Computing Pro-p Galois Groups

Nigel Boston and Harris Nover

July 22, 2006

Overview of the Talk

- Finite Galois Groups

Overview of the Talk

- Finite Galois Groups
- Infinite Galois Groups

Overview of the Talk

- Finite Galois Groups
- Infinite Galois Groups
- Combining Group Theory and Number Theory Computations

Notation

- $K-$ number field

Notation

- $K-$ number field
- $p-$ rational prime (usually $p = 2$)

Notation

- $K-$ number field
- $p-$ rational prime (usually $p = 2$)
- $S-$ finite set of primes of K none lying above p

Notation

- $K-$ number field
- $p-$ rational prime (usually $p = 2$)
- $S-$ finite set of primes of K none lying above p
- K^S- union of p-extensions of K unramified outside S

Notation

- $K-$ number field
- $p-$ rational prime (usually $p = 2$)
- $S-$ finite set of primes of K none lying above p
- K^S- union of p-extensions of K unramified outside S
- $G-$ $\mathrm{Gal}(K^S/K)$

Why We Care About G

- p-class towers of historical importance (the case of $S = \emptyset$)

Why We Care About G

- p-class towers of historical importance (the case of $S = \emptyset$)
- Root-discriminant bounds: e.g. among totally complex K, how small can $rd(K) := |Disc(K)|^{1/[K:\mathbf{Q}]}$ be? Under GRH, $Liminf \geq 44$. Record: $Liminf \leq 82$ (Hajir-Maire).

Why We Care About G

- p-class towers of historical importance (the case of $S = \emptyset$)
- Root-discriminant bounds: e.g. among totally complex K, how small can $rd(K) := |Disc(K)|^{1/[K:\mathbf{Q}]}$ be? Under GRH, $Liminf \geq 44$. Record: $Liminf \leq 82$ (Hajir-Maire).
- Note: If L/K is unramified, then $rd(L) = rd(K)$. So if $\mathrm{Gal}(K^{\emptyset}/K)$ is infinite, then above $Liminf \leq rd(K)$.

Why We Care About G

- p-class towers of historical importance (the case of $S = \emptyset$)
- Root-discriminant bounds: e.g. among totally complex K, how small can $rd(K) := |Disc(K)|^{1/[K:\mathbf{Q}]}$ be? Under GRH, $Liminf \geq 44$. Record: $Liminf \leq 82$ (Hajir-Maire).
- Note: If L/K is unramified, then $rd(L) = rd(K)$. So if $\mathrm{Gal}(K^{\emptyset}/K)$ is infinite, then above $Liminf \leq rd(K)$.
- The tame case of the Fontaine-Mazur Conjecture: every p-adic representation $G \to GL_n(\mathbf{Z}_p)$ has finite image.

Why We Care About G

- p-class towers of historical importance (the case of $S = \emptyset$)
- Root-discriminant bounds: e.g. among totally complex K, how small can $rd(K) := |Disc(K)|^{1/[K:\mathbf{Q}]}$ be? Under GRH, $Liminf \geq 44$. Record: $Liminf \leq 82$ (Hajir-Maire).
- Note: If L/K is unramified, then $rd(L) = rd(K)$. So if $\mathrm{Gal}(K^{\emptyset}/K)$ is infinite, then above $Liminf \leq rd(K)$.
- The tame case of the Fontaine-Mazur Conjecture: every p-adic representation $G \to GL_n(\mathbf{Z}_p)$ has finite image.
- Interesting pro-p groups arise for group theorists.

Ingredients

- Our goal is to find G. We know various things about G.

Ingredients

- Our goal is to find G. We know various things about G.
- If H is a subgroup of finite index, it equals $\mathrm{Gal}(K^S/L)$ for some number field L.

Ingredients

- Our goal is to find G. We know various things about G.
- If H is a subgroup of finite index, it equals $\mathrm{Gal}(K^S/L)$ for some number field L.
- By class field theory, its maximal abelian quotient H/H' is isomorphic to the p-primary part $Cl_S(L)$ of a ray class group of L (and in particular is finite).

Ingredients

- Our goal is to find G. We know various things about G.
- If H is a subgroup of finite index, it equals $\mathrm{Gal}(K^S/L)$ for some number field L.
- By class field theory, its maximal abelian quotient H/H' is isomorphic to the p-primary part $Cl_S(L)$ of a ray class group of L (and in particular is finite).
- By Burnside's basis theorem, the generator rank $d(G)$ equals $d(G/G') = d(Cl_S(K))$.

Ingredients

- Our goal is to find G. We know various things about G.
- If H is a subgroup of finite index, it equals $\mathrm{Gal}(K^S/L)$ for some number field L.
- By class field theory, its maximal abelian quotient H/H' is isomorphic to the p-primary part $Cl_S(L)$ of a ray class group of L (and in particular is finite).
- By Burnside's basis theorem, the generator rank $d(G)$ equals $d(G/G') = d(Cl_S(K))$.
- Shafarevich: $0 \leq r(G) - d(G) \leq r_1 + r_2 - 1 + \theta_S$ ($\theta_S = 0, 1$).

Ingredients

- Our goal is to find G. We know various things about G.
- If H is a subgroup of finite index, it equals $\mathrm{Gal}(K^S/L)$ for some number field L.
- By class field theory, its maximal abelian quotient H/H' is isomorphic to the p-primary part $Cl_S(L)$ of a ray class group of L (and in particular is finite).
- By Burnside's basis theorem, the generator rank $d(G)$ equals $d(G/G') = d(Cl_S(K))$.
- Shafarevich: $0 \leq r(G) - d(G) \leq r_1 + r_2 - 1 + \theta_S$ ($\theta_S = 0, 1$).
- In certain cases, e.g. $K = \mathbf{Q}$, the relations of G come from local, i.e. tame, relations. These say that the generator τ_i of inertia at $q_i \in S$ satisfies $\tau_i^{\sigma_i} = \tau_i^{q_i}$ - note we do not know the Frobenius elements σ_i in terms of the generators τ_i of G.

Finite G

- Our strategy (NB, Leedham-Green) is to search for G by finding successively larger quotients of it, namely its p-central series quotients.

Finite G

- Our strategy (NB, Leedham-Green) is to search for G by finding successively larger quotients of it, namely its p-central series quotients.
- Bad news: sometimes we find a short list of candidates for G, rather than a unique G.

Finite G

- Our strategy (NB, Leedham-Green) is to search for G by finding successively larger quotients of it, namely its p-central series quotients.
- Bad news: sometimes we find a short list of candidates for G, rather than a unique G.
- Good news: these candidates are usually so similar that any question you ask of them (order, nilpotency class, ...) will have a unique answer.

Finite G

- Our strategy (NB, Leedham-Green) is to search for G by finding successively larger quotients of it, namely its p-central series quotients.
- Bad news: sometimes we find a short list of candidates for G, rather than a unique G.
- Good news: these candidates are usually so similar that any question you ask of them (order, nilpotency class, ...) will have a unique answer.
- We focus on fields K such that $rd(K)$ is small but $Cl_\emptyset(K)$ is large.

Finite G

- Our strategy (NB, Leedham-Green) is to search for G by finding successively larger quotients of it, namely its p-central series quotients.
- Bad news: sometimes we find a short list of candidates for G, rather than a unique G.
- Good news: these candidates are usually so similar that any question you ask of them (order, nilpotency class, ...) will have a unique answer.
- We focus on fields K such that $rd(K)$ is small but $Cl_\emptyset(K)$ is large.
- The method also yields theoretical results (same input $\Longrightarrow$ same output) E.g. Benjamin, Lemmermeyer, Snyder computed 2-class towers of imaginary quadratic K with $Cl_\emptyset(K) = [2, 2, 2]$ but left gaps.

O'Brien's Algorithm

- The lower p-central series of a p-group G is given by: $P_0(G) = G, \quad P_{k+1}(G) = P_k(G)^p[G, P_k(G)].$ So $G = P_0(G) \geq P_1(G) \geq \ldots$

O'Brien's Algorithm

- The lower p-central series of a p-group G is given by: $P_0(G) = G, \quad P_{k+1}(G) = P_k(G)^p[G, P_k(G)].$ So $G = P_0(G) \geq P_1(G) \geq \ldots$
- The smallest c such that $P_c(G) = \{1\}$ is the p-class of G.

O'Brien's Algorithm

- The lower p-central series of a p-group G is given by: $P_0(G) = G, \quad P_{k+1}(G) = P_k(G)^p[G, P_k(G)].$ So $G = P_0(G) \geq P_1(G) \geq \ldots$
- The smallest c such that $P_c(G) = \{1\}$ is the p-class of G.
- We obtain a sequence of p-quotients $G = G/P_c(G) \to G/P_{c-1}(G) \to \ldots G/P_1(G) \cong (\mathbf{Z}/p)^{d(G)}$.

O'Brien's Algorithm

- The lower p-central series of a p-group G is given by: $P_0(G) = G, \quad P_{k+1}(G) = P_k(G)^p[G, P_k(G)]$. So $G = P_0(G) \geq P_1(G) \geq \ldots$
- The smallest c such that $P_c(G) = \{1\}$ is the p-class of G.
- We obtain a sequence of p-quotients $G = G/P_c(G) \to G/P_{c-1}(G) \to \ldots G/P_1(G) \cong (\mathbf{Z}/p)^{d(G)}$.
- If $H \cong G/P_{k+1}(G)$ and $K \cong G/P_k(G)$, we say that H is an immediate descendant of K.

O'Brien's Algorithm

- The lower p-central series of a p-group G is given by: $P_0(G) = G, \quad P_{k+1}(G) = P_k(G)^p[G, P_k(G)].$ So $G = P_0(G) \geq P_1(G) \geq \ldots$
- The smallest c such that $P_c(G) = \{1\}$ is the p-class of G.
- We obtain a sequence of p-quotients $G = G/P_c(G) \to G/P_{c-1}(G) \to \ldots G/P_1(G) \cong (\mathbf{Z}/p)^{d(G)}$.
- If $H \cong G/P_{k+1}(G)$ and $K \cong G/P_k(G)$, we say that H is an immediate descendant of K.
- O'Brien's algorithm finds all immediate descendants of a given p-group K (up to isomorphism).

Method with Leedham-Green

- To find our Galois group G, we successively find $G/P_k(G)$ $(k = 1, 2, \ldots)$.

Method with Leedham-Green

- To find our Galois group G, we successively find $G/P_k(G)$ $(k = 1, 2, ...)$.
- Note that $G/P_1(G) = (\mathbf{Z}/p)^{d(G)}$ and $d(G) = d(Cl_S(K))$.

Method with Leedham-Green

- To find our Galois group G, we successively find $G/P_k(G)$ $(k = 1, 2, ...)$.
- Note that $G/P_1(G) = (\mathbf{Z}/p)^{d(G)}$ and $d(G) = d(Cl_S(K))$.
- Given $G/P_{k-1}(G)$, O'Brien's algorithm yields all possible $G/P_k(G)$.

Method with Leedham-Green

- To find our Galois group G, we successively find $G/P_k(G)$ $(k = 1, 2, \ldots)$.
- Note that $G/P_1(G) = (\mathbf{Z}/p)^{d(G)}$ and $d(G) = d(Cl_S(K))$.
- Given $G/P_{k-1}(G)$, O'Brien's algorithm yields all possible $G/P_k(G)$.
- We only save those $G/P_k(G)$ that are number theoretically feasible- namely that do not violate information we have about abelianizations of low index subgroups of G or about the generator and relation ranks of G.

Generating Lattice Data

- For simplicity of exposition, take the case $p = 2$ and $S = \emptyset$. For the general case the same ideas apply with class groups replaced by certain ray class groups. We want $G = \mathrm{Gal}(K^{\emptyset}/K)$.

Generating Lattice Data

- For simplicity of exposition, take the case $p = 2$ and $S = \emptyset$. For the general case the same ideas apply with class groups replaced by certain ray class groups. We want $G = \mathrm{Gal}(K^{\emptyset}/K)$.
- First calculate the 2-class group $Cl_{\emptyset}(K)$. This tells us G/G' and so $G/P_1(G)$ and $d(G)$.

Generating Lattice Data

- For simplicity of exposition, take the case $p = 2$ and $S = \emptyset$. For the general case the same ideas apply with class groups replaced by certain ray class groups. We want $G = \mathrm{Gal}(K^{\emptyset}/K)$.
- First calculate the 2-class group $Cl_{\emptyset}(K)$. This tells us G/G' and so $G/P_1(G)$ and $d(G)$.
- Explicit class field theory yields all unramified quadratic extensions of K. For each such L we compute $Cl_{\emptyset}(L)$.

Generating Lattice Data

- For simplicity of exposition, take the case $p = 2$ and $S = \emptyset$. For the general case the same ideas apply with class groups replaced by certain ray class groups. We want $G = \mathrm{Gal}(K^{\emptyset}/K)$.
- First calculate the 2-class group $Cl_{\emptyset}(K)$. This tells us G/G' and so $G/P_1(G)$ and $d(G)$.
- Explicit class field theory yields all unramified quadratic extensions of K. For each such L we compute $Cl_{\emptyset}(L)$.
- Stop there, or find all unramified quadratic extensions of all such L and their 2-class groups. Check for duplicates.

Generating Lattice Data

- For simplicity of exposition, take the case $p = 2$ and $S = \emptyset$. For the general case the same ideas apply with class groups replaced by certain ray class groups. We want $G = \mathrm{Gal}(K^{\emptyset}/K)$.
- First calculate the 2-class group $Cl_{\emptyset}(K)$. This tells us G/G' and so $G/P_1(G)$ and $d(G)$.
- Explicit class field theory yields all unramified quadratic extensions of K. For each such L we compute $Cl_{\emptyset}(L)$.
- Stop there, or find all unramified quadratic extensions of all such L and their 2-class groups. Check for duplicates.
- Now you have the abelianizations of all index ≤ 4 subgroups of G.

Pruning the Tree (Abelianizations)

- Given $G/P_{k-1}(G)$, find all its immediate descendants.

Pruning the Tree (Abelianizations)

- Given $G/P_{k-1}(G)$, find all its immediate descendants.
- For each such P, compute its subgroups of index ≤ 4 and their abelianizations.

Pruning the Tree (Abelianizations)

- Given $G/P_{k-1}(G)$, find all its immediate descendants.
- For each such P, compute its subgroups of index ≤ 4 and their abelianizations.
- Compare with the abelianizations of subgroups of index ≤ 4 of G. .

Pruning the Tree (Abelianizations)

- Given $G/P_{k-1}(G)$, find all its immediate descendants.
- For each such P, compute its subgroups of index ≤ 4 and their abelianizations.
- Compare with the abelianizations of subgroups of index ≤ 4 of G. .
- The abelianizations for P have to be no bigger than those for G.

Pruning the Tree (Abelianizations)

- Given $G/P_{k-1}(G)$, find all its immediate descendants.
- For each such P, compute its subgroups of index ≤ 4 and their abelianizations.
- Compare with the abelianizations of subgroups of index ≤ 4 of G. .
- The abelianizations for P have to be no bigger than those for G.
- For k large enough, the abelianizations for P must equal those for G.

Pruning the Tree (Abelianizations)

- Given $G/P_{k-1}(G)$, find all its immediate descendants.
- For each such P, compute its subgroups of index ≤ 4 and their abelianizations.
- Compare with the abelianizations of subgroups of index ≤ 4 of G. .
- The abelianizations for P have to be no bigger than those for G.
- For k large enough, the abelianizations for P must equal those for G.
- Delete any P that fail either of these two constraints.

Pruning the Tree (Cohomology)

- Lemma: If $G_k = G/P_k(G)$, then the difference between the p-multiplicator rank and nuclear rank of G is at most $r(G)$.

Pruning the Tree (Cohomology)

- Lemma: If $G_k = G/P_k(G)$, then the difference between the p-multiplicator rank and nuclear rank of G is at most $r(G)$.
- Moreover, we have earlier bounds for $r(G)$ - for instance if K is totally complex, $0 \leq r(G) - d(G) \leq [K : \mathbf{Q}]/2$. Knowing $d(G)$ this bounds $r(G)$.

Pruning the Tree (Cohomology)

- Lemma: If $G_k = G/P_k(G)$, then the difference between the p-multiplicator rank and nuclear rank of G is at most $r(G)$.
- Moreover, we have earlier bounds for $r(G)$ - for instance if K is totally complex, $0 \leq r(G) - d(G) \leq [K : \mathbf{Q}]/2$. Knowing $d(G)$ this bounds $r(G)$.
- For the immediate descendant under consideration, P, delete it if the difference between its p-multiplicator rank and nuclear rank is too large.

Pruning the Tree (Cohomology)

- Lemma: If $G_k = G/P_k(G)$, then the difference between the p-multiplicator rank and nuclear rank of G is at most $r(G)$.
- Moreover, we have earlier bounds for $r(G)$ - for instance if K is totally complex, $0 \leq r(G) - d(G) \leq [K : \mathbf{Q}]/2$. Knowing $d(G)$ this bounds $r(G)$.
- For the immediate descendant under consideration, P, delete it if the difference between its p-multiplicator rank and nuclear rank is too large.
- You can also keep track of inertial generators and complex conjugation (no help if $S = \emptyset$ and K is totally complex!).

Narrowing Candidates

- If this process terminates, then we know G is on the list of candidates (so G is finite).

Narrowing Candidates

- If this process terminates, then we know G is on the list of candidates (so G is finite).
- This (often long) list can be shortened by finding an index 4 subgroup whose index 8 subgroups differ among the different candidates.

Narrowing Candidates

- If this process terminates, then we know G is on the list of candidates (so G is finite).
- This (often long) list can be shortened by finding an index 4 subgroup whose index 8 subgroups differ among the different candidates.
- Find the field corresponding to this index 4 subgroup.

Narrowing Candidates

- If this process terminates, then we know G is on the list of candidates (so G is finite).
- This (often long) list can be shortened by finding an index 4 subgroup whose index 8 subgroups differ among the different candidates.
- Find the field corresponding to this index 4 subgroup.
- Find its unramified quadratic extensions and their 2-class groups.

Narrowing Candidates

- If this process terminates, then we know G is on the list of candidates (so G is finite).
- This (often long) list can be shortened by finding an index 4 subgroup whose index 8 subgroups differ among the different candidates.
- Find the field corresponding to this index 4 subgroup.
- Find its unramified quadratic extensions and their 2-class groups.
- See which of the candidates have matching abelianizations.

Example

- Let $K = \mathbf{Q}(\sqrt{-3135})$.

Example

- Let $K = \mathbf{Q}(\sqrt{-3135})$.
- $rd(K) = 56$ so if K has an infinite 2-class tower, then the liminf bound drops from 82 to 56.

Example

- Let $K = \mathbf{Q}(\sqrt{-3135})$.
- $rd(K) = 56$ so if K has an infinite 2-class tower, then the liminf bound drops from 82 to 56.
- Its 2-class group is $[2, 2, 2]$, one of the cases Benjamin-Lemmermeyer-Snyder left open.

Example

- Let $K = \mathbf{Q}(\sqrt{-3135})$.
- $rd(K) = 56$ so if K has an infinite 2-class tower, then the liminf bound drops from 82 to 56.
- Its 2-class group is $[2, 2, 2]$, one of the cases Benjamin-Lemmermeyer-Snyder left open.
- Lattice data - K has 7 unramified quadratic extensions; the 2-class groups are $[2, 2, 2]$ (three times), $[2, 8]$ (twice), $[2, 2, 2, 2]$ (once), $[2, 16]$ (once).

Example

- Let $K = \mathbf{Q}(\sqrt{-3135})$.
- $rd(K) = 56$ so if K has an infinite 2-class tower, then the liminf bound drops from 82 to 56.
- Its 2-class group is $[2, 2, 2]$, one of the cases Benjamin-Lemmermeyer-Snyder left open.
- Lattice data - K has 7 unramified quadratic extensions; the 2-class groups are $[2, 2, 2]$ (three times), $[2, 8]$ (twice), $[2, 2, 2, 2]$ (once), $[2, 16]$ (once).
- At the next level we get 31 fields, degree 4 over K, and their 2-class groups.

Example (Continued)

- $G/P_1(G) \cong (\mathbf{Z}/2)^3$, which by O'Brien has 67 immediate descendants.

Example (Continued)

- $G/P_1(G) \cong (\mathbf{Z}/2)^3$, which by O'Brien has 67 immediate descendants.
- Of these, 4 fail the cohomological condition.

Example (Continued)

- $G/P_1(G) \cong (\mathbf{Z}/2)^3$, which by O'Brien has 67 immediate descendants.
- Of these, 4 fail the cohomological condition.
- A further 44 have too large an abelianization.

Example (Continued)

- $G/P_1(G) \cong (\mathbf{Z}/2)^3$, which by O'Brien has 67 immediate descendants.
- Of these, 4 fail the cohomological condition.
- A further 44 have too large an abelianization.
- Another 18 have an index 2 subgroup with too large abelianization.

Example (Continued)

- $G/P_1(G) \cong (\mathbf{Z}/2)^3$, which by O'Brien has 67 immediate descendants.
- Of these, 4 fail the cohomological condition.
- A further 44 have too large an abelianization.
- Another 18 have an index 2 subgroup with too large abelianization.
- Leaves 1 immediate descendant, which must be $G/P_2(G)$!

Example (Continued)

- This group has 186 immediate descendants.

Example (Continued)

- This group has 186 immediate descendants.
- All but 16 (all order 256) fail cohomological or abelianization criterion.

Example (Continued)

- This group has 186 immediate descendants.
- All but 16 (all order 256) fail cohomological or abelianization criterion.
- The search grows, but ultimately we're left with 240 candidates for G.

Example (Continued)

- This group has 186 immediate descendants.
- All but 16 (all order 256) fail cohomological or abelianization criterion.
- The search grows, but ultimately we're left with 240 candidates for G.
- We apply the cohomological criterion to low index subgroups of each candidate, leaving 84 survivors.

Example (Continued)

- This group has 186 immediate descendants.
- All but 16 (all order 256) fail cohomological or abelianization criterion.
- The search grows, but ultimately we're left with 240 candidates for G.
- We apply the cohomological criterion to low index subgroups of each candidate, leaving 84 survivors.
- Computing extensions of particular degree 4 extensions of K eventually cut us down to 4 candidates, all order 8192 and of derived length 3.

Upshot in Finite Case

- The search for fields of low discriminant but infinite 2-class tower has a long history.

Upshot in Finite Case

- The search for fields of low discriminant but infinite 2-class tower has a long history.
- Several years ago, Stark asked if $\mathbf{Q}(\sqrt{-2379})$ (2-class group $[4, 4]$) has infinite 2-class tower, i.e. infinite G. Bush showed it finite and obtained the first examples with derived length 3.

Upshot in Finite Case

- The search for fields of low discriminant but infinite 2-class tower has a long history.
- Several years ago, Stark asked if $\mathbf{Q}(\sqrt{-2379})$ (2-class group $[4,4]$) has infinite 2-class tower, i.e. infinite G. Bush showed it finite and obtained the first examples with derived length 3.
- Next promising case, $\mathbf{Q}(\sqrt{-3135})$, shown to have finite G by Nover.

Upshot in Finite Case

- The search for fields of low discriminant but infinite 2-class tower has a long history.
- Several years ago, Stark asked if $\mathbf{Q}(\sqrt{-2379})$ (2-class group $[4,4]$) has infinite 2-class tower, i.e. infinite G. Bush showed it finite and obtained the first examples with derived length 3.
- Next promising case, $\mathbf{Q}(\sqrt{-3135})$, shown to have finite G by Nover.
- Next one, $\mathbf{Q}(\sqrt{-5460})$, leads to combinatorial explosion but is suspected to have finite G.

Upshot in Finite Case

- The search for fields of low discriminant but infinite 2-class tower has a long history.
- Several years ago, Stark asked if $\mathbf{Q}(\sqrt{-2379})$ (2-class group $[4,4]$) has infinite 2-class tower, i.e. infinite G. Bush showed it finite and obtained the first examples with derived length 3.
- Next promising case, $\mathbf{Q}(\sqrt{-3135})$, shown to have finite G by Nover.
- Next one, $\mathbf{Q}(\sqrt{-5460})$, leads to combinatorial explosion but is suspected to have finite G.
- Perhaps there are better lower bounds for Liminf ?!

Infinite G

- We know very little about infinite G.

Infinite G

- We know very little about infinite G.
- How do we proceed in this case?

Infinite G

- We know very little about infinite G.
- How do we proceed in this case?
- Idea: Write down everything we know about G and find all such pro-p groups!

An Experiment

- Let $K = \mathbf{Q}$, $p = 2$, and $S = \{q, r\}$, where $q, r \equiv 5 \pmod 8$.

An Experiment

- Let $K = \mathbf{Q}$, $p = 2$, and $S = \{q, r\}$, where $q, r \equiv 5 \pmod 8$.
- G has pro-2 presentation of the form $< x, y \mid x^a = x^q, y^b = y^r >$ (unknown a, b).

An Experiment

- Let $K = \mathbf{Q}$, $p = 2$, and $S = \{q, r\}$, where $q, r \equiv 5 \pmod 8$.
- G has pro-2 presentation of the form $< x, y \mid x^a = x^q, y^b = y^r >$ (unknown a, b).
- Then $G =< x, y \mid x^c = x^5, y^d = y^5 >$ (unknown c, d).

An Experiment

- Let $K = \mathbf{Q}$, $p = 2$, and $S = \{q, r\}$, where $q, r \equiv 5 \pmod 8$.
- G has pro-2 presentation of the form $< x, y \mid x^a = x^q, y^b = y^r >$ (unknown a, b).
- Then $G =< x, y \mid x^c = x^5, y^d = y^5 >$ (unknown c, d).
- If $q, r \equiv 5 \pmod 8$ and q is a 4th power mod r but not vice versa, then G is infinite.

An Experiment

- Let $K = \mathbf{Q}$, $p = 2$, and $S = \{q, r\}$, where $q, r \equiv 5 \pmod 8$.
- G has pro-2 presentation of the form $< x, y \mid x^a = x^q, y^b = y^r >$ (unknown a, b).
- Then $G =< x, y \mid x^c = x^5, y^d = y^5 >$ (unknown c, d).
- If $q, r \equiv 5 \pmod 8$ and q is a 4th power mod r but not vice versa, then G is infinite.
- Idea: pick random words c, d and look at $< x, y \mid x^c = x^5, y^d = y^5 >$.

An Experiment

- Let $K = \mathbf{Q}$, $p = 2$, and $S = \{q, r\}$, where $q, r \equiv 5 \pmod 8$.
- G has pro-2 presentation of the form $< x, y \mid x^a = x^q, y^b = y^r >$ (unknown a, b).
- Then $G =< x, y \mid x^c = x^5, y^d = y^5 >$ (unknown c, d).
- If $q, r \equiv 5 \pmod 8$ and q is a 4th power mod r but not vice versa, then G is infinite.
- Idea: pick random words c, d and look at $< x, y \mid x^c = x^5, y^d = y^5 >$.
- If the abelianizations of its low index subgroups are all finite and the sizes of its p-quotients do not stabilize (within range of computer), then save c, d.

An Experiment (Continued)

- We thus obtain some plausible c, d and so plausible G.

An Experiment (Continued)

- We thus obtain some plausible c, d and so plausible G.
- Amazing observation - the G that survive belong to one special family.

An Experiment (Continued)

- We thus obtain some plausible c, d and so plausible G.
- Amazing observation - the G that survive belong to one special family.
- Conjecture: (1) G has presentation of the form $< x, y \mid x^a = x^5, y^4 = 1 >$ (2) Moreover, the orders of $G/P_k(G)$ $(k = 1, 2, ...)$ are $2^2, 2^5, 2^8, 2^{11}, 2^{14}, 2^{16}, 2^{20}, 2^{24}, 2^{30}, 2^{36}, 2^{44}, 2^{52}, 2^{64}, 2^{76}, 2^{93}, ..$

Strategy in Infinite Case

- A Golod-Shafarevich (G-S) group is one satisfying $r(G) \leq d(G)^2/4$.

Strategy in Infinite Case

- A Golod-Shafarevich (G-S) group is one satisfying $r(G) \leq d(G)^2/4$.
- To show that G is infinite, it's enough to find a G-S subgroup of finite index.

Strategy in Infinite Case

- A Golod-Shafarevich (G-S) group is one satisfying $r(G) \leq d(G)^2/4$.
- To show that G is infinite, it's enough to find a G-S subgroup of finite index.
- The Virtual Golod-Shafarevich (VGS) Conjecture says that infinite G always have a G-S subgroup of finite index.

Strategy in Infinite Case

- A Golod-Shafarevich (G-S) group is one satisfying $r(G) \leq d(G)^2/4$.
- To show that G is infinite, it's enough to find a G-S subgroup of finite index.
- The Virtual Golod-Shafarevich (VGS) Conjecture says that infinite G always have a G-S subgroup of finite index.
- Strategy to prove G infinite - find family of groups that G belongs to; find their G-S subgroup; locate the corresponding field; apply Golod-Shafarevich to it.

Tame Fontaine-Mazur Conjecture

- Recall this says that no G has an infinite quotient that's a subgroup of some $GL_n(\mathbf{Z}_p)$.

Tame Fontaine-Mazur Conjecture

- Recall this says that no G has an infinite quotient that's a subgroup of some $GL_n(\mathbf{Z}_p)$.
- The VGS conjecture implies more generally that every infinite G has a large action on a locally finite, rooted tree.

Arboreal Galois Representations

- If T is a locally finite, rooted tree, then a continuous homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T)$ is called an arboreal Galois representation.

Arboreal Galois Representations

- If T is a locally finite, rooted tree, then a continuous homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T)$ is called an arboreal Galois representation.
- One source of these comes from the extension of the tame Fontaine-Mazur conjecture.

Arboreal Galois Representations

- If T is a locally finite, rooted tree, then a continuous homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T)$ is called an arboreal Galois representation.
- One source of these comes from the extension of the tame Fontaine-Mazur conjecture.
- Another source comes from Galois action on roots of iterates of a polynomial.

Arboreal Galois Representations

- If T is a locally finite, rooted tree, then a continuous homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T)$ is called an arboreal Galois representation.
- One source of these comes from the extension of the tame Fontaine-Mazur conjecture.
- Another source comes from Galois action on roots of iterates of a polynomial.
- In analogy to p-adic Galois representations, we look to characterize their images and the images of their Frobenius elements.

Example (with Rafe Jones)

- Let $f = (x+1)^2 - 2 \in \mathbf{Q}[x]$.

Example (with Rafe Jones)

- Let $f = (x+1)^2 - 2 \in \mathbf{Q}[x]$.
- The nth iterate of f has discriminant a 2-power, so the Galois action on its roots is ramified only at 2 and ∞. (These roots form the nth level of a tree T.)

Example (with Rafe Jones)

- Let $f = (x+1)^2 - 2 \in \mathbf{Q}[x]$.
- The nth iterate of f has discriminant a 2-power, so the Galois action on its roots is ramified only at 2 and ∞. (These roots form the nth level of a tree T.)
- Big Question: Is the union of the splitting fields of all these iterates the maximal 2-extension of $\mathbf{Q}$ unramified outside 2 and ∞?

Example (with Rafe Jones)

- Let $f = (x+1)^2 - 2 \in \mathbf{Q}[x]$.
- The nth iterate of f has discriminant a 2-power, so the Galois action on its roots is ramified only at 2 and ∞. (These roots form the nth level of a tree T.)
- Big Question: Is the union of the splitting fields of all these iterates the maximal 2-extension of $\mathbf{Q}$ unramified outside 2 and ∞?
- Thanks to Klüners and Fieker, we find the Galois groups of the nth iterates $(n = 1, 2, ..., 7)$, which have orders $2^1, 2^3, 2^6, 2^{11}, 2^{22}, 2^{43}, 2^{86}$.

Conjecture

- The Basilica group $B = < a, b >$ is a known subgroup of Aut(T) with similar growth.

Conjecture

- The Basilica group $B = < a, b >$ is a known subgroup of $\mathrm{Aut}(T)$ with similar growth.
- Conjecture: The Galois group of the nth iterate over $\mathbf{Q}(i)$ is the subgroup $< [a, b], aba >$ acting on the 2^n vertices of T at level n.

Conjecture

- The Basilica group $B =< a, b >$ is a known subgroup of Aut(T) with similar growth.
- Conjecture: The Galois group of the nth iterate over $\mathbf{Q}(i)$ is the subgroup $< [a, b], aba >$ acting on the 2^n vertices of T at level n.
- The closure of $< [a, b], aba >$ is not free.

Conjecture

- The Basilica group $B =< a, b >$ is a known subgroup of Aut(T) with similar growth.
- Conjecture: The Galois group of the nth iterate over $\mathbf{Q}(i)$ is the subgroup $< [a, b], aba >$ acting on the 2^n vertices of T at level n.
- The closure of $< [a, b], aba >$ is not free.
- The Galois group over $\mathbf{Q}(i)$ of the maximal 2-extension unramified outside 2 and ∞ is free (Markscheitis, 1963).

Conjecture

- The Basilica group $B =< a, b >$ is a known subgroup of $\mathrm{Aut}(T)$ with similar growth.
- Conjecture: The Galois group of the nth iterate over $\mathbf{Q}(i)$ is the subgroup $< [a, b], aba >$ acting on the 2^n vertices of T at level n.
- The closure of $< [a, b], aba >$ is not free.
- The Galois group over $\mathbf{Q}(i)$ of the maximal 2-extension unramified outside 2 and ∞ is free (Markscheitis, 1963).
- Consequence: Answer to the big question is no. (In fact, we just need that $\overline{B}$ contains no nonabelian free pro-2 subgroup.)