

On the minimal ramification problem for semiabelian groups

DANNY NEFTIN

JOINT WITH HERSHY KISILEVSKY AND JACK SONN

Department of Mathematics
Technion - Israel Institute of Technology
Haifa, Israel

<http://www.math.technion.ac.il/~neftind>

Midwest Number Theory Conference for Graduate Students 2010

Restricted Ramification

Prime decomposition

Let G be a finite group.

Restricted Ramification

Prime decomposition

Let G be a finite group.

Number fields

$$\begin{array}{c} K \\ | \\ \mathbb{Q} \end{array} \quad G$$

Restricted Ramification

Prime decomposition

Let G be a finite group.

Number fields

Rings of integers

$$\begin{array}{c} K \\ | \\ \mathbb{Q} \end{array} \quad G$$

$$\begin{array}{c} O_K \\ | \\ \mathbb{Z} \end{array}$$

Restricted Ramification

Prime decomposition

Let G be a finite group.

Number fields

$$\begin{array}{c} K \\ | \\ \mathbb{Q} \end{array} \quad G$$

Rings of integers

$$\begin{array}{c} \mathcal{O}_K \\ | \\ \mathbb{Z} \end{array}$$

Primes

$$\begin{array}{c} (p) = \mathfrak{p}_1^e \cdots \mathfrak{p}_r^e \\ | \\ p \end{array}$$

Recall: p is *ramified* if $e > 1$.

Restricted Ramification

Prime decomposition

Let G be a finite group.

Number fields

Rings of integers

Primes

$$\begin{array}{c} K \\ | \\ \mathbb{Q} \end{array} \begin{array}{c} \\ G \\ \end{array}$$

$$\begin{array}{c} O_K \\ | \\ \mathbb{Z} \end{array}$$

$$\begin{array}{c} (p) = \mathfrak{p}_1^e \cdots \mathfrak{p}_r^e \\ | \\ p \end{array}$$

Recall: p is *ramified* if $e > 1$.

Problem

Given a group G and a finite set S of rational primes. When is there a G -extension ramified only at primes of S ?

Restricted Ramification

Prime decomposition

Let G be a finite group.

Number fields

Rings of integers

Primes

$$\begin{array}{c} K \\ | \\ \mathbb{Q} \end{array} \begin{array}{c} G \\ | \\ \end{array}$$

$$\begin{array}{c} O_K \\ | \\ \mathbb{Z} \end{array}$$

$$\begin{array}{c} (p) = \mathfrak{p}_1^e \cdots \mathfrak{p}_r^e \\ | \\ p \end{array}$$

Recall: p is *ramified* if $e > 1$.

Problem

Given a group G and a finite set S of rational primes. When is there a G -extension ramified only at primes of S ?

The Minimal Ramification Problem

Problem

Given a finite group G :

What is the minimal number of ramified primes in a G -extension of \mathbb{Q} ?

Open cases:

The Minimal Ramification Problem

Problem

Given a finite group G :

What is the minimal number of ramified primes in a G -extension of \mathbb{Q} ?

Open cases:

- Nilpotent groups,

The Minimal Ramification Problem

Problem

Given a finite group G :

What is the minimal number of ramified primes in a G -extension of \mathbb{Q} ?

Open cases:

- Nilpotent groups,
- Dihedral groups D_n ,

The Minimal Ramification Problem

Problem

Given a finite group G :

What is the minimal number of ramified primes in a G -extension of \mathbb{Q} ?

Open cases:

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

The Minimal Ramification Problem

Problem

Given a finite group G :

What is the minimal number of ramified primes in a G -extension of \mathbb{Q} ?

Open cases:

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

A lower bound

Consequences from Minkowski's Theorem

- In any non-trivial extension of \mathbb{Q} there exists a ramified prime.

A lower bound

Consequences from Minkowski's Theorem

- In any non-trivial extension of \mathbb{Q} there exists a ramified prime.
- If G is abelian there are at least $\text{rk}(G)$ ramified primes (including the infinite prime).

A lower bound

Consequences from Minkowski's Theorem

- In any non-trivial extension of \mathbb{Q} there exists a ramified prime.
- If G is abelian there are at least $\text{rk}(G)$ ramified primes (including the infinite prime).
- Generally, for a group $G \neq \{1\}$ the number of ramified primes is at least:

$$d(G) := \begin{cases} \text{rk}(G/[G, G]) \end{cases}$$

A lower bound

Consequences from Minkowski's Theorem

- In any non-trivial extension of \mathbb{Q} there exists a ramified prime.
- If G is abelian there are at least $\text{rk}(G)$ ramified primes (including the infinite prime).
- Generally, for a group $G \neq \{1\}$ the number of ramified primes is at least:

$$d(G) := \begin{cases} \text{rk}(G/[G, G]) & \text{if } G \neq [G, G] \\ 1 & \text{if } G = [G, G]. \end{cases}$$

A lower bound

Consequences from Minkowski's Theorem

- In any non-trivial extension of \mathbb{Q} there exists a ramified prime.
- If G is abelian there are at least $\text{rk}(G)$ ramified primes (including the infinite prime).
- Generally, for a group $G \neq \{1\}$ the number of ramified primes is at least:

$$d(G) := \begin{cases} \text{rk}(G/[G, G]) & \text{if } G \neq [G, G] \\ 1 & \text{if } G = [G, G]. \end{cases}$$

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized over \mathbb{Q} with $d(G)$ ramified primes.

Previous Evidence

The conjecture holds for:

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized over \mathbb{Q} with $d(G)$ ramified primes.

Previous Evidence

The conjecture holds for:

- abelian groups,

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized over \mathbb{Q} with $d(G)$ ramified primes.

Previous Evidence

The conjecture holds for:

- 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 over \mathbb{Q} with $d(G)$ ramified primes.

Previous Evidence

The conjecture holds for:

- 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 over \mathbb{Q} with $d(G)$ ramified primes.

Previous Evidence

The conjecture holds for:

- 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 over \mathbb{Q} with $d(G)$ ramified primes.

Previous Evidence

The conjecture holds for:

- 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),
- S_n for a few small values of n (Jones-Roberts 2008, Rebayev 2009),

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized over \mathbb{Q} with $d(G)$ ramified primes.

Previous Evidence

The conjecture holds for:

- 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),
- S_n for a few small values of n (Jones-Roberts 2008, Rebayev 2009),
- groups of order at most 32 (Boston-Markin 2009),

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized over \mathbb{Q} with $d(G)$ ramified primes.

Previous Evidence

The conjecture holds for:

- 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),
- S_n for a few small values of n (Jones-Roberts 2008, Rebayev 2009),
- groups of order at most 32 (Boston-Markin 2009),
- many other small order groups.

The Conjecture

The Boston-Markin Conjecture (2009)

Every finite group G can be realized over \mathbb{Q} with $d(G)$ ramified primes.

Previous Evidence

The conjecture holds for:

- 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),
- S_n for a few small values of n (Jones-Roberts 2008, Rebayev 2009),
- groups of order at most 32 (Boston-Markin 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 abelian groups;

Semiabelian groups

Definition

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

- 1 \mathcal{S} contains all abelian groups;
- 2 if $G \in \mathcal{S}$ and $G \rightarrow H$ 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 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 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 $A \rtimes H \in \mathcal{S}$;

Frequency (Dentzer, Schneps)

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 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 $A \rtimes H \in \mathcal{S}$;

Frequency (Dentzer, Schneps)

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

Order	Total	Non-semiabelian
2^6	267	10
2^7	2328	82
3^5	67	10
3^6	504	54

Semiabelian groups

Definition

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

- 1 \mathcal{S} contains all 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 $A \rtimes H \in \mathcal{S}$;

Frequency (Dentzer, Schneps)

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

Order	Total	Non-semiabelian
2^6	267	10
2^7	2328	82
3^5	67	10
3^6	504	54

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 $G \rightarrow H$ with $d(G) = d(H)$, 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 $G \rightarrow H$ with $d(G) = d(H)$, then $H \in \mathcal{G}_p$.

Theorem (Kisilevsky, Sonn)

Every $G \in \mathcal{G}_p$ can be realized over \mathbb{Q} with $d(G)$ -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 $G \rightarrow H$ with $d(G) = d(H)$, then $H \in \mathcal{G}_p$.

Theorem (Kisilevsky, Sonn)

Every $G \in \mathcal{G}_p$ can be realized over \mathbb{Q} with $d(G)$ -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 $G \rightarrow H$ with $d(G) = d(H)$, then $H \in \mathcal{G}_p$.

Theorem (Kisilevsky, Sonn)

Every $G \in \mathcal{G}_p$ can be realized over \mathbb{Q} with $d(G)$ -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, \dots, G_r :

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

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 :

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

- Let $wl(G)$ 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, \dots, G_r :

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

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

Theorem (KNS)

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 :

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

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

Theorem (KNS)

- ① Every semiabelian group G can be realized with $wl(G)$ 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, \dots, G_r :

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

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

Theorem (KNS)

- 1 Every semiabelian group G can be realized with $\text{wl}(G)$ ramified primes.
- 2 For every **nilpotent** semiabelian group G , $\text{wl}(G) = d(G)$.

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 :

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

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

Theorem (KNS)

- 1 Every semiabelian group G can be realized with $\text{wl}(G)$ ramified primes.
- 2 For every **nilpotent** semiabelian group G , $\text{wl}(G) = d(G)$.

Consequences Proof Other groups End

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 :

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

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

Theorem (KNS)

- 1 Every semiabelian group G can be realized with $wl(G)$ ramified primes.
- 2 For every **nilpotent** semiabelian group G , $wl(G) = d(G)$.

Consequences

Proof

Other groups

End

Consequences

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

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

Corollary II

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

Consequences

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

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

Corollary II

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

Iterated wreath products

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

Consequences

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

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

Corollary II

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

Iterated wreath products

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

- $wl(G) = r$.

Consequences

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

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

Corollary II

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

Iterated wreath products

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

- $wl(G) = r$.
- $d(G) = \text{rk}(G_1 \times \dots \times G_r)$.

Consequences

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

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

Corollary II

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

Iterated wreath products

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

- $wl(G) = r$.
- $d(G) = \text{rk}(G_1 \times \dots \times G_r)$.
- $wl(G) = d(G)$ if and only if there is a prime p that divides all $|G_i|$.

Consequences

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

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

Corollary II

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

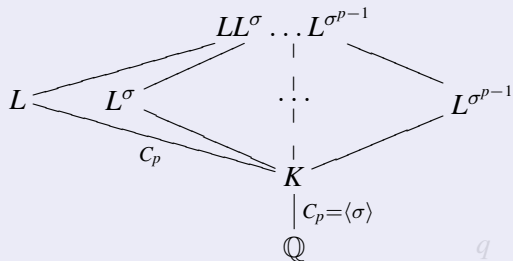
Iterated wreath products

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

- $wl(G) = r$.
- $d(G) = \text{rk}(G_1 \times \dots \times G_r)$.
- $wl(G) = d(G)$ if and only if there is a prime p that divides all $|G_i|$.

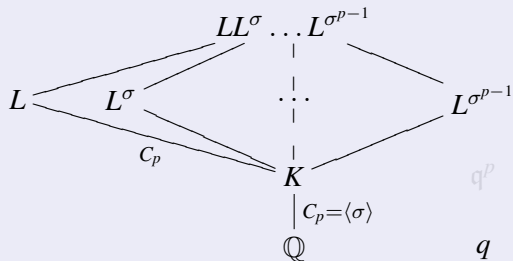
Example

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



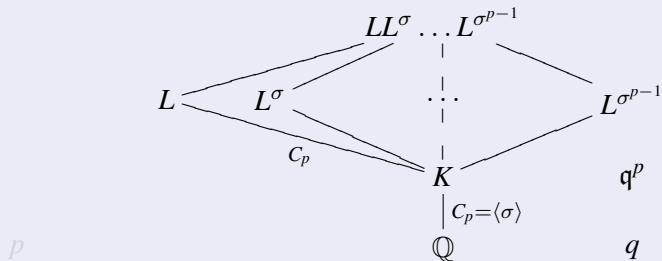
Example

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



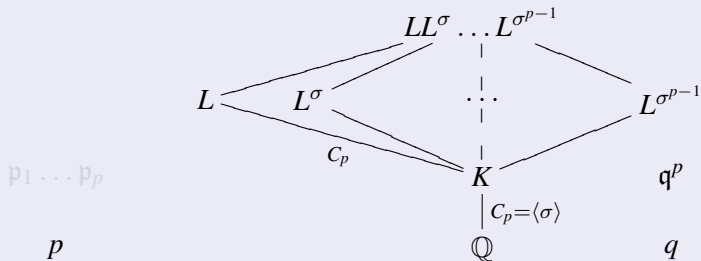
Example

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



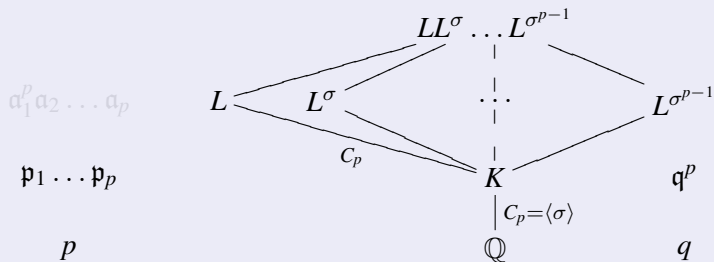
Example

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



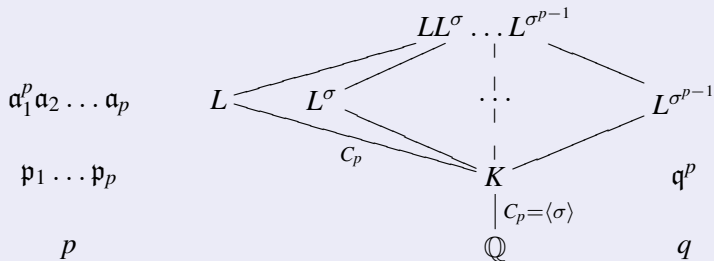
Example

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



Example

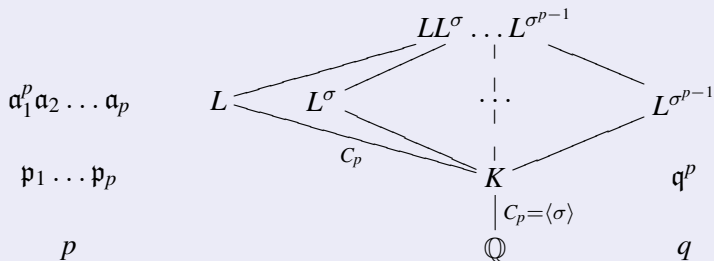
$G = C_p \wr C_p$ with two ramified primes



To find such a p we use:

Example

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



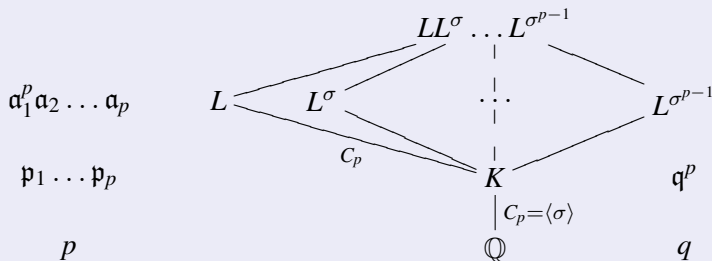
To find such a p we use:

Splitting Lemma, Kisilevsky-Sonn (2005)

Let K be a number field and $r \in \mathbb{N}$. 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 at \mathfrak{p} and only at \mathfrak{p} .

Example

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



To find such a p we use:

Splitting Lemma, Kisilevsky-Sonn (2005)

Let K be a number field and $r \in \mathbb{N}$. 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 at \mathfrak{p} and only at \mathfrak{p} .

Other semiabelian groups

Open cases

- $G = C_p \wr C_q$ for distinct primes p, q .

Other semiabelian groups

Open cases

- $G = C_p \wr C_q$ for distinct primes p, q .
- For n odd and $G = D_n$ the tame minimal ramification problem is equivalent to:

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

Other semiabelian groups

Open cases

- $G = C_p \wr C_q$ for distinct primes p, q .
- For n odd and $G = D_n$ the tame minimal ramification problem is equivalent to:

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

- Only finitely many S_3 -extensions with 1 ramified prime are known.

Other semiabelian groups

Open cases

- $G = C_p \wr C_q$ for distinct primes p, q .
- For n odd and $G = D_n$ the tame minimal ramification problem is equivalent to:

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

- Only finitely many S_3 -extensions with 1 ramified prime are known.

Questions?

You can find both the slides and the paper at

<http://www.technion.ac.il/~neftin>