SUMMARY OF RESEARCH

CAM MCLEMAN

Aside from some more recent research in algebraic graph theory ([MM09], [MM]) and arithmetic geometry ([MR], [JM09]), my primary research is in the field of algebraic number theory, and more specifically in class field theory. In particular, I focus on the interplay between group-theoretic and class-field-theoretic contributions to the study of Galois groups of class field towers. As will be explained in this research summary, I have proved a refinement of the famous Golod-Shafarevich inequality, and used this refinement (a Golod-Shafarevich equality) to study a class of these groups (namely, $KV$ groups, to be defined later). One application is a computation of the sizes of various canonically-defined subgroups of tower groups, which concludes in providing a rather large cardinality bound on a particular type of $KV$ group. The conditions thus placed on groups of this type are restrictive enough so that no finite group is known to satisfy all of them. A second application of my research is a succinct cohomological condition for the infinitude of the $p$-class field tower over a quadratic imaginary number field. These results will be stated precisely after a quick summary of the background material.

Let $K$ be a number field and $p$ a prime. Class field theory provides a distinguished field extension $K^{(1)}$ of $K$, the so-called Hilbert $p$-class field of $K$, defined as the maximal abelian $p$-extension of $K$ which is everywhere unramified. By iterating this construction, i.e., by obtaining the Hilbert $p$-class field $K^{(2)}$ of $K^{(1)}$, and so on, we arrive at a tower (the $p$-class field tower over $K$) of extensions

$$K = K^{(0)} \subset K^{(1)} \subset K^{(2)} \subset \cdots \subset K^{(n)} \subset K^{(n+1)} \subset \cdots,$$

each term of which contains arithmetic information about the previous one, and hence about $K$ itself. An immediate first question is whether or not this tower stabilizes for a given base field $K$, which by class field theory occurs if and only if $K$ admits a finite algebraic extension whose ring of integers has class number prime to $p$ (a subtle arithmetic condition which arises, for example, in attempts to prove Fermat’s Last Theorem). Also of major interest is the length of the tower over $K$, i.e., the minimal (possibly infinite) $n$ such that $K^{(n)} = K^{(n+k)}$ for all $k \geq 0$, and the folklore “unbounded lengths conjecture” that there exist number fields with arbitrarily long finite class field towers. Regardless of the length, it is easy to check that the top of the tower $K^{(\infty)} := \bigcup_{n=0}^{\infty} K^{(n)}$ is Galois over $K$, and we are led to the question of describing the pro-$p$-group $G := \text{Gal}(K^{(\infty)}/K)$, the tower group over $K$. In particular, the question of whether or not the tower stabilizes is rephrased simply as asking when $G$ is finite, and the unbounded lengths conjecture is rephrased as asking if a finite such $G$ can have arbitrarily long derived series.

Among the very few results we have available to resolve these questions, of principal importance is the famous theorem of Golod and Shafarevich ([GS64]). A weak form of this states that if a finite $p$-group $G$ is given a minimal pro-$p$-presentation with $d$ generators and $r$ relations, then we must have $r > \frac{d^2}{4}$. Even recent papers cite this as the state of the art, but there is much more we can extract from a full version of Golod-Shafarevich ([Ko69]), which we will need some preliminaries to state. Suppose that $G$ is a $d$-generated pro-$p$-group, and let $F$ be the free pro-$p$-group on the generators of $G$, giving a presentation $1 \to R \to F \to G \to 1$. Let $I = \langle \sigma - 1 \rangle_{\sigma \in G}$ be the augmentation ideal inside of the group ring $\mathbb{F}_p[F]$, and define the Zassenhaus filtration of $F$ by

$$F_n := \{ f \in F \mid f - 1 \in I^n \}.$$  

For a given element $f \in F$, we define the level of $f$ to be the unique $n$ such that $f \in F_{n} \setminus F_{n+1}$. Choose a (topological) generating set $\{ \rho_i \}_{i \in I}$ for $R$ as a normal subgroup of $F$, and let $r_k$ denote the number of these relations of level $k$. The stronger version of the Golod-Shafarevich inequality due to Koch states that for a
finite $p$-group $G$, and any presentation as above, we have the following inequality for all $t \in (0, 1)$:
\[
\sum_{k=2}^{\infty} r_k t^k - dt + 1 > 0.
\]

We now return to tower groups, and assume that $p > 2$ (the case $p = 2$ having been much more extensively studied). Here we can use other properties of a tower group $G$ in the case that $K$ is a quadratic imaginary number field:
- Shafarevich ([Sh63]) has calculated that $r(G) = d(G)$.
- Koch and Venkov ([KV74]) proved that $G$ admits a presentation with $r_{2k} = 0$ for all $k$.

These facts at hand, this stronger version of Golod-Shafarevich implies that $G$ is infinite whenever $d \geq 3$. We note that when $d = 1$, $G$ is cyclic and hence corresponds to a $p$-class field tower of length 1, so the only non-trivial (i.e., length strictly between 1 and infinity) towers over quadratic imaginary number fields with $d(G) = 2$. We will call such groups $KV$ groups. It is worth emphasizing that class field theory tells us that $d$ can be computed as the $p$-rank of the class group of $K$, which led to the first examples of infinite class field towers by finding number fields with large class groups.

The application of Golod-Shafarevich to conclude that $d < 3$ for finite towers is only the beginning of the story for $KV$ groups. Namely, the Golod-Shafarevich inequality reduces in this case to the statement that $t^i + t^j - 2t + 1 > 0$ for all $t \in (0, 1)$, where $i$ and $j$ are the levels of the two relations chosen to generate $R$ as a normal subgroup of $F$. Combined with the parity argument of Koch-Venkov that we can take both $i$ and $j$ to be odd for a quadratic imaginary number field, we are left with very few possible relation levels for which this inequality is not violated. Specifically, since the polynomials $t^5 + t^7 - 2t + 1$ and $2t^5 - 2t + 1$ both have roots in the unit interval (and hence violate the inequality), we find that the pair $(i, j)$ must assume one of only three possible values:
\[(i, j) \in \{(3, 3), (3, 5), (3, 7)\}.
\]

For a given $G$, we can choose a presentation with relations of deepest possible level, and refer to the uniquely defined pair $(i, j)$ above as the $Zassenhaus type$ (or $Z$-type) of the group.

We turn now to my research, which was motivated in part by the numerics of the third of these three Zassenhaus types – the polynomial $t^5 + t^7 - 2t + 1$ is minimized on the unit interval at approximately $(0.67, 0.02)$, so that while the Golod-Shafarevich inequality does not quite rule out this option, it suggests that such a group must be rather exceptional. Also suggested by this observation is that better book-keeping of whatever error terms are responsible for the “inequality” in the Golod-Shafarevich inequality might rule out the $(3, 7)$ possibility altogether. Keeping track of these errors leads to a Golod-Shafarevich $equality$, for which we will need some notation. First, since the successive factors $G_n/G_{n+1}$ of the Zassenhaus filtration of $G$ are naturally $\mathbb{F}_p$-vector spaces, we can define $a_n = \dim_{\mathbb{F}_p} G_n/G_{n+1}$, an important series of invariants which appear in the Golod-Shafarevich equality below. Finally, let $c_n = \dim_{\mathbb{F}_p} \mathbb{F}_p[G]/I^n$.

**Theorem** (M., [Mc09]). For a finite $p$-group $G$, and all other notation as above, we have
\[
\sum_{k=2}^{\infty} r_k t^k - dt + 1 = \prod_{n=1}^{\infty} \left( \frac{1 - t^n}{1 - I^n} \right)^{a_n} + \sum_{k=1}^{\infty} c_k t^n
\]
for all $t \in (0, 1)$, and for some sequence of “error coefficients” $e_n$ defined explicitly in the paper.

**Remarks.**
- The history of the building of this result is rather complex, and my contribution is only the latest in a series of contributions from Golod and Shafarevich ([GS64]), Koch ([Ko69]), and Jennings ([Je41]).
- Though we don’t define the $e_n$ terms here, we remark that they are non-negative integers which eventually agree with the $c_n$, which in turn stabilize at $|G|$. Thus both of these power series converge and are non-zero on the unit interval, which leads to a strict improvement of the Golod-Shafarevich inequality. It is worth noting that it is by no means $a priori$ clear that the right-hand side of this equation is a polynomial.

The “full” Golod-Shafarevich inequality from before is now just the observation that the right-hand side of the equality is positive on the unit interval. Further, I prove in [Mc08a] some lower bounds on $e_n$ and
upper bounds on $c_n$ which I use to improve the strongest-known form of the Golod-Shafarevich inequality, and lead to some fairly strong conclusions about our $Z$-type $(3,7)$ groups from above. In brief, the fact that the inequality $t^2 + t^3 - 2t + 1 > 0$ was only barely satisfied implies strong combinatorial restrictions on the sequence of $a_n$‘s, and since $|G| = p^{\sum a_n}$, these restrictions allow us to conclude that the group must be rather large for the inequality to hold. Finally, the Golod-Shafarevich equality lets us compute small values of $a_n$, and we can conclude about the following tower groups of this $Z$-type.

**Theorem** (M., [Mc09]). Let $G$ be a finite $p$-group of $Z$-type $(3,7)$. Then $|G : G_2| = p^2$, and $|G_2 : G_3| = |G_3 : G_4| = |G_4 : G_5| = p$. If we write $G_{ab} \approx (p^a, p^b)$ with $1 \leq a \leq b$ and further suppose that $p > 7$, we have $|G| \geq p^{20+2a+b}$. In particular, $|G| \geq p^{23}$, and $|G'| \geq p^{20+a} \geq p^{21}$.

This result translates via the language of class field towers into the following corollary:

**Corollary.** Let $K$ be a quadratic imaginary number field with $p$-class group isomorphic to $(p^a, p^b)$ (with $1 \leq a \leq b$, and $p > 7$), and suppose that $G := \text{Gal}(K^{(\infty)}/K)$ is of $Z$-type $(3,7)$. Then $|G| \geq p^{20+2a+b} \geq p^{23}$. In particular, $|\text{Gal}(K^{(\infty)}/K^{(1)})| \geq p^{20+a} \geq p^{21}$.

This cardinality bound, in conjunction with my computation of the index of each of the first few dimension subgroup of such a group, represents new and severe limitations on the set of groups which can occur in towers of the above type. In particular, no finite group is known to satisfy all of these properties. Finally, we mention a more recent result building on work of Vogel [Vo04], a succinct cohomological condition for the infinitude of a KV group.

**Theorem** (M., [Mc08b]). Let $K$ be a quadratic imaginary number field with tower group $G$ satisfying $d(G) = 2$. Choose a basis $\{\chi_1, \chi_2\}$ for $H^1(G, F_p)$, and suppose $p > 3$. Then $G$ is infinite if the triple Massey products $(\chi_1, \chi_2, \chi_1)$ and $(\chi_1, \chi_2, \chi_2)$ both vanish. For $p = 3$, we need in addition the triviality of the triple Massey products $(\chi_1, \chi_1, \chi_1)$ and $(\chi_1, \chi_2, \chi_2)$.

A major next step will be to calculate these triple Massey products. This has been done successfully in the $p = 2$ case by Morishita and Vogel, but is completely open for $p$ odd. This is the next step in my research, the ultimate goal being a succinct necessary and sufficient condition for the infinitude of the $p$-class field tower over a quadratic imaginary number field, a specific form of which I conjecture in [Mc08b].

**References**


