The phrase "Profinite Arithmetic Geometry"
Red Lodge, Wednesday April 5

Part I. 1st Fratt. Principle and the group $M_{\boldsymbol{g}}$
Part II. Inflation to $M_{\boldsymbol{g}} = M_{\boldsymbol{g},p}$ and Lift Invariants
Part III. p-Poincaré duality gives sufficiency for $C_{G_{k+1}}(\boldsymbol{g}_k) \neq \emptyset$
Part IV. Basic Braid Orbit questions
Part V. g-p' Cusps and 2nd Fratt. Princ.
App.A$_2$. Full limit group questions
App.B$_1$. Higher Order g-p' Cusps

Set up for the phrase

Start with a space $\mathcal{H}$ (or a moduli problem): points $\boldsymbol{p} \Leftrightarrow$ objects $W_{\boldsymbol{p}}$ with an attached group G (not dependent on $\boldsymbol{p}$). Assume G has a functorial profinite cover G^* (determined by $\mathcal{H}$).

"Profinite arithmetic geometry:" Any quotient H of G^* mapping through G gives a collection $C_H(W_{\boldsymbol{p}})$ of objects mapping to W. Expect this for the projective system of those $C_H(W_{\boldsymbol{p}})$, running over H:

Group cohomology of G^* interprets significant properties of the projective system $\{C_H(W_{\boldsymbol{p}})\}_H$.

Modular Towers: Unramified extensions of a cover

$\mathbb{P}^1_z = \mathbb{C}_z \dot{\cup} \{\infty\}$ is the project z-line; and $W_{\boldsymbol{p}}$ is a compact Riemann surface (geometrically Galois) cover $\varphi : X \to \mathbb{P}^1_z$ with group G (of order divisible by p). It has a Nielsen class $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$.

Extensions: Unramified extensions $\psi : Y \to X$ of φ, with $\varphi \circ \psi$ Galois (group H) as φ varies.

If $H \to G$ splits, then $\varphi \circ \psi$ has the form $W \times_{\mathbb{P}^1_z} X$ ($W \to \mathbb{P}^1_z$ maybe not Galois). Unless $H \to G$ *Frattini*, there is a proper factorization of $\varphi : Y \to Y' \to X$, presenting Y as $W \times_{\mathbb{P}^1_z} Y'$.

Part I. 1st Fratt. Principle and the group M_g

Restrict to most mysterious part: Covers without such a factorization. Denote these $\mathcal{C}_\varphi$.

Assume G is p-perfect. We'll show structure on $\mathcal{C}_\varphi$, based on cohomology of two groups:

- universal p-Frattini cover ${}_p\tilde{G}$ of G; and a
- dim 2 p-Poincaré Dual group $M_{\varphi,p}$.

Both groups are virtually pro-p. Most significant is how much $M_{\varphi,p}$ depends on φ.

Use Nielsen classes

$$\mathrm{Ni}(G,\mathbf{C})^{\mathrm{in}} \stackrel{\mathrm{def}}{=} \{(g_1,\dots,g_r) \mid g_1\cdots g_r \stackrel{\mathrm{def}}{=} \Pi(\boldsymbol{g}) = 1, \boldsymbol{g}\in\mathbf{C}, \langle\boldsymbol{g}\rangle = G\}.$$

Given the Nielsen class association with a cover, $\varphi \leftrightarrow \boldsymbol{g} \in \mathrm{Ni}(G,\mathbf{C})^{\mathrm{in}}$, characterize $C_H(\varphi)$ as

$$\{\boldsymbol{g}_H \in \mathrm{Ni}(H,\mathbf{C})^{\mathrm{in}} \text{ with } \boldsymbol{g}_H \mod G = \boldsymbol{g}\}.$$

FP1 — Why p' conjugacy classes **C**?:
With $g\in G$ and $p^u||\mathrm{ord}(g)$, $u\ge 1$,
then $g'\in G_1$ over $g \implies p^{u+1}||\mathrm{ord}(g)$.

Defining $M_{\boldsymbol{g}}$ and related groups

Define $D_{\bar{\boldsymbol{\sigma}}}$: Presented as $\langle \bar\sigma_1, \ldots, \bar\sigma_r \rangle$ modulo the normal subgroup generated by

$$\bar{\boldsymbol{\sigma}} \stackrel{\text{def}}{=} \{\bar\sigma_i^{\mathrm{ord}(g_i)}, i = 1, \ldots, r, \text{ and } \bar\sigma_1 \cdots \bar\sigma_r\}.$$

Define $M_{\boldsymbol{g}}$: Complete $D_{\bar{\boldsymbol{\sigma}}}$ using p-power index subgroups of $\ker(D_{\bar{\boldsymbol{\sigma}}} \to G)$, normal in $D_{\bar{\boldsymbol{\sigma}}}$. Tacit: $M_{\boldsymbol{g}}$ has distinguished generators $\bar\sigma_1, \ldots, \bar\sigma_r$.

Define $\tilde{K}_{\bar{\boldsymbol{\sigma}}^*}$:

Remove relation $\bar{\sigma}_1 \cdots \bar{\sigma}_r = 1$ from $D_{\bar{\boldsymbol{\sigma}}}$. Denote generators by $\bar{\sigma}_1^*, \ldots, \bar{\sigma}_r^*$:
$\{\langle \bar{\sigma}_i^* \rangle / (\bar{\sigma}_i^*)^{\mathrm{ord}(g_i)}\}_{i=1}^r$ freely generate $K_{\bar{\boldsymbol{\sigma}}}$.

Complete $K_{\bar{\boldsymbol{\sigma}}^*}$ using p-power index subgroups of $\ker(K_{\bar{\boldsymbol{\sigma}}^*} \to G)$, normal in $K_{\boldsymbol{\sigma}}$. Form a natural surjection $\psi_{\bar{\boldsymbol{\sigma}}^*} : \tilde{K}_{\bar{\boldsymbol{\sigma}}^*} \to M_{\boldsymbol{g}}$.

Geometric construction of $M_{\boldsymbol{g}}$ and $K_{\bar{\boldsymbol{\sigma}}^*}$

Suppose $\boldsymbol{g}_k \in \mathrm{Ni}(G_k, \mathbf{C})$ lies over $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$.

Lemma 1. *Mapping $M_{\boldsymbol{g}}$ generators $\bar\sigma_1, \dots, \bar\sigma_r$ to entries of ${}_k\boldsymbol{g}$ gives a homomorphism $\mu_k : M_{\boldsymbol{g}} \to G_k$.*

If $h_1^*, \dots, h_r^* \in \mathbf{C} \cap G_{k+1}^r$ lie (resp.) over entries of ${}_k\boldsymbol{g}$, then $\mu_{k+1} : \tilde{K}_{\bar{\boldsymbol{\sigma}}^*} \to G_{k+1}$ by $\bar\sigma_i^* \mapsto h_i^*$, $i = 1, \dots, r$, extends μ_k.

Part II. Inflation to $M_{\boldsymbol{g}} = M_{\boldsymbol{g},p}$ and Lift Invariants

Main goal: Cohomological characterizations

1. When is each of the $C_{G_k}(\boldsymbol{g})$ nonempty.
2. When for each $\boldsymbol{g}_k \in C_{G_k}(\boldsymbol{g})$ and $k' > k$, the collection $C_{G_{k'}}(\boldsymbol{g}_k)$ is nonempty.

One-one correspondence: $M_{\boldsymbol{g}} \to G$ factoring through $H \to G \Leftrightarrow \boldsymbol{g}_H \in C_H(\boldsymbol{g})$. Denote the corresponding map $M_{\boldsymbol{g}} \to H$ by $\psi_{\boldsymbol{g}_H}$.

Fundamental limit group questions

Let $\{\boldsymbol{g}_k \in C_{G_k}(\boldsymbol{g})\}_{k=0}^{\infty}\} = \tilde{\boldsymbol{g}}$ be a projective sequence. Defines a *cusp* branch.

These define a *component* branch: $\{\mathrm{Ni}'_k\}_{k=0}^{\infty}$, Ni'_k the *braid orbit* of $\boldsymbol{g}_k$ (p. 12).

Definition 2. Then, $\tilde{\boldsymbol{g}}$ defines a homomorphism $\psi_{\tilde{\boldsymbol{g}}} : M_{\boldsymbol{g}} \to {}_p\tilde{G}$. This $\psi_{\tilde{\boldsymbol{g}}}$ (up to *braid equivalence*) gives ${}_p\tilde{G}$ as a *limit group* of $\psi_{\boldsymbol{g}}$.

Expression (1) (resp. (2)) means ${}_p\tilde{G}$ is *a* (resp. the *only*) isomorphism class of limit groups for the standard component tree.

Cohomology start:

With $M_k = \ker(G_{k+1} \to G_k)$,
$\dim_{\mathbb{Z}/p}(H^2(G_k, M_k)) = 1$ [Fr95, Lem. 2.3].

Lemma 3. [Fr05c, Lem. 4.15], [We05, Prop. 3.2] *For* $\boldsymbol{g}_k \in C_{G_k}(\boldsymbol{g})$*, the obstruction to finding* $\boldsymbol{g}_{k+1} \in C_{G_{k+1}}(\boldsymbol{g}_k)$ *is inflation* $\inf_{G_{k+1},G_k}(\psi_{\boldsymbol{g}_k})$ *to* $H^2(M_{\boldsymbol{g}}, M_k)$ *of a generator of* $H^2(G_k, M_k)$*.*

Denote maximal quotient of M_k on which G_k acts trivially by $\mathrm{Sc}_{p,k} = \mathrm{Sc}_k$: *exponent p quotient of Schur multiplier of G_k.*

The lifting invariant s_k

Kernel of natural cover $R_k \to G_k$ identifies with Sc_k.

Lemma 4. *Over* $\boldsymbol{g}' = (g_1', \dots, g_r') \in \mathrm{Ni}(G_k, \mathbf{C})$ *is a unique* $\boldsymbol{g}'' \in (R_k)^r \cap \mathbf{C}$. *This defines*

$$s_k(\boldsymbol{g}') \in \ker(R_k \to G_k) \text{ as } \Pi(\boldsymbol{g}'') \stackrel{\text{def}}{=} g_1'' \cdots g_r''.$$

$C_{G_{k+1}}(\boldsymbol{g}')$ *nonempty* $\Longrightarrow$ $s_k(\boldsymbol{g}') = 0$ *(add. not.).*

[Ser90a] defines s_k when $G_k = A_n$ and $R_k \to G_k$ is the Spin cover of A_n. I give examples later of computing this and higher cases.

Part III. p-Poincaré duality gives sufficiency for $C_{G_{k+1}}(\boldsymbol{g}_k) \neq \emptyset$

Proposition 5. *Lem. 4 condition is sufficient:*

$$\tilde{\alpha} \stackrel{\text{def}}{=} \inf_{G_{k+1}, G_k} (\psi_{\boldsymbol{g}_k}) \neq 0 \implies s_k(\boldsymbol{g}_k) \neq 0.$$

Use μ_{k+1} of Lem. 1 for an explicit obstruction to lifting $M_{\boldsymbol{g}} \to G$. For $\bar{g} \in M_{\boldsymbol{g}}$ choose $h_{\bar{g}} \in G_k$ as the image in G_k of a lift to $\tilde{K}_{\bar{\boldsymbol{\sigma}}^*} \cap \mathbf{C}$ over $\bar{g}$.

Compute the 2-cocycle

$$\tilde{\alpha}(\bar{g}_1, \bar{g}_2) = h_{\bar{g}_1} h_{\bar{g}_2} (h_{\overline{g_1 g_2}})^{-1}, \bar{g}_1, \bar{g}_2 \in M_{\boldsymbol{g}}$$

describing the obstruction.

As $\psi_{\bar{\boldsymbol{\sigma}}^*}$ is a homomorphism, the discrepancy between $\alpha(\bar{g}_1, \bar{g}_2)$ and 1 is the leeway in reps. for $h_{\overline{g_1 g_2}}$ lying over $\overline{g_1 g_2}$.

When the cocycle $\tilde{\alpha}(\bar{g}_1, \bar{g}_2)$ vanishes

Each $\tilde{\alpha}(\bar{g}_1, \bar{g}_2)$ is a word in $\ker(K_{\bar{\boldsymbol{\sigma}}^*} \longrightarrow M_{\boldsymbol{g}})$, products of conjugates of $h_1^* \cdots h_r^*$. It vanishes if you can choose $(h_1^*, \ldots, h_r^*)$ (as in Lem. 1) so $h_1^* \cdots h_r^* = 1$. Recall: Dual of M_k^* as an $M_{\boldsymbol{g}}$ module is $\mathrm{Hom}(M_k, \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}(M_k, \mathbb{Z}/p)$, ($\mathbb{Q}_p/\mathbb{Z}_p$ is the duality module for $M_{\boldsymbol{g}}$).

Apply p-Poincaré duality:

(D^{2,0}) $H^2(M_{\boldsymbol{g}}, M_k) \times H^0(M_{\boldsymbol{g}}, M_k^*) \longrightarrow H^2(M_{\boldsymbol{g}}, \mathbb{Z}/p)$ is a perfect pairing (apply $\beta \in H^0(M_{\boldsymbol{g}}, M_k^*)$ to values of a 2-cycle in $H^2(M_{\boldsymbol{g}}, M_k)$).

Identify $H^0(M_{\boldsymbol{g}}, M_k^*)$ with

$$H_0(M_{\boldsymbol{g}}, D \otimes M_k) \simeq D \otimes_{\mathbb{Z}/p[M_{\boldsymbol{g}}]} M_k,$$

with $D = \mathbb{Z}/p$ (as $\mathbb{Z}/p[M_{\boldsymbol{g}}]$ module).

$\mathrm{Sc}_{p,k}$ appears (p. 7):

So, the tensor product $D \otimes_{\mathbb{Z}/p[M_{\boldsymbol{g}}]} M_k$ is the maximal quotient of M_k on which $M_{\boldsymbol{g}}$ (and so G_k) acts trivially. So, Identify $D \otimes_{\mathbb{Z}/p[M_{\boldsymbol{g}}]} M_k$ with $\mathrm{Sc}_{p,k}$.

Now pair $\tilde{\alpha}(\bullet, \bullet) \in H^2(M_{\boldsymbol{g}}, M_k)$ against $\beta \in H^0(M_{\boldsymbol{g}}, M_k^*)$. Further, regard $\beta \overset{\text{def}}{=} \beta_R$ as the linear functional on M_k from the kernel of the induced map $G_{k+1} \to R$, with $R \to G_k$ a central extension with $\mathbb{Z}/p = \ker(R \to G_k)$.

Conclusion of the result

Let $\boldsymbol{g}$ be the image of $(h_1^*, \ldots, h_r^*)$ in $\mathrm{Ni}(G_k, \mathbf{C})$. So, $\beta_R(\tilde{\alpha}) = s_R(\boldsymbol{g})$, the lifting invariant value.

The pairing is perfect. Conclude: Obstruction to extend $M_{\boldsymbol{g}} \to G_k$ to $M_{\boldsymbol{g}} \to G_{k+1}$ is trivial if and only if $s_R(\boldsymbol{g})$ is trivial over all such $R \to G_k$.

Part IV. Basic Braid Orbit questions

Hurwitz monodromy group $H_r = \langle q_1, \dots, q_{r-1} \rangle$ acts on $\{M_{\boldsymbol{g}}\}_{\boldsymbol{g} \in \mathrm{Ni}(G,\mathbf{C})}$ and on

$$\{M_{\tilde{\boldsymbol{g}}}\}_{\{\tilde{\boldsymbol{g}} \in \{\lim\limits_{\longleftarrow k} C_{G_k}(\boldsymbol{g})\}}.$$

Here's q_i on distinguished generators: $(\bar{\sigma}_1, \dots, \bar{\sigma}_r)$

$$\mapsto (\bar{\sigma}_1, \dots, \bar{\sigma}_{i-1}, \bar{\sigma}_i \bar{\sigma}_{i+1} \bar{\sigma}_i^{-1}, \bar{\sigma}_i, \bar{\sigma}_{i+2}, \dots, \bar{\sigma}_r).$$

Projective sequence of spaces:

Any $M_{\tilde{\boldsymbol{g}}}$ gives a braid orbit $\{(\tilde{\boldsymbol{g}})q\}_{q\in H_r} \stackrel{\text{def}}{=} \tilde{O}$: For $\tilde{\boldsymbol{g}} \in \tilde{O}$, all the $M_{\tilde{\boldsymbol{g}}}$ are isomorphic.

$\tilde{O}$ defines a projective sequence of reduced Hurwitz space components $\tilde{\mathcal{H}}_{\tilde{O}} \stackrel{\text{def}}{=} \{\mathcal{H}_{\tilde{O},k}\}_{k=0}^{\infty}$.

Abelianization: Replacing ${}_p\tilde{G}$ by its abelianization ${}_p\tilde{G}/(\ker_0, \ker_0)$ produces corresponding spaces. Let $R \to G_0$ be the *maximal central p extension of* G_0. Analog for abelianization in Prop. 5 for projective sequence of components requires just one test, $s_R(\boldsymbol{g}_0) = 0$, but $\ker(R \to G_0)$ may not have exponent p. Resulting spaces like *Shimura varieties*.

The Main Conjecture and ℓ-adic points

1. For a braid orbit O in a Nielsen class $\mathrm{Ni}(G, \mathbf{C})$, how to assure there is such a $\tilde{O}$ extending O?

2. Given $\tilde{O}$ from (1), when can you guarantee some number field is a definition field for all levels of $\tilde{\mathcal{H}}_{\tilde{O}}$: $\tilde{O}$ defines a PSC_K?

3. Given (2), could all levels have K points?

Results to questions have come entirely through properties of projective systems of *cusps*!!

This approach —non-obviously —generalizes aspects of modular curves.

Proposition 6. *Assume* $\tilde{O}$ *satisfies (3). With* K' *a completion of* K *at a prime not dividing* $|G|$*, there is a projective system of* K' *cusps.*

An outline, based on generalizing [DEm04], says the conclusion of Prop. 6 implies a special projective system $\{\boldsymbol{g}_k \in \mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}\}_{k=0}^{\infty}$: *g-$p'$ cusp branch*.

Part V. g-p' Cusps and 2nd Fratt. Princ.

Definition 7 (g-p' cusps). Let p, prime, divide $|G|$, p' classes **C**, $\boldsymbol{g}$ $=\in$ $\mathrm{Ni}(G,\mathbf{C})$. Then, $\boldsymbol{g}$ defines a (first order) *g-p' cusp* if it partitions as $(g_1,\dots,g_{i_1},g_{i_1+1},\dots,g_{i_2},\dots,g_{i_t})$ so:

[p' part.] $\langle g_{i_j+1},\dots,g_{i_{j+1}}\rangle = G_j$ is a p' group; and

[p' gen.] $\langle \Pi(g_{i_j+1},\dots,g_{i_{j+1}}), j=1,\dots,t\rangle$ is also a p' group.

App. B_1 has higher order (inductive) g-p' cusps.

2nd Fratt. Princ: For $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$ a g-p' cusp, there is a $\tilde{O}$ extending its braid orbit $O_{\boldsymbol{g}}$ (as in (1)).

A_n examples of two braid orbits from lifting inv.

Example 8 (A_n and 3-cycles). For each pair (n, r) with $r \geq n$, there are exactly two braid orbits on $\mathrm{Ni}(A_n, \mathbf{C}_{3^r})$. One contains a g-$2'$ representative and the other is obstructed at level 0. Braid orbit reps for $n = r = 4$ (see App. B_2 in Talk 2):

$$\begin{aligned} \boldsymbol{g}_{4,+} &= ((1\,3\,4), (1\,4\,3), (1\,2\,3), (1\,3\,2)), \\ \boldsymbol{g}_{4,-} &= ((1\,2\,3), (1\,3\,4), (1\,2\,4), (1\,2\,4)). \end{aligned}$$

Nonbraidable, isomorphic $M_{\tilde{\boldsymbol{g}}}$

Suppose two extensions $M_{\boldsymbol{g}_i} \to G$, arise from $\boldsymbol{g}_i \in \mathrm{Ni}(G, \mathbf{C})$, $i = 1, 2$. Assume they are isomorphic. Still might not be braidable.

The Nielsen class $\mathrm{Ni}(G_1(A_4), \mathbf{C}_{\pm 3^2})$ has six braid orbits. Two extensions correspond to the two H-M components called $\mathcal{H}_1^{+,\beta}$, $\mathcal{H}_1^{+,\beta^{-1}}$. An *outer* automorphism of $G_1(A_4)$ takes $\boldsymbol{g}_1$ to $\boldsymbol{g}_2$, giving elements in different braid orbits. These are H-M components, so *FP2* gives isomorphic extensions $M_{\boldsymbol{g}_i} \to {}_p\tilde{G}$, $i = 1, 2$ in distinct braid orbits.

App. A_1: Full limit group questions

Consider all quotients H of ${}_p\tilde{G}$ (rather than just G_k s). You get a much bigger world of limit groups: limit group over $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$ is a maximal projective sequence of such H s with $\mathcal{C}_H(\boldsymbol{g})$ not the emptyset.

Proposition 9. *Akin to Prop. 5, if G^* is a full limit group, it has this property:*

$\mathbb{Z}/p$ extension: There is only one possible Frattini extension $R^* \to G^*$ of $G^* \to G$ with kernel a $\mathbb{Z}/p$ module. Then, $\ker(R^* \to G^*) = \mathbb{Z}/p$, and s_{G^*} gives the obstruction.

Revisiting nonelementary modular curves: For each odd p, $\mathrm{Ni}((\mathbb{Z}/p)^2 \times^s \{\pm 1\}, \mathbf{C}_{2^4})$ has exactly one limit group, $(\mathbb{Z}_p)^2 \times^s \{\pm 1\}$. This is an alternate description of all modular curves. A universal Heisenberg group gives the obstruction running over all odd p [Fr05c, App. A.2].

App. B_1: Higher Order g-p' Cusps

Def.: (possibly *higher order*) g-p' cusps. (Darren Semmen): Some rooted planar tree, has elements of G labeling its vertices, and these hold.

1. The root has label 1.
2. The leaves of the tree have labels $g_1, \ldots, g_r$ in clockwise order.
3. Labels of vertices one level up and adjacent to vertex x generate a p'-group with their product (in clockwise order) the label of x.

Harder to detect, but includes more possibilities than 1st order g-p' reps. FP2 says such a $\boldsymbol{g}$ has a braid orbit whose p-Nielsen limit is ${}_p\tilde{G}$.

Bibliography

[BF02] Paul Bailey, and Michael D. Fried, *Hurwitz monodromy, spin separation and higher levels of a modular tower*, Arith. fund. groups and noncomm. alg. (Berk., CA, 1999), Proc. Sympos. Pure Math., vol. 70, AMS Prov. RI, 2002, pp. 79–220. MR1935406 (2005b:14044)

[Ca05a] A. Cadoret, *Harbater-Mumford subvarieties of moduli spaces of covers*, to appear in Math. Ann.

[De04] P. Dèbes, *Modular Towers: Construction and Diophantine Questions*, this volume.

[DDe04] P. Dèbes and B. Deschamps, *Corps ψ-libres et théorie inverse de Galois infinie*, J. für die reine und angew. Math. **574** (2004), 197–218

[DEm04] P. Dèbes and M. Emsalem, *Harbater-Mumford Components and Hurwitz Towers*, Journal of the Institute of Mathematics of Jussieu (2005).

[Fr95] Michael D. Fried, *Introduction to modular towers: generalizing dihedral group–modular curve connections*, Recent developments in the inverse Galois problem (Seattle, WA, 1993), Contemp. Math., vol. 186, Amer. Math. Soc., Providence, RI, 1995, pp. 111–171. [MR1352270 (97a:11070)]

[Fr05a] M. D. Fried, *The place of exceptional covers among all diophantine relations*, J. Finite Fields **11** (2005) 367–433, www.math.uci.edu/˜mfried/#math.

[Fr05b] M. D. Fried, *Alternating groups and moduli space lifting invariants*: www.math.uci.edu/˜mfried/#mt.

[Fr05c] M. D. Fried, *The Main Conjecture of Modular Towers and its higher rank generalization*, in Groupes de Galois arith. et diff. (Lum. 2004; eds. D. Bertrand and P. Dèbes), Sem. et Congres **13**, 2006. www.math.uci.edu/˜mfried/talkfiles/lum03-12-04.html

[Fr05d] M.D. Fried, 5 lectures on the profinite geometry and arithmetic of Modular Towers (MTs); London, Ontario, October 2005, www.math.uci.edu/˜ mfried/talkfiles/london-texas10-05.html:

1. Dihedral groups: Seeing cusps on modular curves from their MT Viewpoint.
2. Alternating groups: The role of g-p' cusps.
3. Colloq.: Cryptography and Schur's Conjecture.
4. Limit groups: Mapping class group orbits and maximal Frattini quotients of dimension 2 p-Poincarè dual groups.
5. Galois closure groups: Outline proof of the Main Conjecture for r=4; variants of Regular Inverse Galois Problem; Serre's Open Image Theorem.

[Fr06] M. D. Fried, *Riemann's existence theorem: An* *elementary approach to moduli*, Five of the six chapters are at www.math.uci.edu/~mfried/#ret.

[FrJ04] M. D. Fried and M. Jarden, *Field arithmetic*, Ergebnisse der Mathematik III, **11**, Springer Verlag, New edition 2004, ISBN 3-540-22811-x.

[R90] K. Ribet, *Review of [Ser68]*, BAMS **22** (1990), 214–218.

[Ser68] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, 1st ed., McGill Univ. Lecture Notes, Benjamin, NY • Amst., 1968, written in collab. with Willem Kuyk and John Labute; 2nd corrected ed. pub. by A. K. Peters, Wellesley, MA, 1998.

[Ser90a] J.-P. Serre, *Relêvements dans* $\tilde{A}_n$, C. R. Acad. Sci. Paris **311** (1990), 477–482.

[Ser90b] J.-P. Serre, *Revêtements a ramification impaire et thêta-caractéristiques*, C. R. Acad. Sci. Paris **311** (1990), 547–552.

[Ser91] J.-P. Serre, *Galois Cohomology*, translated from the Springer French edition of 1964 by Patrick Ion, 1997, based on the revised (and completed) fifth French edition of 1994.

[We05] Th. Weigel, *Maximal* ℓ*-Frattini quotients of* ℓ*-Poincare duality groups of dimension 2*, volume for O. H. Kegel on his 70th birthday, Arkiv der Mathematik–Basel (2005).