

SUMMARY OF RESEARCH

CAM MCLEMAN

My research is in the field of algebraic number theory, particularly on the interplay between some group-theoretic and class-field-theoretic contributions to the study of some particularly important Galois groups (*interesting tower groups*, to be defined later). As will be explained, I have proved a refinement of the famous Golod-Shafarevich inequality, and used this refinement (a Golod-Shafarevich *equality*) to compute the sizes of various canonically-defined subgroups of interesting tower groups. As an application, I provide evidence, in the form of a rather large cardinality bound, that one of the three *a priori* possible types of these groups never actually occurs, thereby putting further restrictions on this particularly mysterious class of groups. We now turn to making this precise.

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

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

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 . 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. More generally, it is not difficult to show that the top of the tower $K^{(\infty)} := \bigcup_{i=0}^{\infty} K^{(i)}$ 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 $r > \frac{d^2}{4}$. Many 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 $1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$. 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

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

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 for technical reasons that $p > 2$. 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 *interesting tower groups*. It is worth mentioning 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 interesting tower 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 $t^9 + t^3 - 2t + 1$ 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 $t^7 + t^3 - 2t + 1$ is minimized on the unit interval at approximately $(.67, .02)$, 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 led me to a Golod-Shafarevich *equality*, for which we will need some new notation. First, one checks easily that the successive factors G_n/G_{n+1} of the Zassenhaus filtration of G are naturally \mathbb{F}_p -vector spaces, and we 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, 2007). *For a finite p -group G , and all other notation as above, we have*

$$\sum_{k=2}^{\infty} r_k t^k - dt + 1 = \prod_{n=1}^{\infty} \left(\frac{1 - t^n}{1 - t^{np}} \right)^{a_n} + \frac{\sum e_n t^n}{\sum c_n t^n}$$

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 here, we remark that they are non-negative integers which eventually agree with the c_n , which in turn stabilize at $|G|$, so that both of these power series converge and are non-zero on the unit interval. 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 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. Namely, the fact that the inequality $t^7 + t^3 - 2t + 1 > 0$ was only barely satisfied implies strong combinatorial restrictions on the sequence of a_n ’s, and since $|G| = p^{\sum a_n}$, those 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 the following about interesting tower groups.

Theorem (M, 2007). *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 $|G'| \geq p^{20+a} \geq p^{21}$.*

Remarks. There are similar results for the dimension factors for the Z -type $(3, 3)$ and $(3, 5)$ cases, but the cardinality bounds apply only to the $(3, 7)$ case. Also, there are slightly weaker cardinality bounds for the $(3, 7)$ case with $p \leq 7$.

The above theorem 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 subgroups 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.

Future Work. There are several branch points at this stage of my research. I outline here a few of the more promising ideas:

- It is easy to isolate the key properties of quadratic imaginary number fields which facilitated the theorem, namely that $r = d$ and that $r_{2k} = 0$. There are potentially other fields where the same tricks may apply. CM fields are natural candidates, and there is a natural reformulation of the needed results into a more cohomological setting ([KL89]) which may prove more tractable. On a related note, Romyar Sharifi (e.g. [Sh07]) has had success in showing the finiteness of class field towers over some CM (namely, cyclotomic) fields by appealing to verified cases of Greenberg’s conjecture.
- Similarly, much of this theory could be carried over to other 2-generated 2-related groups. Another class of such groups which has gained prominence recently are the Galois groups $\text{Gal}(\mathbb{Q}_S/\mathbb{Q})$ of the maximal extension of \mathbb{Q} unramified outside a set S consisting of two primes. Nigel Boston (e.g. [Bo06]) has made progress writing down presentations for these groups, and has found a combinatorially-described set of parameters for the relations occurring in these presentations. It would not be surprising if the combinatorics related to dimension subgroups were related to the combinatorics surrounding the relations in these groups, but this relationship has yet to be explored.
- Denis Vogel ([Vo04]) has shown that the fact that $r_2 = 0$ implies the existence of well-defined triple Massey products on the p -part of the class group. His calculations of these products should lead to a clearer picture of the image of the relations defining G under the Magnus map, which were important for my calculations for the first few values of a_n . It is likely that the Massey product interpretation will extend these calculations.

REFERENCES

- [Bo06] Boston, Nigel. *Reducing the Fontaine-Mazur Conjecture to Group Theory*. In *Progress in Galois Theory*. Developments in Mathematics Series, Volume 12. Springer, 2005.
- [Bu03] Bush, M.R. *Computation of the Galois groups associated to the 2-class towers of some quadratic fields*. *J. Number Theory* **100**. 2003. 313-325.
- [GS64] Golod, E.S. and Safarevic, I.R. *On Class Field Towers* (in Russian). *Izv. Akad. Nauk. SSSR*. **28**, 1964. 261–272. (English translation by K. A. Hirsch *AMS Translations* (2) **48**, 91-102).
- [Je41] Jennings, S. A. *The structure of the group ring of a p -group over a modular field*. *Trans. Amer. Math. Soc.* 50, (1941). 175–185.
- [KL89] Kisilevsky, H. and Labute, J. *On a sufficient condition for the p -class tower of a CM-field to be infinite*. *Théorie des nombres* (Quebec, PQ, 1987), 556–560, de Gruyter, Berlin, 1989.
- [Ko69] Koch, Helmut. *Zum Satz von Golod-Shafarevich*. (German) *Math. Nachr.* 42 (1969), 321–333.
- [KV74] Koch, H. and Venkov, B. *The p -tower of class fields for an imaginary quadratic field (Russian)*. *Zap. Nau. Sem. Leningrad Otdel. Mat. Inst. Steklov (LOMI)* 46 (1974).
- [Sh63] Shafarevich, I. *Extensions with prescribed ramification points*. *Inst. Hautes tudes Sci. Publ. Math.* No. 18 1963 71–95.
- [Sh07] Sharifi, Romyar. *On Galois groups of unramified pro- p extensions*, in preparation.
- [Vo04] Vogel, Denis. *Massey Products in the Galois Cohomology of Number Fields*. PhD thesis, University of Heidelberg, 2004.