

HEURISTICS FOR 2-CLASS TOWERS OF CYCLIC CUBIC FIELDS

NIGEL BOSTON AND MICHAEL R. BUSH

ABSTRACT. We consider the Galois group $G_2(K)$ of the maximal unramified 2-extension of K where K/\mathbb{Q} is cyclic of degree 3. We also consider the group $G_2^+(K)$ where ramification is allowed at infinity. In the spirit of the Cohen-Lenstra heuristics, we identify certain types of pro-2 group as the natural spaces where $G_2(K)$ and $G_2^+(K)$ live when the 2-class group of K is 2-generated. While we do not have a theoretical scheme for assigning probabilities, we present data and make some observations and conjectures about the distribution of such groups.

1. INTRODUCTION

In the 1980s, Cohen and Lenstra [7] gave a theoretical framework for the variation of class groups of quadratic fields. The Cohen-Lenstra idea is twofold: the first part is to identify, in any relevant number-theoretical situation, the correct collection of groups which can arise as the groups of number-theoretical interest; the second part is to define a natural measure or probability distribution on this collection. The heuristic then is that the probability attached to the group in the identified collection is the same as the frequency of occurrence as a group of number-theoretical interest.

In [4] and [5], we initiated the study of a natural non-abelian extension of Cohen and Lenstra's work. For a number field K and rational prime p , we considered the Galois group $G_p(K)$ of the maximal unramified p -extension of K . Note that the maximal abelian quotient $G_p(K)^{\text{ab}}$ is isomorphic to the p -class group of K by class field theory. We call $G_p(K)$ the p -class tower group of K , since that is how it first arose in the 1930s in the work of Artin, Hasse, Furtwängler and others. In [4], together with Farshid Hajir, we treated the case of imaginary quadratic fields and in [5] the case of real quadratic fields, when p is an odd prime. The content of each of these papers included a) an identification of the “right” collection of groups, b) an investigation of an associated measure giving the frequency of groups within that collection, and c) a numerical study of p -class tower groups of both types of quadratic field to test the conjecture developed using a) and b).

In this work, we treat cyclic cubic fields in a similar manner for the most interesting case when $p = 2$. The situation when $p > 3$ gives rise to a theory very much like that elucidated in our earlier papers, and one that fits naturally into the more general framework recently developed by Liu, Wood, and Zureick-Brown [13]. The case of $p = 2$ is as yet uncharted and introduces some new and unexpected considerations, related to the fact that the ground field \mathbb{Q} contains a primitive p th root of unity [10], [14]. Here even the study of frequency of p -class groups is relatively untouched, with some first steps taken by Malle and Adam [17], building on [14] and [15]. The case of $p = 3$ is quite different, and related to extensions of genus theory [11], [18].

2010 *Mathematics Subject Classification.* 11R29, 11R16.

Key words and phrases. Cohen-Lenstra heuristics, class field tower, cyclic cubic field, ideal class group.

The organization of the paper is as follows. In Section 2, we introduce our main objects of interest, cyclic cubic fields and their narrow and wide 2-class tower groups. This leads us to focus on a subclass of 2-groups, called valid, and we describe how these are represented by the nodes of a tree. In Section 3, we associate to each valid group a 3-tuple of abelian groups, called its IPAD. The IPADs of tower groups are readily calculated and can then be used to identify the groups or at least narrow down the possibilities. In Section 4, we use embedding theory and Galois cohomology to show that the narrow 2-class tower groups lie in a certain class of groups, which we call 2-special, and in Section 5 we likewise identify a class of groups, called 2-select, that contains the wide 2-class tower groups.

We conjecture that every 2-special group does arise as the narrow tower group of some cyclic cubic field and that every 2-select group arises as the wide tower group of some such field. Ultimately we would like to know the joint distribution, but there appear to be some as yet unknown subtleties as to the support of this distribution. After summarizing previous work on the distribution for the wide 2-class groups, in Section 7 we present data on the narrow and wide IPADs of the first 500,000 cyclic cubic fields with 2-generated 2-class group, ordered by discriminant. This is then used to substantiate the claims at the start of this paragraph.

Although we cannot obtain general formulae for how frequently a given group arises as a narrow or wide 2-class tower group, the data give us explicit, albeit somewhat mysterious, values for the joint distribution of the 2-class 3 quotients of the narrow and wide tower groups. We can also pin down the joint distribution induced on the abelianizations (the narrow and wide 2-class groups).

One consequence is an explanation of Rubinstein-Salzedo's observation that cyclic cubic fields with 2-class group of order 4 have 2-class tower group of order 4 about 53.7% of the time and of order 8 about 46.3% of the time. At the same time we explain why this is still consistent with the conjecture that unramified $(\mathbb{Z}/2)^2$ -extensions of cyclic cubic fields are as likely as not to extend to unramified Q_8 -extensions.

Lastly, in Section 8, we consider the possibility of infinite narrow 2-class towers. By random search, filtering out presentations that yield finite or 2-adic analytic groups, we are led to a very special family of groups. Moreover, the corresponding wide 2-class tower group then turns out to be a certain group of order 2048.

2. PRELIMINARIES

Throughout this paper, K will denote a cyclic cubic field with $\Delta = \text{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle$ where σ is an automorphism of order 3. Let $\text{Cl}_2(K)$ denote the 2-class group of K and $G_2(K) = \text{Gal}(K^{nr,2}/K)$ where $K^{nr,2}/K$ is the maximal unramified 2-extension of K . We will call $G_2(K)$ the *2-class tower group of K* . By class field theory, $\text{Cl}_2(K)$ is isomorphic to the abelianization $G_2(K)/[G_2(K), G_2(K)]$. If we allow ramification at infinity, then we get the narrow analogs of these objects. In particular, we will let $\text{Cl}_2^+(K)$ denote the narrow 2-class group and call $G_2^+(K)$ the *narrow 2-class tower group of K* . To distinguish, $\text{Cl}_2(K)$ and $G_2(K)$ are often called *wide*.

By the Schur-Zassenhaus Theorem, the Galois group Δ acts by conjugation on $G_2(K)$ and $G_2^+(K)$. Moreover $G_2(K)$ is the quotient of $G_2^+(K)$ by the closure of complex conjugation under this action. Under the isomorphism to the corresponding wide and narrow 2-class

groups, the induced action on the abelianizations translates into the usual Galois action on ideal classes. Let V denote the unique irreducible $\mathbb{F}_2[\Delta]$ -module of dimension 2 over \mathbb{F}_2 .

Lemma 2.1. *As $\mathbb{F}_2[\Delta]$ -modules, $\text{Cl}_2(K)/\text{Cl}_2(K)^2$ and $\text{Cl}_2^+(K)/\text{Cl}_2^+(K)^2$ are each isomorphic to V^d for some non-negative integer d . It follows that the generator rank g of $\text{Cl}_2(K)$ (which equals that of $G_2(K)$) is even, namely $2d$, and equal to that of $\text{Cl}_2^+(K)$ (and so of $G_2^+(K)$).*

Proof. Since $\gcd(2, 3) = 1$, no ideal class I can be fixed under this action since the product $I\sigma(I)\sigma^2(I)$ is trivial. By Maschke's Theorem, it follows that the $\mathbb{F}_2[\Delta]$ -module $\text{Cl}_2(K)/\text{Cl}_2(K)^2$ decomposes as a direct sum of copies of V . In particular, we see that the generator rank is always even since V has dimension 2. Similar arguments apply to $\text{Cl}_2^+(K)$ and $G_2^+(K)$. By [1], the generator ranks of $\text{Cl}_2(K)$ and $\text{Cl}_2^+(K)$ differ by at most 1 and so they are always equal in our situation. \square

The group $G_2(K)$ is a finitely presented pro-2 group and $\text{Cl}_2(K)$ is a finite abelian 2-group. Before proceeding further we recall some notions and terminology from group theory that will be useful. For a pro-2 group G , recall that $d(G) = \dim_{\mathbb{F}_2} H^1(G, \mathbb{F}_2)$ and $r(G) = \dim_{\mathbb{F}_2} H^2(G, \mathbb{F}_2)$ are its minimal number of (topological) generators and relations, respectively. Setting $g = d(G)$, we can view G as a quotient of the free pro-2 group F on g generators x_1, \dots, x_g .

The 2-central series of a pro-2 group G is the series of closed subgroups defined by:

$$P_0(G) = G, \quad P_{n+1}(G) = P_n(G)^2[G, P_n(G)].$$

Note that $P_1(G)$ is the Frattini subgroup, $\Phi(G)$. If $P_n(G) = 1$ for some n and n is minimal, then we say G has 2-class n . Finite 2-groups always have finite 2-class. If G is a finitely generated pro-2 group, then $Q_n(G) := G/P_n(G)$ is a finite 2-group which we call the maximal 2-class n quotient of G . We say that G is a descendant of $Q_n(G)$ and call $Q_{n+1}(G)$ an immediate descendant or child of $Q_n(G)$ (if not isomorphic to it). If we connect groups that are immediate descendants with an edge, then the finite g -generated 2-groups form a tree with root the elementary abelian 2-group $(\mathbb{Z}/2)^g$. There is an algorithm due to O'Brien [19], implemented in MAGMA [2], that yields all the children of any given p -group, thus allowing one to compute successive levels of this tree.

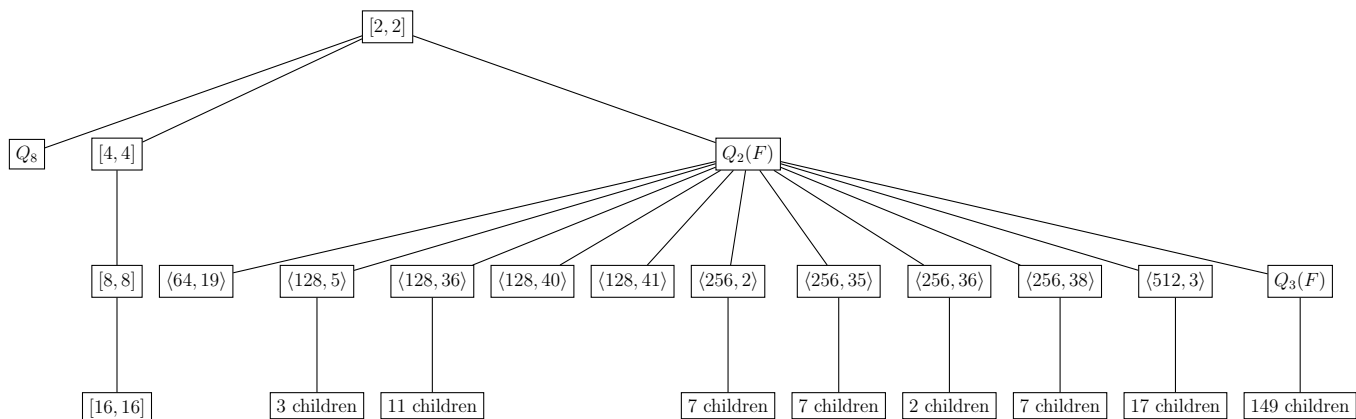
In later sections, we will restrict attention to the situation where $G = G_2(K)$ has generator rank $g = d(G) = 2$. In this case, $Q_1(G) \cong (\mathbb{Z}/2)^2$. For brevity's sake, we use the standard notation $[2, 2]$ for this abelian group. By O'Brien's algorithm, $[2, 2]$ has 7 children, namely $[2, 4]$, D_8 , Q_8 , $[4, 4]$, two other groups of order 16, and $Q_2(F)$ of order 32.

Definition 2.2. A 2-generator (pro)-2-group with an automorphism of order 3 will be called *valid*.

All the Galois groups we are considering are valid, thanks to the Δ -action. If G is valid, then since the subgroups in its 2-central series are characteristic, the quotient $Q_n(G)$ is itself valid for all $n \geq 1$. Of the 7 children of $[2, 2]$, only Q_8 , $[4, 4]$, and $Q_2(F)$ are valid. Of these, Q_8 has no children, whereas the only valid descendants of $[4, 4]$ are the abelian groups $[2^n, 2^n]$. This can be verified by first showing that the 2-covering group for $[2^n, 2^n]$ (as defined in [19]) is the group G^* of order 2^{2n+3} with presentation

$$G^* = \langle x, y \mid x^{2^{n+1}}, y^{2^{n+1}}, (x, y)^2, (x, (x, y)), (y, (x, y)) \rangle$$

FIGURE 1. Tree of valid 2-groups of 2-class at most 4.



where $(x, y) = x^{-1}y^{-1}xy$. By considering suitable quotients of this group, one can verify that $[2^n, 2^n]$ has 4 children for all $n \geq 2$ and that only the child $[2^{n+1}, 2^{n+1}]$ is valid.

It follows that most of the groups we encounter later are descendants of $Q_2(F)$. This has 93 children, but only 11 of them are valid.

Of these 11, 3 are childless; 1 has just 2 valid children, both childless; 1 has 3 valid children and a very straightforward subtree of descendants; 3 have 7 valid children; 1 has 11 valid children; 1 has 17 valid children; and 1 has 149 valid children.

Figure 1 depicts this tree. Note that $\langle n, i \rangle$ is shorthand for $\text{SmallGroup}(n, i)$ in the standard Magma database [2].

3. IPADs

Note that the use of IPAD in this section differs slightly from our usage in [4] and [5], where we did not include abelianizations of any index p^2 subgroups.

Let G be a 2-generator pro-2 group. Then it has three (open) maximal subgroups M and if G is valid, these form an orbit under the order-three automorphism and so are isomorphic.

Definition 3.1. The IPAD of a valid G , $IPAD(G)$, consists of a triple of finite abelian groups, namely G^{ab} , M^{ab} , $\Phi(G)^{ab}$.

For example, for $G = \text{SmallGroup}(8, 4)$ ($= Q_8$), $IPAD(G) = [[2, 2]; [4]; [2]]$, whereas for $G = \text{SmallGroup}(64, 19)$, $IPAD(G) = [[4, 4]; [2, 2, 4]; [2, 2, 4]]$. Several small valid 2-groups are determined up to isomorphism by their IPAD. This includes the two groups just given.

The motivation behind this definition is that we will be able to compute the IPADs of various Galois groups of interest to us, raising the question of whether these IPADs enable us to identify the Galois groups.

We can determine which groups correspond to a given IPAD by tracking how the IPAD varies as we move down the O'Brien trees introduced in Section 2. In particular, the IPAD of a group is a quotient of the IPAD of any of its descendants and if the IPADs are the same for a group and a child, then every subsequent descendant will have the same IPAD.

Table 1 organizes IPADs into clumps according to the complexity of their entries and indicates which valid groups have each IPAD. Different clumps correspond to different parts

of the tree: for instance the first clump consists of the quaternion group of order 8 and the abelian groups $[2^n, 2^n]$.

TABLE 1. Groups with a given IPAD.

$[2, 2]; [2,]$	$\langle 4, 2 \rangle$
$[2, 2]; [4]; [2]$	$\langle 8, 4 \rangle$
$[4, 4]; [2, 4]; [2, 2]$	$\langle 16, 2 \rangle$
$[8, 8]; [4, 8]; [4, 4]$	$\langle 64, 2 \rangle$
$[16, 16]; [8, 16]; [8, 8]$	$\langle 256, 39 \rangle$
...	
$[4, 4]; [2, 2, 4]; [2, 2, 2]$	$\langle 32, 2 \rangle$
$[4, 4]; [2, 2, 4]; [2, 2, 4]$	$\langle 64, 19 \rangle$
$[4, 4]; [2, 2, 4]; [2, 4, 4]$	$\langle 128, 40 \rangle, \langle 128, 41 \rangle$
$[4, 4]; [2, 4, 4]; [4, 4, 4]$	$\langle 256, 36 \rangle$, its 2 children of order 1024 (both childless)
$[4, 4]; [2, 2, 8]; [4, 4, 4]$	$\langle 256, 38 \rangle$
$[4, 4]; [2, 2, 8]; [4, 4, 8]$	$\langle 512, 858 \rangle$
$[4, 4]; [2, 2, 8]; [4, 8, 8]$	3 groups order 1024 (all childless - children of $\langle 256, 38 \rangle$)
$[4, 4]; [2, 2, 16]; [8, 8, 8]$	3 groups order 2048 (children of $\langle 256, 38 \rangle$), all descendants of 2 of these
...	
$[8, 8]; [2, 4, 8]; [2, 4, 4]$	$\langle 128, 5 \rangle$
$[8, 8]; [2, 4, 8]; [2, 8, 8]$	$\langle 512, 104 \rangle, \langle 512, 106 \rangle$ (both childless - children of $\langle 128, 5 \rangle$)
$[8, 8]; [2, 4, 8]; [4, 4, 4]$	$\langle 256, 2 \rangle, \langle 512, 451 \rangle$ (childless - child of $\langle 256, 2 \rangle$)
$[8, 8]; [2, 4, 16]; [4, 8, 8]$	2 children of $\langle 256, 2 \rangle$ and all their descendants
$[8, 8]; [2, 8, 8]; [4, 8, 8]$	2 children of $\langle 256, 2 \rangle$ and all their descendants
...	
$[4, 4]; [2, 2, 4]; [2, 2, 2, 2, 2]$	$\langle 128, 36 \rangle$ and all its descendants
$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	$\langle 256, 35 \rangle$ and all its descendants (includes $\langle 512, 844 \rangle$)
$[8, 8]; [2, 4, 8]; [2, 2, 2, 4, 4]$	$\langle 512, 3 \rangle$ and many but not all its descendants
...	

4. THE CLASS OF NARROW TOWER GROUPS

Our first interesting observation was that there appears to be no cyclic cubic field K such that $G_2(K) \cong [4, 4]$. This can be proved using embedding theory.

Theorem 4.1. *There is no cyclic cubic field K whose 2-class tower group is isomorphic to $[4, 4]$.*

Proof. Let L/K be a Galois 2-extension with Galois group G which is unramified at all finite primes and Galois over \mathbb{Q} . Then there exists a Galois extension E/\mathbb{Q} , containing L , unramified over K at all finite primes, with $\text{Gal}(E/L)$ isomorphic to the Schur multiplier $M(G \rtimes \Delta)$ [9] (Corollary 2 to Theorem 3.13). In particular, for $G = [4, 4]$, $M(G \rtimes \Delta) \cong \mathbb{Z}/4$ and $\text{Gal}(E/\mathbb{Q}) \cong \langle 192, 4 \rangle$. Complex conjugation is an element of order 1 or 2 inside its center ($= \text{Gal}(E/L)$) and in particular therefore does not generate it. It follows that there is a nontrivial subextension of E/L unramified at all finite and infinite primes, so L cannot be the maximal unramified 2-extension of K . \square

More generally, this same argument suggests that we should focus on the narrow class tower group, which we have denoted $G_2^+(K)$. The above embedding theory argument extends to

imply that $G_2^+(K)$ belongs to a certain special family of groups. This theory is elucidated in [13] where the authors call this Property E. We will call groups with Property E special.

Theorem 4.2. *Suppose G is a finite 2-group which is valid and satisfies $d(G) = 2$. The following are equivalent.*

- (1) G has no central extension by $\mathbb{Z}/2$ that is valid.
- (2) The Schur multiplier $M(G \rtimes \Delta)$ is trivial.
- (3) Let F be free pro-2 on 2 generators x, y . Let σ be the automorphism of order 3 defined by $\sigma(x) = y^{-1}, \sigma(y) = xy^{-1}$. Let $X = \{u^{-1}\sigma(u) : u \in \Phi(F)\}$. For $u \in X$, let π_u denote the pair $\{u, \sigma(u)\}$. G is a finite quotient of F by a finite number of pairs π_u .

Proof. Proposition 3.12 of [13]. □

Definition 4.3. A group satisfying any of these equivalent statements will be called *special*.

An exhaustive check finds that there are only 6 special groups of order at most 512, namely $\langle 8, 4 \rangle, \langle 64, 19 \rangle, \langle 256, 36 \rangle, \langle 512, 451 \rangle, \langle 512, 844 \rangle, \langle 512, 858 \rangle$.

Definition 4.4. Call the group k -special if it can be presented as in (3) above, using no more than k pairs.

Galois cohomology implies that if $G = G_2^+(K)$ with K cyclic cubic, then $r(G) - d(G) \leq 2$. This follows from (11.12) in Section 11.3 of [12]. It follows that:

Theorem 4.5. *If K is a cyclic cubic field with $d(Cl_2(K)) = 2$, then $G_2^+(K)$ is a 2-special 2-group if it is finite.*

Proof. By the above, $r(G_2^+(K)) \leq 4$ and now proceed as in Proposition 3.21 of [13]. □

Of the 6 special groups above, all but $\langle 512, 844 \rangle$ are 2-special ($\langle 512, 844 \rangle$ has relation rank 6). Working systematically, we discover that there are exactly 9 2-special groups of 2-class at most 4. With high confidence extensive searches indicate that there are 28 2-special groups of 2-class at most 5 and at least 800 of 2-class at most 6. To do this we took 2 pairs (as in Theorem 4.2 (3)) at random from the Frattini subgroup of $Q_7(F)$ 100 million times and saved any groups this yielded that had 2-class 6 or less. After the first million or so, no new groups of 2-class 5 or less or of order 2^{20} or less appeared.

Table 2 indicates for each small n how many 2-special groups there are of order 2^n and 2-class at most 6. (The smallest 2-special groups of 2-class 7 found so far have order 2^{17} . With high confidence our table is complete for $n \leq 20$.) The ones for $n \leq 9$ were identified above. The two for $n = 10$ are the children of $\langle 256, 36 \rangle$ referenced in the IPAD table.

In computing lists of 2-special groups, we observed they are mostly childless (for instance, out of the 800 in our list, all but 19 are childless). More specifically, using the notion of nuclear rank defined in [19], we conjecture the following (note that childless groups are precisely those with nuclear rank 0):

Conjecture 4.6. *Every 2-special group has nuclear rank 0 or 2. Its valid children are always 2-special.*

Interestingly the special, but not 2-special, group $\langle 512, 844 \rangle$ has 3 valid children, one of which is 2-special but the other two of which are not special.

The 800 2-special 2-groups found will be ordered by the compact presentation of their standard presentation [20]. We will use N_k to refer to the k th group in this list. For

$k = 1, 2, \dots, 5$, these are respectively $\langle 8, 4 \rangle, \langle 64, 19 \rangle, \langle 256, 36 \rangle, \langle 512, 858 \rangle, \langle 512, 451 \rangle$. N_6 and N_7 are the two valid children of $\langle 256, 36 \rangle$, of order 1024. N_8 is the 2-special child of $\langle 512, 844 \rangle$, so of 2-class 5, of order 2048, whereas N_9 and N_{10} are children of $\langle 256, 38 \rangle$ and $\langle 256, 2 \rangle$ respectively, so of 2-class 4, of order 2048. This explicitly describes all 2-special groups of order at most 2048.

TABLE 2. Number of 2-special groups by order and 2-class.

$\log_2(\text{Order})$	1	2	3	4	5	6
3	0	1	0	0	0	0
6	0	0	1	0	0	0
8	0	0	1	0	0	0
9	0	0	0	2	0	0
10	0	0	0	2	0	0
11	0	0	0	2	1	0
12	0	0	0	0	4	2
13	0	0	0	0	4	0
14	0	0	0	0	4	0
15	0	0	0	0	0	10
16	0	0	0	0	0	7
17	0	0	0	0	6	28
19	0	0	0	0	0	72
20	0	0	0	0	0	30

Having seen that our narrow tower groups are 2-special, the following conjecture suggests itself. This takes care of part (a) of the Cohen-Lenstra methodology, namely identifying the right class of groups on which to place a distribution. In the next section we do likewise for wide tower groups.

Conjecture 4.7. *Every finite 2-special 2-group arises as the narrow tower group of some cyclic cubic field.*

In Section 7 we investigate this conjecture by using IPADs.

5. THE CLASS OF WIDE TOWER GROUPS

Recall that $G_2(K)$ is the quotient of $G_2^+(K)$ by complex conjugation, where we have to quotient by the normal subgroup generated by it and its images under the Δ -action. We therefore introduce the following terminology.

Definition 5.1. If G is a valid 2-group and $z \in G$ of order 1 or 2, then the quotient of G by the normal Δ -invariant subgroup generated by z will be called *viable*.

A viable quotient of a special group will be called *select*. A viable quotient of a k -special group is called k -select.

By Theorem 4.5, the wide tower group of a cyclic cubic field is 2-select.

By computing all the viable quotients of the groups in our list of 2-special groups, we find that 2-select groups are also relatively rare. The 2-select groups of order at most 512 (ordered by compact presentations) are precisely the 14 groups $\langle 4, 2 \rangle, \langle 8, 4 \rangle, \langle 32, 2 \rangle, \langle 64, 19 \rangle, \langle 128, 40 \rangle, \langle 256, 305 \rangle, \langle 256, 306 \rangle, \langle 256, 2 \rangle, \langle 256, 38 \rangle, \langle 256, 35 \rangle, \langle 256, 36 \rangle, \langle 512, 844 \rangle, \langle 512, 858 \rangle, \langle 512, 451 \rangle$.

Extending the reasoning of Theorem 4.2, there is a nice characterization of select groups along the lines of Theorem 4.2 (2).

Theorem 5.2. *A valid group G is select if and only if the Schur multiplier $M(G \rtimes \Delta)$ is of order 1 or 2.*

One unusual observation is that all the pairs of 2-special and 2-select groups obtained by taking all viable quotients of the 800 groups in our list of 2-special groups have elementary abelian kernel, except for one case, namely the quotient $\langle 32, 2 \rangle$ of N_{12} .

We can now carry out part (a) of the Cohen-Lenstra methodology for wide tower groups.

Conjecture 5.3. *Every finite 2-select 2-group arises as the wide tower group of some cyclic cubic field.*

We give evidence for this conjecture in Section 7. One fascinating observation is that there do exist, however, many pairs consisting of a 2-special group N and a 2-select group W where W is a viable quotient of the N for which (empirically) no cyclic cubic field K exists with $G_2^+(K) \cong N$ and $G_2(K) \cong W$.

6. PREVIOUS WORK ON FREQUENCIES

In this section we describe earlier work conjecturing how often the 2-class group of a cyclic cubic field is isomorphic to a given group. There appears to be no previous work on how often the narrow 2-class group is isomorphic to a given group.

Let V denote the abstract irreducible $\mathbb{F}_2[\mathbb{Z}/3]$ -module of dimension 2 (in other words, $[2, 2]$ with an automorphism of order 3 cyclically permuting its nontrivial elements). As noted earlier, as a Δ -module, $Cl_2(K)/Cl_2(K)^2$ is isomorphic to V^d for some non-negative integer d . We set $g = 2d$.

Malle [14] conjectured that $d = 1$ occurs for about 14.2% of cyclic cubic fields. He also conjectured that among such cases $Cl_2(K) \cong [2^n, 2^n]$ with frequency $15/16^n$. We will focus on the case $d = 1$ (and so $g = 2$) and suppose $G_2(K)^{ab} \cong [2^n, 2^n]$.

6.1. $n = 1$. Of the 3 valid children of $[2, 2]$, only $\langle 8, 4 \rangle$ has abelianization $[2, 2]$ and it has no descendants. It follows that in the case $n = 1$, $G_2(K)$ is either $[2, 2]$ or $\langle 8, 4 \rangle$. It is natural to ask how often each arises. Rubinstein-Salzedo [22] considered this question for K ramified at a single prime and found that, of 377529 such fields, 53.7% have $G_2(K) \cong [2, 2]$ whereas 46.3% have $G_2(K) \cong \langle 8, 4 \rangle$. We shall return to and give some reasoning for this disparity later.

6.2. **General n .** In [15], Malle conjectured that a given 2-torsion \mathfrak{D} -module H of even rank $2d$ should arise as $Cl_2(K)$ with frequency

$$2((2)_\infty(16)_\infty/(4)_\infty^2)2^{d^2}(4)_{d+1}/(|H|\text{Aut}_{\mathfrak{D}}(H))$$

where $\mathfrak{D} = \mathbb{Z}[\Delta]$ and $(q)_r = \prod_{i=1}^r (1 - q^{-i})$. For $d = 1$, this simplifies to $1.5995/(|H|\text{Aut}_{\mathfrak{D}}(H))$.

7. DATA

In this section, we present some data regarding the distribution of narrow and wide IPADs and discuss various conjectures. The data were obtained by starting from Malle's tables of cyclic cubic fields [16]. Ordering by discriminant, the first 500,000 fields K with 2-generated

2-class group were extracted. The wide and narrow 2-class groups of K along with various extensions of degree 2 and 4 were computed in order to determine the wide and narrow IPADs of K . The distribution (both an absolute count and the relative proportions) of the narrow and wide IPAD pairs that arose can be found in Tables 3 and 4. We have divided the collection of fields into three nested sets $I_1 \subseteq I_2 \subseteq I_3$. The first contains the first 100,000 fields, the second contains the first 200,000 fields and the third contains the full set of 500,000 fields. Most of the observed proportions seem fairly stable as the set of fields is enlarged.

The computations were implemented using PARI/GP [21], version 2.9.2 running on 2×2.66 GHz 6-Core Intel Xeon processors. The computations were run in parallel across multiple cores and took about 18,000 core hours. For some fields more than one attempt was required due to precision issues and the time spent on failed attempts is not included.

TABLE 3. Census of the most common extended IPADs.

Narrow	Wide	I_1	I_2	I_3
$[2, 2]; [4]; [2]$	$[2, 2]; [2]; []$	50500	101172	251883
$[2, 2]; [4]; [2]$	$[2, 2]; [4]; [2]$	25022	49829	124661
$[4, 4]; [2, 2, 4]; [2, 2, 4]$	$[2, 2]; [4]; [2]$	18006	36225	91413
$[4, 4]; [2, 4, 4]; [4, 4, 4]$	$[4, 4]; [2, 2, 4]; [2, 2, 2]$	1225	2411	6098
$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	$[4, 4]; [2, 2, 4]; [2, 2, 2]$	1220	2357	5894
$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	$[4, 4]; [2, 2, 4]; [2, 2, 4]$	586	1169	3018
$[8, 8]; [2, 4, 8]; [4, 4, 4]$	$[4, 4]; [2, 2, 4]; [2, 2, 4]$	578	1180	2982
$[4, 4]; [2, 2, 8]; [4, 4, 8]$	$[4, 4]; [2, 2, 4]; [2, 2, 4]$	625	1212	2967
$[4, 4]; [2, 4, 4]; [4, 4, 4]$	$[4, 4]; [2, 2, 4]; [2, 4, 4]$	415	826	2061
$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	$[4, 4]; [2, 2, 4]; [2, 2, 2, 2, 2]$	397	832	2050
$[8, 8]; [4, 4, 8]; [2, 2, 4, 4, 8]$	$[4, 4]; [2, 4, 4]; [4, 4, 4]$	196	395	1044
$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	187	416	983
$[8, 8]; [4, 4, 8]; [2, 2, 4, 4, 8]$	$[8, 8]; [2, 4, 8]; [4, 4, 4]$	140	234	590
$[8, 8]; [4, 4, 8]; [2, 2, 4, 4, 8]$	$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	116	232	570
$[8, 8]; [2, 4, 16]; [4, 8, 8]$	$[8, 8]; [2, 4, 8]; [4, 4, 4]$	79	157	379
$[4, 4]; [2, 2, 16]; [8, 8, 8]$	$[4, 4]; [2, 2, 8]; [4, 4, 4]$	76	149	372
$[8, 8]; [4, 8, 8]; [2, 2, 8, 8, 8]$	$[4, 4]; [2, 4, 4]; [4, 4, 4]$	74	145	352
$[8, 8]; [4, 4, 8]; [2, 2, 4, 4, 8]$	$[4, 4]; [2, 2, 8]; [4, 4, 4]$	63	117	340
$[8, 8]; [2, 8, 8]; [4, 8, 8]$	$[8, 8]; [2, 4, 8]; [4, 4, 4]$	42	87	213
$[8, 8]; [4, 4, 8]; [2, 2, 4, 4, 8]$	$[4, 4]; [2, 2, 8]; [4, 4, 8]$	41	81	212
Other IPADs (73 types)		412	774	1918
Total		100000	200000	500000

In Table 5, for the most common pairs of narrow/wide IPADs, with the help of Table 1, we infer what the corresponding narrow tower group and wide tower group must be. The last column gives a guess (based on the observed frequency) for the proportion of cyclic cubic fields that have those narrow and wide IPADs.

Note that this proves Conjecture 4.7 for N_k for $k = 1, 2, 3, 4, 5$ and Conjecture 5.3 for the first five 2-select groups. The 16th, 19th, and 20th rows of Table 3 show that $\langle 256, 38 \rangle$, $\langle 512, 451 \rangle$, and $\langle 512, 858 \rangle$ respectively satisfy Conjecture 5.3.

We can also ask which viable quotients of N_k arise as wide tower groups. For N_1 both do, but for N_2 , whereas both $\langle 64, 19 \rangle$ and $\langle 32, 2 \rangle$ are viable quotients, their IPADs have not been seen for any cyclic cubic field as the wide IPAD paired with the narrow IPAD of N_2 . We therefore believe that if the narrow group is N_2 (i.e., $\langle 64, 19 \rangle$), then the wide group must

TABLE 4. Relative proportions of the most common extended IPADs.

Narrow	Wide	I_1	I_2	I_3
$[2, 2]; [4]; [2]$	$[2, 2]; [2]; []$	0.5050	0.5059	0.5038
$[2, 2]; [4]; [2]$	$[2, 2]; [4]; [2]$	0.2502	0.2491	0.2493
$[4, 4]; [2, 2, 4]; [2, 2, 4]$	$[2, 2]; [4]; [2]$	0.1801	0.1811	0.1828
$[4, 4]; [2, 4, 4]; [4, 4, 4]$	$[4, 4]; [2, 2, 4]; [2, 2, 2]$	0.0123	0.0121	0.0122
$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	$[4, 4]; [2, 2, 4]; [2, 2, 2]$	0.0122	0.0118	0.0118
$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	$[4, 4]; [2, 2, 4]; [2, 2, 4]$	0.0059	0.0058	0.0060
$[8, 8]; [2, 4, 8]; [4, 4, 4]$	$[4, 4]; [2, 2, 4]; [2, 2, 4]$	0.0058	0.0059	0.0060
$[4, 4]; [2, 2, 8]; [4, 4, 8]$	$[4, 4]; [2, 2, 4]; [2, 2, 4]$	0.0063	0.0061	0.0059
$[4, 4]; [2, 4, 4]; [4, 4, 4]$	$[4, 4]; [2, 2, 4]; [2, 4, 4]$	0.0042	0.0041	0.0041
$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	$[4, 4]; [2, 2, 4]; [2, 2, 2, 2, 2]$	0.0040	0.0042	0.0041
$[8, 8]; [4, 4, 8]; [2, 2, 4, 4, 8]$	$[4, 4]; [2, 4, 4]; [4, 4, 4]$	0.0020	0.0020	0.0021
$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	0.0019	0.0021	0.0020
$[8, 8]; [4, 4, 8]; [2, 2, 4, 4, 8]$	$[8, 8]; [2, 4, 8]; [4, 4, 4]$	0.0014	0.0012	0.0012
$[8, 8]; [4, 4, 8]; [2, 2, 4, 4, 8]$	$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	0.0012	0.0012	0.0011
$[8, 8]; [2, 4, 16]; [4, 8, 8]$	$[8, 8]; [2, 4, 8]; [4, 4, 4]$	0.0008	0.0008	0.0008
$[4, 4]; [2, 2, 16]; [8, 8, 8]$	$[4, 4]; [2, 2, 8]; [4, 4, 4]$	0.0008	0.0007	0.0007
$[8, 8]; [4, 8, 8]; [2, 2, 8, 8, 8]$	$[4, 4]; [2, 4, 4]; [4, 4, 4]$	0.0007	0.0007	0.0007
$[8, 8]; [4, 4, 8]; [2, 2, 4, 4, 8]$	$[4, 4]; [2, 2, 8]; [4, 4, 4]$	0.0006	0.0006	0.0007
$[8, 8]; [2, 8, 8]; [4, 8, 8]$	$[8, 8]; [2, 4, 8]; [4, 4, 4]$	0.0004	0.0004	0.0004
$[8, 8]; [4, 4, 8]; [2, 2, 4, 4, 8]$	$[4, 4]; [2, 2, 8]; [4, 4, 8]$	0.0004	0.0004	0.0004
Other IPADs (73 types)		0.0041	0.0039	0.0038

TABLE 5. Explanation and conjectural frequency of IPAD pairs.

Narrow	Wide	Explanation	Obs freq	Conj freq
$[2, 2]; [4]; [2]$	$[2, 2]; [2]; []$	$N_1 \rightarrow \langle 4, 2 \rangle$	0.5038	1/2
$[2, 2]; [4]; [2]$	$[2, 2]; [4]; [2]$	$N_1 \rightarrow \langle 8, 4 \rangle$	0.2493	1/4
$[4, 4]; [2, 2, 4]; [2, 2, 4]$	$[2, 2]; [4]; [2]$	$N_2 \rightarrow \langle 8, 4 \rangle$	0.1828	3/16
$[4, 4]; [2, 4, 4]; [4, 4, 4]$	$[4, 4]; [2, 2, 4]; [2, 2, 2]$	$N_3 \rightarrow \langle 32, 2 \rangle$	0.0122	3/256
$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	$[4, 4]; [2, 2, 4]; [2, 2, 2]$	7.2 below	0.0118	3/256
$[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]$	$[4, 4]; [2, 2, 4]; [2, 2, 4]$	7.3 below	0.0060	3/512
$[8, 8]; [2, 4, 8]; [4, 4, 4]$	$[4, 4]; [2, 2, 4]; [2, 2, 4]$	$N_5 \rightarrow \langle 64, 19 \rangle$	0.0060	3/512
$[4, 4]; [2, 2, 8]; [4, 4, 8]$	$[4, 4]; [2, 2, 4]; [2, 2, 4]$	$N_4 \rightarrow \langle 64, 19 \rangle$	0.0059	3/512
$[4, 4]; [2, 4, 4]; [4, 4, 4]$	$[4, 4]; [2, 2, 4]; [2, 4, 4]$	N_3 or N_6 or $N_7 \rightarrow \langle 128, 40 \rangle$	0.0041	1/256

be $\langle 8, 4 \rangle$. With the same reasoning we make the following conjecture. The only slightly different case is (2), since N_3 has both $\langle 128, 40 \rangle$ and $\langle 32, 2 \rangle$ as viable quotients with fields existing with the corresponding pair of narrow/wide IPADs. If, however, we check the first 6 such fields K with wide tower group $\langle 128, 40 \rangle$, by looking at the narrow 2-class group of a certain octic extension of K , we see that the narrow tower group is not N_3 (so is N_6 or N_7).

Conjecture 7.1. (1) If a cyclic cubic field has narrow tower group $N_2 = \langle 64, 19 \rangle$, then its wide tower group is $\langle 8, 4 \rangle$.

(2) If a cyclic cubic field has narrow tower group $N_3 = \langle 256, 36 \rangle$, then its wide tower group is $\langle 32, 2 \rangle$.

(3) If a cyclic cubic field has narrow tower group N_4 , then its wide tower group is $\langle 64, 19 \rangle$.

(4) If a cyclic cubic field has narrow tower group N_5 , then its wide tower group is $\langle 64, 19 \rangle$.

- (5) If a cyclic cubic field has narrow tower group N_6 , then its wide tower group is $\langle 128, 40 \rangle$.
(6) If a cyclic cubic field has narrow tower group N_7 , then its wide tower group is $\langle 128, 40 \rangle$.

Remark 7.2. Consider the 5th row in Table 5. The wide tower group is $\langle 32, 2 \rangle$. Of the 800 2-special groups, only N_8 and N_{12} have this narrow IPAD and a viable quotient isomorphic to $\langle 32, 2 \rangle$. We can distinguish between these two cases by computing narrow class groups of certain octic extensions of K . We did this for 6 fields with this pair of IPADs and in each case the narrow tower group turned out not to be N_8 . We also found some larger 2-special groups, of 2-class 7 and order 2^{20} , with this IPAD and a viable quotient isomorphic to $\langle 32, 2 \rangle$.

Remark 7.3. Consider the 6th row in Table 5. The wide tower group is $\langle 64, 19 \rangle$. Of the 800 2-special groups, only N_8 has this narrow IPAD and a viable quotient isomorphic to $\langle 64, 19 \rangle$. We do not know whether there exist larger 2-special groups with this property.

Remark 7.4. Let G be a 2-select group. It is fundamental to ask which 2-special groups have G as a viable quotient. The above remarks consider this briefly for $G = \langle 32, 2 \rangle$ and $\langle 64, 19 \rangle$ respectively. The last section of this paper indicates that if G is a certain group of order 2048, then it is a viable quotient of some infinite 2-special group. Extensive investigations suggest that $\langle 4, 2 \rangle$ is a viable quotient of only N_1 and that $\langle 8, 4 \rangle$ is a viable quotient of only N_1 and N_2 . We do not know whether every 2-select group is a viable quotient of only finitely many 2-special groups. This will be key in understanding the joint distribution we seek.

In some cases it is very clear how often a certain 2-special 2-group arises as $G_2^+(K)$ as K varies. For instance, for $\langle 8, 4 \rangle$, the frequency is almost exactly $3/4$, whereas for $\langle 64, 19 \rangle$ the frequency is almost exactly $3/16$. What is perhaps surprising is that the frequencies do not match the proportion of pairs of pairs yielding a given 2-special group by the method of Theorem 4.2 (3).

Ideally, we would like a formula for the proportion of fields with a given narrow 2-class tower group N and given wide 2-class tower group W , in terms of N and W , but since we have yet to understand which pairs (N, W) arise, even a conjectural formula is currently out of reach. We can, however, use the data to make some related conjectures regarding proportions of fields.

7.1. Proportion for narrow 2-class 3 quotients. More detailed analysis allows us to make reliable conjectures as to the frequencies with which $Q_3(G_2^+(K))$ arises as K varies.

Lemma 7.5. *Among 2-special groups G , the form of $\text{IPAD}(G)$ determines $Q_3(G)$. In particular, with the help of Table 1,*

- (1) if $\text{IPAD}(G) = [[2, 2]; [4]; [2]]$, then $Q_3(G) = \langle 8, 4 \rangle$;
- (2) if $\text{IPAD}(G) = [[4, 4]; [2, 2, 4]; [2, 2, 4]]$, then $Q_3(G) = \langle 64, 19 \rangle$;
- (3) if $\text{IPAD}(G) = [[*, *]; [-, -, -]; [-, -, -]]$, then $Q_3(G) = \langle 256, 2 \rangle$;
- (4) if $\text{IPAD}(G) = [[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]]$, then $Q_3(G) = \langle 256, 35 \rangle$;
- (5) if $\text{IPAD}(G) = [[4, 4]; [2, 4, 4]; [4, 4, 4]]$, then $Q_3(G) = \langle 256, 36 \rangle$;
- (6) if $\text{IPAD}(G) = [[4, 4]; [-, -, -]; [-, -, -]]$, other than above, then $Q_3(G) = \langle 256, 38 \rangle$;
- (7) if $\text{IPAD}(G) = [[*, *]; [-, -, -]; [-, -, -, -, -]]$, then $Q_3(G) = Q_3(F)$ of order 1024.

Here $*$ stands for an integer ≥ 8 and $-$ stands for an integer ≥ 2 .

Using this and our data on occurrence of IPADs, we obtain the following conjectural frequencies for $Q_3(G_2^+(K))$ given in Table 6.

TABLE 6. Conjectural frequency for $Q_3(G_2^+(K))$.

Group	Obs freq	Conj freq
$\langle 8, 4 \rangle$	0.7531	3/4
$\langle 64, 19 \rangle$	0.1828	3/16
$\langle 256, 2 \rangle$	0.0080	1/128
$\langle 256, 35 \rangle$	0.0239	3/128
$\langle 256, 36 \rangle$	0.0163	1/64
$\langle 256, 38 \rangle$	0.0079	1/128
$Q_3(F)$	0.0079	1/128

It is a mystery as to why such similar groups as $\langle 256, 35 \rangle$ and $\langle 256, 38 \rangle$ do not arise equally often.

7.2. Proportion for wide 2-class 3 quotients. Likewise, we can make reliable conjectures as to the frequencies with which $Q_3(G_2(K))$ arises as K varies.

Lemma 7.6. *Among 2-select groups, the form of $IPAD(G)$ determines $Q_3(G)$. In particular, with the help of Table 1,*

- (1) if $IPAD(G) = [[2, 2]; [2]; []]$, then $Q_3(G) = \langle 4, 2 \rangle$;
 - (2) if $IPAD(G) = [[2, 2]; [4]; [2]]$, then $Q_3(G) = \langle 8, 4 \rangle$;
 - (3) if $IPAD(G) = [[4, 4]; [2, 2, 4]; [2, 2, 2]]$, then $Q_3(G) = \langle 32, 2 \rangle$;
 - (4) if $IPAD(G) = [[4, 4]; [2, 2, 4]; [2, 2, 4]]$, then $Q_3(G) = \langle 64, 19 \rangle$;
 - (5) if $IPAD(G) = [[4, 4]; [2, 2, 4]; [2, 2, 2, 2, 2]]$, then $Q_3(G) = \langle 128, 36 \rangle$;
 - (6) if $IPAD(G) = [[4, 4]; [2, 2, 4]; [2, 4, 4]]$, then $Q_3(G) = \langle 128, 40 \rangle$;
 - (7) if $IPAD(G) = [[*, *]; [-, -, -]; [-, -, -]]$, then $Q_3(G) = \langle 256, 2 \rangle$;
 - (8) if $IPAD(G) = [[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]]$, then $Q_3(G) = \langle 256, 35 \rangle$;
 - (9) if $IPAD(G) = [[4, 4]; [2, 4, 4]; [4, 4, 4]]$, then $Q_3(G) = \langle 256, 36 \rangle$;
 - (10) if $IPAD(G) = [[4, 4]; [-, -, -]; [-, -, -]]$, other than above, then $Q_3(G) = \langle 256, 38 \rangle$;
 - (11) if $IPAD(G) = [[*, *]; [-, -, -]; [-, -, -, -, -]]$, then $Q_3(G) = Q_3(F)$ of order 1024.
- Here $*$ stands for an integer ≥ 8 and $-$ stands for an integer ≥ 2 .

TABLE 7. Conjectural frequency for $Q_3(G_2(K))$.

Group	Obs freq	Conj freq
$\langle 4, 2 \rangle$	0.5038	1/2
$\langle 8, 4 \rangle$	0.4321	7/16
$\langle 32, 2 \rangle$	0.0240	3/128
$\langle 64, 19 \rangle$	0.0179	9/512
$\langle 128, 36 \rangle$	0.0041	1/256
$\langle 128, 40 \rangle$	0.0041	1/256
$\langle 256, 2 \rangle$	0.0036	7/2048
$\langle 256, 35 \rangle$	0.0034	7/2048
$\langle 256, 36 \rangle$	0.0028	3/1024
$\langle 256, 38 \rangle$	0.0035	7/2048
$Q_3(F)$	0.0006	1/2048

7.3. Joint distribution for narrow/wide 2-class 3 quotients. Since we actually compute how often various narrow and wide IPAD pairs occur together, we can refine the computations of the last two subsections to give a conjectural joint distribution on the 77 possibilities given by Lemmas 7.4 and 7.5. Summing its columns and rows gives the marginal distributions given in Tables 6 and 7. A key step in guessing the joint distribution for the narrow and wide tower groups would be to understand Table 8.

TABLE 8. Conjectural joint distribution for $(Q_3(G_2(K)), Q_3(G_2^+(K)))$.

Narrow	$\langle 8, 4 \rangle$	$\langle 64, 19 \rangle$	$\langle 256, 2 \rangle$	$\langle 256, 35 \rangle$	$\langle 256, 36 \rangle$	$\langle 256, 38 \rangle$	$Q_3(F)$
Wide							
$\langle 4, 2 \rangle$	1/2	0	0	0	0	0	0
$\langle 8, 4 \rangle$	1/4	3/16	0	0	0	0	0
$\langle 32, 2 \rangle$	0	0	0	3/256	3/256	0	0
$\langle 64, 19 \rangle$	0	0	3/512	3/512	0	3/512	0
$\langle 128, 36 \rangle$	0	0	0	1/256	0	0	0
$\langle 128, 40 \rangle$	0	0	0	0	1/256	0	0
$\langle 256, 2 \rangle$	0	0	1/512	0	0	0	3/2048
$\langle 256, 35 \rangle$	0	0	0	1/512	0	0	3/2048
$\langle 256, 36 \rangle$	0	0	0	0	0	0	3/1024
$\langle 256, 38 \rangle$	0	0	0	0	0	1/512	3/2048
$Q_3(F)$	0	0	0	0	0	0	1/2048

7.4. Narrow/wide 2-class group pairs. As noted in Lemma 2.1, the number of generators of the wide and narrow 2-class groups are the same. It is, however, possible for the 2-class groups not to be isomorphic, although the difference cannot be large. In fact the ratio of their orders is always 1 or 4.

This follows from the exact sequence

$$1 \rightarrow (\pm 1)^3 / \text{sgn}_\infty(O_K^*) \rightarrow Cl_2^+(K) \rightarrow Cl_2(K) \rightarrow 1$$

[6] and the fact that the orders of $Cl_2^+(K)$ and $Cl_2(K)$ are both squares.

TABLE 9. Conjectural frequency for narrow/wide 2-class group pairs.

Narrow	Wide	Obs freq	Conj freq
$[2, 2]$	$[2, 2]$	0.7531	3/4
$[4, 4]$	$[2, 2]$	0.1828	3/16
$[4, 4]$	$[4, 4]$	0.0481	3/64
$[8, 8]$	$[4, 4]$	0.0118	3/256
$[8, 8]$	$[8, 8]$	0.0032	3/1024
$[16, 16]$	$[8, 8]$	0.0007	3/4096
$[16, 16]$	$[16, 16]$	0.0002	3/16384
...	...		

Conjecture 7.7. *Among cyclic cubic fields K with 2-generator 2-class group, following Table 9, we conjecture that $Cl_2^+(K) \cong [2^n, 2^n] \cong Cl_2(K)$ for a proportion $3/2^{4n-2}$ of fields and that $Cl_2^+(K) \cong [2^{n+1}, 2^{n+1}]$ and $Cl_2(K) \cong [2^n, 2^n]$ for a proportion $3/2^{4n}$ of fields.*

Note that this is consistent with Malle's heuristics (Section 6) since $3/2^{4n-2} + 3/2^{4n} = 15/16^n$. It is also consistent with Conjecture 6.2.3 of [6] since each predicts that the narrow and wide 2-class groups should agree 4/5 of the time.

Looking at these data closer, when $Cl_2^+(K) \cong [2, 2]$ and $Cl_2(K) \cong [2, 2]$, we know that $G_2^+(K) \cong \langle 8, 4 \rangle$ and $G_2(K) \cong \langle 8, 4 \rangle$ or $[2, 2]$. From the first two lines of Table 4, the first possibility empirically occurs half as often as the second (so of the 3/4, the first accounts for 1/2 and the second for 1/4). When $Cl_2^+(K) \cong [4, 4]$ and $Cl_2(K) \cong [2, 2]$, the third line of Table 5 actually indicates that $G_2^+(K) \cong \langle 64, 19 \rangle$ and $G_2(K) \cong \langle 8, 4 \rangle$.

Combining these, then, as K varies, $G_2(K) \cong [2, 2]$ for 1/2 of the time whereas $G_2(K) \cong \langle 8, 4 \rangle$ for $1/4 + 3/16 = 7/16$ of the time. This matches Rubinstein-Salzedo's [22] observations well, since $8/15$ is close to 53.7%. We do, however, still make the following conjecture.

Conjecture 7.8. *Precisely one half of unramified $[2, 2]$ -extensions of cyclic cubic fields extend to unramified $\langle 8, 4 \rangle$ -extensions.*

How do we reconcile this with the Rubinstein-Salzedo observation? The point is that the other cases with $g = 2$ (where $G_2(K)^{ab}$ is $[4, 4]$ or $[8, 8]$ or ...) necessarily have $G_2(K)$ being a descendant of $Q_2(F)$ (see the earlier discussion of the $g = 2$ O'Brien tree, as in Figure 1). It therefore has $\langle 8, 4 \rangle$ as a quotient. It follows that all these other cases, accounting for 1/16 of all cases, give rise to an unramified $\langle 8, 4 \rangle$ -extension, and so there are overall $7/16 + 1/16 = 1/2$ such cases!

8. SPECULATION ON INFINITE NARROW CLASS TOWERS

There is no explicit example known of a Galois group of an infinite p -extension of a number field, ramified at only finitely many primes, not including any primes above p . There has, however, been plenty of speculation as to what kind of pro- p group this Galois group can or cannot be [3]. The goal of this section is to see whether our theory sheds any light on this matter.

Suppose that a cyclic cubic field K has an infinite narrow 2-class tower. Since every g -generator $(g + 2)$ -relator pro- p group is infinite if $g \geq 6$ by Golod-Shafarevich, our method below provides little useful information for large g . The simplest situation to consider is where $G_2^+(K)$ is a 2-generator, so 4-relator, pro-2 group. Note that we do not know of any such K with infinite narrow 2-class tower, but on the other hand we do not know one does not exist.

What can we say then about $G_2^+(K)$, if such a K does exist? By class field theory every open subgroup has finite abelianization (sometimes called the FAb property). Indeed, the Fontaine-Mazur conjecture [8] applies to say that $G_2^+(K)$ should have no 2-adic representations with infinite image.

Also, we might suspect that $G_2^+(K)$ is a 2-special pro-2 group, using the obvious extension of Definition 4.4 to infinite groups. This allows us to carry out the experiment whereby we choose u_1, u_2 from $\Phi(F)$ and consider the 2-special group $G := \langle x, y \mid v_1, \sigma(v_1), v_2, \sigma(v_2) \rangle$, where $v_i = u_i^{-1} \sigma(u_i)$. Choosing random words (of some bounded length) in $\Phi(F)$ a million times, we put the corresponding G through two filters.

The first filter checks that the order of $Q_c(G)$ continues to grow as c increases. We check this at least up to $c = 32$. The second filter checks that subgroups of G of small index have finite abelianization. In practice, Magma allows us to check this for subgroups of index

1, 2, 4, 8, 16 (with cores of 2-power index so they do arise in the pro-2 group given by the presentation).

While these are not complete checks that G is infinite and FAb, they do filter out most presentations. We find that the following two types of groups are left. We study them via the sequence $\log_2 |Q_c(G)|$. The groups G all have IPAD $[[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]]$.

A typical sequence for the first type of group is 2, 5, 8, 11, 15, 18, 23, 28, 30, 33, 36, 38, 41, 44, 46, 49, 52, 54, 57, 60, 62, 65, 68, 70, 73, 76, 78, 81, 84, 86, 89, 92, It is characterized by ultimate periodicity in the differences, which is a strong indication that G is indeed infinite. It is, however, also an indication that the group may be 2-adic analytic, which would be forbidden by Fontaine-Mazur. One can also compute abelianizations of normal subgroups of index at least up to 4096 and see that their ranks are apparently bounded, indicating finite Prüfer rank. The pro-2 groups of finite Prüfer rank are exactly the 2-adic analytic ones.

Apparently, then, the only surviving type of group is the second, whose sequence is 2, 5, 8, 11, 14, 16, 20, 24, 28, 31, 35, 39, 45, 53, 60, 65, 71, 78, 88, 99, 109, 119, 131, 146, 162, 178, 192, 206, 224, 247, 269, 293, ... or similar. We do not have an exact description of this sequence. One example is for $u_1 = (y^{-1}, x^{-1})^2$, $u_2 = (yx^{-1}y^{-1}x^{-1})^2$. An element of order 2 here is, for example, $(x^2y^{-2})^2$. The corresponding viable quotients have IPAD $[[4, 4]; [2, 2, 8]; [2, 2, 2, 2, 4]]$, but what is most interesting about them is that they are finite, in fact isomorphic to a certain 2-select group of 2-class 5 and order 2^{11} . Whatever element of order 2 is used appears to lead to the same group.

ACKNOWLEDGEMENTS. We thank Brandon Alberts, Jordan Ellenberg, Farshid Hajir, Yuan Liu, John Voight, Jiuya Wang, and Melanie Matchett Wood for helpful conversations and feedback. The work of MRB was partially supported by summer Lenfest Grants from Washington and Lee University.

REFERENCES

- [1] J. V. Armitage, A. Fröhlich, *Class numbers and unit signatures*, Mathematika **14** (1967), 94–98.
- [2] W. Bosma, J. J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., **24** (1997), 235–265.
- [3] N. Boston, *Galois groups of tamely ramified p -extensions*, J. Théorie des Nombres de Bordeaux, **19** (2007), no. 1, 59–70.
- [4] N. Boston, M.R. Bush, F. Hajir, *Heuristics for p -class towers of imaginary quadratic fields*, Math. Ann. **368** (2017), no. 1–2, 633–669.
- [5] N. Boston, M.R. Bush, F. Hajir, *Heuristics for p -class towers of real quadratic fields*, Jour. Inst. Math. Jussieu, (2019), 1–24.
- [6] B. Breen, I. Varma, J. Voight, *On unit signatures and narrow class groups of odd abelian number fields: structure and heuristics*, <https://arxiv.org/abs/1910.00449>, preprint, 2019.
- [7] H. Cohen, H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, pp. 33–62 in: Number theory, Noordwijkerhout 1983, LNM **1068**, Springer, Berlin, 1984.
- [8] J.-M. Fontaine, B. Mazur, *Geometric Galois representations*, in Coates, John; Yau, S.-T. (eds.), Elliptic curves, modular forms, & Fermat’s last theorem (Hong Kong, 1993), Series in Number Theory, 1, Int. Press, Cambridge, MA, pp. 41–78.
- [9] A. Fröhlich, *Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields*, Contemp. Math., **24**, (1983), Amer. Math. Soc, Providence.
- [10] D. Garton, *Random matrices, the Cohen-Lenstra heuristics, and roots of unity*, Algebra & Number Theory, **9** (2015), 149–171.

- [11] J. Klys, *The distribution of p -torsion in degree p cyclic fields*, Algebra & Number Theory, **14** (2020), 815–854.
- [12] H. Koch, “Galois theory of p -extensions.” With a foreword by I. R. Shafarevich. Translated from the 1970 German original by Franz Lemmermeyer. With a postscript by the author and Lemmermeyer. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002.
- [13] Y. Liu, M. Matchett Wood, D. Zureick-Brown, *A predicted distribution for Galois groups of maximal unramified extensions*, <https://arxiv.org/abs/1907.05002>, preprint, 2019.
- [14] G. Malle, *Cohen-Lenstra heuristic and roots of unity*, J. Number Theory **128** (2008), 2823–2835.
- [15] G. Malle, *On the distribution of class groups of number fields*, Experimental Math **19**(4) (2010), 465–474.
- [16] G. Malle, Tables of cyclic cubic extensions K/\mathbb{Q} with $|d_K| < 10^{16}$: https://service.mathematik.uni-kl.de/~numberfieldtables/KT_3/download.html.
- [17] G. Malle, M. Adam *A class group heuristic based on the distribution of 1-eigenspaces in matrix groups*, J. Number Theory **149** (2015), 225–235.
- [18] D.C. Mayer, M. Ayadi, A. Derhem, *p -class field towers of cyclic cubic fields*, preprint, 2018.
- [19] E.A. O’Brien, *The p -group generation algorithm*, J. Symbolic Comput. **9** (1990), 677–698.
- [20] E.A. O’Brien, *Isomorphism testing for p -groups*, J. Symbolic Comput. **17** (1994), 133–147.
- [21] The PARI Group, PARI/GP version 2.9.2, Bordeaux, 2017, <http://pari.math.u-bordeaux.fr/>.
- [22] S. Rubinstein-Salzedo, *Invariants for A_4 fields and the Cohen–Lenstra heuristics*, International J. Number Theory **10**(5) (2014), 1259–1276.
- [23] J.-P. Serre, *Topics in Galois Theory*, Taylor & Francis (2008).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN - MADISON, 480 LINCOLN DRIVE, MADISON, WI 53706, USA

Email address: `boston@math.wisc.edu`

DEPARTMENT OF MATHEMATICS, WASHINGTON AND LEE UNIVERSITY, LEXINGTON, VIRGINIA 24450, USA

Email address: `bushm@wlu.edu`