \wr H \to A \rtimes H$ is c-preserving.

Iterating

Take a minimal decomposition $H = A_2H_2$ and obtain B_2 using Step II. We get a corresponding c-preserving epimorphism $B \wr (B_2 \wr H_2) \to G$. Iterating this process we obtain abelian p-groups $B_1, \ldots, B_r$ and a c-preserving epimorphism $B_1 \wr (B_2 \wr \ldots \wr B_r) \to G$.

Proof of Theorem II, Step II, Wreath Products

Step I

Let G be a non-trivial semiabelian group and $G = AH$ a minimal decomposition. Then the induced epimorphism $A \rtimes H \to G = AH$ is c-preserving.

Step II

There is an epimorphism $\pi : A \wr H = A^{|H|} \rtimes H \to A \rtimes H$. Let B be a minimal subgroup of A for which the restriction of π to $B \wr H$ is an epimorphism. Then $\pi : B \wr H \to A \rtimes H$ is c-preserving.

Iterating

Take a minimal decomposition $H = A_2H_2$ and obtain B_2 using Step II. We get a corresponding c-preserving epimorphism $B \wr (B_2 \wr H_2) \to G$. Iterating this process we obtain abelian p-groups $B_1, \ldots, B_r$ and a c-preserving epimorphism $B_1 \wr (B_2 \wr \ldots \wr B_r) \to G$.

Questions?

You can find both the slides and the paper at

`http://www-personal.umich.edu/~neftin/index.html`