Five lectures on the profinite arithmetic geometry of Modular Towers, for London, Ontario, Oct. 2005: Mike Fried, UCI and MSU-B www.math.uci.edu/~mfried/talkfiles/london-texas10-05.html

Talks # 1 and # 2 foreshadow Modular Towers (**MT**s). Talks # 4 and # 5 investigate them directly. Lecture dependencies: #1 $\mapsto$ #2, #3 $\mapsto$ #5; # 3 requires only upper-division algebra; # 1 has the context for # 4.

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

Modular curves systematically use cusps. **MT**s has a group approach to those cusps that generalizes modular curves and their applications. This uses combinatorial groups: subgroups and quotients of *braid groups* (*mapping class groups*) acting on *Nielsen classes* defined by conjugacy classes in any finite group G. Applications vary with the conjugacy classes and with equivalences on Nielsen classes. [Fr06] contains everything you need for Riemann's Existence Theorem and Braid actions.

Dihedral groups: Seeing cusps on modular curves from their **MT** *Viewpoint*

Our Regular Inverse Galois Problem (RIGP) analogy: The modular curve tower for an odd prime p is to **MT**s as the dihedral group D_p is to all p-*perfect* finite groups.

The RIGP asks if for each finite group G some Galois extension $L/\mathbb{Q}(z)$ has group G and $L \cap \mathbb{C} = \mathbb{Q}$. Attached to this are branch points with associated (branch cycle) conjugacy classes **C** of G.

The *Branch Cycle Lemma* limits those **C** that can define a $\mathbb{Q}$ realization. I will explain why each p-perfect group G and set of p' conjugacy classes challenges the RIGP.

- As do modular curve towers, **MT**s have levels corresponding to powers of a prime.
- Our (weak) Main Conjecture on **MT**s says $\mathbb{Q}$ points disappear at high tower levels.

When we use four conjugacy classes, **MT** levels (starting from level 0) are upper half-plane quotients covering the classical j-line. Yet, rarely are they modular curves.

Alternating groups: The role of g-p' cusps

Modular curve towers are **MT**s defined by dihedral groups and four repetitions of the involution conjugacy class. We open the application territory with the case G is an alternating group A_n ($n \geq 4$), $p = 2$ and **C** consists of $r \geq n-1$ 3-cycles. The use of homological algebra is immediate. Describing level 0 **MT** components generalizes Serre's Stiefel-Whitney approach to Spin covers [Ser90b]. There are either 1 or 2 components: each has a Spin invariant value [Fr05b].

This "example" combined with modular curves lie at two extremes in understanding **MT**s. What organizes this example is the notion of g-p' cusps.

Present Inverse Galois applications ([Ca05a], [De04], [DDe04] and [DEm04]) use a special case of g-p' cusps, called *Harbater-Mumford*. A theme in these lectures is that results for H-M cusps should generalize to g-p' cusps, with all of them being avatars of moduli properties that resemble what happens at the "widest" modular curve cusps.

Colloquium: Cryptography and Schur's Conjecture

I will define capitalized words during the talk.

In 1831, 19 year old Everiste Galois introduced **FINITE FIELDS**. The easiest are PRIME finite fields: Integers modulo a prime. You may know bankers who never heard of Galois, yet they know of cryptography and finite fields. Addition and multiplication on these keep financial data secure.

Numbers in a finite field form an **ABELIAN group**. The nonzero numbers form a **CYCLIC** group. This allows encoding data using special polynomials: the easiest being odd degree **CYCLIC POLYNOMIALS** x^3, x^5, ... In 1919 (1923), Group theorist Isaiah Schur guessed at a complete list of polynomials that could encode data in large prime finite fields. These are special cases of *exceptional covers*. We explain why Schur's guess (solved in 1969, after over 500 partial results) was correct. Main tools are **NONABELIAN GALOIS THEORY**, also introduced by Galois, and complex variables.

We conclude with comments on [Fr05a] and [GMS03]. These start from Schur's conjecture to show how exceptional covers are integral to the modern topics of *Serre's Open Image Theorem* and *chow motives*.

Limit groups: Maximal Frattini quotients of dim. 2 p-Poincaré dual groups

The Main **MT** Conjecture matters only when a particular tower has a projective system of components. We rephrase finding such systems to solving embedding problems for group extensions. Here are our key words: What are the maximal p-Frattini quotients (limit groups) of orientable dimension 2 p-Poincaré dual groups defined by a mapping class group orbit.

The legacy work for this is in [Br82] and [Ser91]. We use Weigel's Theorem to get results on possible limit groups ([Fr05c] and [We05]). Even modular curves give something new. A universal *Heisenberg group* obstruction shows why this case has a unique limit group.

A well-supported conjecture suggests when the limit group is maximal possible: equal to the full *universal p-Frattini cover of G*. It is when a component has what we call a g-p' cusp.

We'll do one example in detail: $G = A_4$, **C** is four 3-cycle conjugacy classes and $p = 2$ [Fr05c]. Applying Wohlfahrt's Theorem shows the two level 0 components aren't modular curves, though they look to be, for they have a modular curve property first noted by Abel.

Galois closure groups: Outline proof of Main Conjecture for $r = 4$; variants of Regular Inverse Galois Problem; Serre's Open Image Theorem

Properties of **MT**s conjecturally generalize two famous modular curve results: Mazur-Merel's uniformally bounding rational points on modular curves, and Serre's *Open Image Theorem* (OIT: [R90], [Ser68]).

Distinguishing them has a **MT** phrasing. The former (resp. latter) is a statement on **MT** components from inner (resp. absolute) Nielsen classes. The Mazur-Merel generalization says we can expect no naive approach to the RIGP for any perfect groups.

We relate Serre's renown on modular curves to cryptology (using exceptional covers: Abstract #3).

The Main Conjecture is a weak **MT** version of Serre's Theorem (for modular curves). We'll outline how the universal p-Frattini cover contributes to proving the Main Conjecture for $r = 4$. The **MT**s for $(A_4, \mathbf{C}_{\pm 3^2})$ and $(A_5, \mathbf{C}_{3^4})$ show the proof pieces in action.

Both contribution RIGP applications: The maximal exponent 2 Frattini cover of A_5 (subscript is 5) has ∞ inequivalent 4 branch point realizations only if one of the two genus 1 (among six) level 1 components has a nontorsion $\mathbb{Q}$ point.

A partial bibliography

[An98] Y. André, *Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire*, Crelle's J. **505** (1998), 203–208.

[Ben91] D.J. Benson, *I: Basic representation theory of finite groups and associative algebras*, Cambridge Studies in advanced math., vol. 30, Cambridge U. Press, Cambridge, 1991.

[Br82] K. Brown, *Cohomology of groups*, Grad. texts in Math. **97**, 1982.

[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).

[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/talkfiles

[Fr05c] M. D. Fried, *The Main Conjecture of Modular Towers and its higher rank generalization*, proceedings of Luminy, March 2004. www.math.uci.edu/~mfried/talkfiles/lum03-12- 04.html has related talk and pdf files.

[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.

[GMS03] R. Guralnick, P. Müller and J. Saxl, *The rational function analoque of a question of Schur and exceptionality of permutations representations*, Memoirs of the AMS **162** 773 (2003), ISBN 0065-9266.

[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).

[We64] K. Wohlfahrt, *An extension of F. Klein's level concept*, Ill. J. Math. **8** (1964), 529–535.