DISTRIBUTIONS OF CLASS GROUPS OF GLOBAL FIELDS NOTES

AARON LANDESMAN

1. INTRODUCTION

Melanie Wood taught a course on distributions of class groups of global fields online in Fall 2020.

These are my "live-TeXed" notes from the course. Conventions are as follows: Each lecture gets its own "chapter," and appears in the table of contents with the date.

Of course, these notes are not a faithful representation of the course, either in the mathematics itself or in the quotes, jokes, and philosophical musings; in particular, the errors are my fault. By the same token, any virtues in the notes are to be credited to the lecturer and not the scribe. Please email suggestions to aaronlandesman@gmail.com.

2. 9/4/20

We begin with some motivation and questions about class groups.

Theorem 2.1 (Heilbronn)**.** *For K an imaginary quadratic field,* $\operatorname{disc} K \to \infty, |\operatorname{Cl}_K| \to \infty$.

Theorem 2.2 (Heegner, Baker, Stark, 1952-1967)**.** *If $d < 0$ then*

$$\operatorname{Cl}_{\mathbb{Q}(\sqrt{-d})} = 1 \iff d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Later, Watkins computed all imaginary quadratic fields with class group of size at most 100.

Theorem 2.3 (Littlewood)**.** *Assuming the generalized Riemann hypothesis (GRH), there is a constant $c > 0$ so that*

$$\operatorname{Cl}_K \geq \frac{c\,|\operatorname{disc}_K|^{1/2}}{\log\log|\operatorname{disc}_K|}.$$

Question 2.4. Can we give an upper bound on the class number in terms of the discriminant?

The answer is yes, and in fact $|\operatorname{Cl}_K| = O(\Delta^{1/2})$. This can be deduced from the Minkowski bound.

Conjecture 2.5 (Gauss)**.** There are infinitely many real quadratic fields with class number 1.

Arithmetic statistics is an emerging field of mathematics asking questions like the following:

Question 2.6. How is Cl_K distributed as K ranges over a certain family of fields?

Remark 2.7. There are several issues with this question. For one, there is not a great measure to define the distribution because we typically work with infinite families of fields. One often gets around this by ordering the fields K in your family by some invariant, such as the discriminant, and then taking the uniform measure on the first N fields and letting $N \to \infty$. For this sequences of measures, one can also ask if they converge to a measure. However, there is another problem with this in general: it is possible for mass to escape, and so they may converge to the 0 measure, which is not a probability distribution.

Fortunately, mass can only escape, it cannot be added, as follows from Fatou's lemma.

Now, let $\mathscr{F}$ be a family of number fields, ordered by discriminant. Let A be a finite abelian group.

Question 2.8. Does the limit

$$\lim_{X\to\infty} \frac{\#\{K \in \mathscr{F} : \mathrm{Cl}_K \simeq A, \mathrm{disc}\, K \leq X\}}{\#\{K \in \mathscr{F} : \mathrm{disc}\, K \leq X\}}$$

exist?

In nearly all cases, this is an open question. Here are is one case where we know the answer:

Example 2.9. Let $\mathscr{F}$ be the set of isomorphism classes of imaginary quadratic fields. Then the limit of Question 2.8 exists and is 0.

Here is a variant:

Question 2.10. What about when we take $\mathscr{F}$ to be isomorphism classes of real quadratic fields. Then, for A an abelian 2-group, does the limit

$$\lim_{X\to\infty} \frac{\#\{K \in \mathscr{F} : \mathrm{Cl}_K[2] \simeq A, \mathrm{disc}\, K \leq X\}}{\#\{K \in \mathscr{F} : \mathrm{disc}\, K \leq X\}}$$

exist?

Again, here it does exist and the limit is 0. This follows from the fact that $\mathrm{Cl}_K[2] \simeq (\mathbb{Z}/2\mathbb{Z})^{\text{number of ramified primes}}$. So, when $\mathrm{Cl}_K[2]$ is small, there are

very few such quadratic fields of discriminant up to X, since we know the density of primes up to X.

Remark 2.11. In order to ask more refined questions, for f a function our given family $\mathscr{F}$ to the real numbers, we will often ask about the following limit:

$$\lim \frac{\sum_{K\in\mathscr{F},\operatorname{disc} K\leq X} f(K)}{\#\{K\in\mathscr{F} : \operatorname{disc} K\leq X\}} = \lim_{X\to\infty}\int_{\mathscr{F}} f(K)d\mu_X = \lim_{X\to\infty}\mathbb{E}_{\mu_X}(f(K)).$$

Here μ_X is the uniform measure on $\mathscr{F}$ for fields of discriminant at most X.

Here are some examples of functions f we can take above. We will often take functions of abelian groups, and the compose with the function from $\mathscr{F}$ to abelian groups sending K to its class group.

Example 2.12.
(1) $f(B) = 1_{B^{\text{odd}}\simeq A}(B)$, the indicator function that the odd part of the abelian group B is isomorphic to A. We often do this for quadratic fields to get around dealing with issues coming from genus theory, i.e., the 2 parts of class groups being very predictable.
(2) $f(B) = 1_{B/B[2]\simeq A}(B)$.
(3) $f(B) = 1_{\text{rk}_p(B)\simeq r}(B)$
(4) $f(B) = 1_{B[p^\infty]\simeq A}(B)$
(5) $f(B) = \#\text{Hom}(B, A)$
(6) $f(B) = \#\text{Surj}(B, A)$
(7) $f(B) = \mathbb{E}\,\text{Surj}(B, A)$. This gives the moments of the distribution and plays the role of $\mathbb{E}(X^k)$, the kth moment of a random variable.

Remark 2.13. It is expected that about 75% of real quadratic fields with prime discriminant have class number 1, but we do not even know if there are infinitely many. Conjectures suggest there exist finite abelian groups that don't appear as class groups of imaginary quadratic fields, though for real quadratic fields, all finite abelian groups are expected to appear as class groups.

3. 9/9/20

Today, we'll begin by introducing the Cohen-Lenstra conjecture on class groups of quadratic fields K.

We'll begin with the case that K is an imaginary quadratic field.

Definition 3.1. Let $\mathscr{I}_X$ denote the set of isomorphism classes of imaginary quadratic fields K with $|\operatorname{disc} K| \leq X$.

Let $\text{Cl}_K^{\text{odd}} := \text{Cl}_K / \text{Cl}_K[2^\infty]$, the odd part of the class group.

Conjecture 3.2 (Cohen-Lenstra, 1984)**.** For a "reasonable" function f from odd order finite abelian groups to $\mathbb{R}$, we have

$$\lim_{X\to\infty} \frac{\sum_{K\in\mathscr{I}_X} f(\mathrm{Cl}_K^{\mathrm{odd}})}{\sum_{K\in\mathscr{I}_X} 1} = \lim_{Y\to\infty} \frac{\sum_{G,|G|\leq Y} \frac{1}{|\operatorname{Aut}(G)|} f(G)}{\sum_{G,|G|\leq Y} \frac{1}{|\operatorname{Aut}(G)|}}$$

where G ranges over odd order finite abelian groups.

Remark 3.3. The precise notion of reasonable was not specified. Cohen and Lenstra thought every positive function was reasonable, though it turns out there are some unreasonable positive functions.

We saw some examples of reasonable functions last time. Here are some more.

Example 3.4. (1) $f = 1_{\text{cyclic}}$ the indicator function that your abelian group is cyclic
(2) $f = 1_{\text{squarefree order}}$

Notation 3.5. We will write μ_X for the uniform measure on $\mathscr{I}_X$. We will write ν_Y for the probability measure on odd order abelian groups of size at most Y which is proportional to $\frac{1}{|\operatorname{Aut}(G)|}$.

We can re-express Cohen-Lenstra's conjecture (3.2) as follows

Conjecture 3.6. We have

$$\lim_{X\to\infty} \mathbb{E}_{\mu_X}(f(\mathrm{Cl}_K^{\mathrm{odd}})) = \lim_{Y\to\infty} E_{\nu_Y}(f(G)).$$

As we mentioned, one annoyance is that

$$\sum_{G \text{ odd order finite abelian groups}} \frac{1}{|Aut(G)|} = \infty.$$

This can already be seen by just considering cyclic groups and noting that $\mathbb{Z}/p\mathbb{Z}$ has $p-1$ automorphisms.

3.1. **Motivations for counting inversely proportional to the automorphisms.**

Question 3.7. What is up with the $\frac{1}{|\operatorname{Aut}(G)|}$ factor?

A useful motto throughout mathematics is that objects appear with frequency inversely proportional to their automorphisms.

Example 3.8. Consider degree three field extensions. Cyclic fields appear once as a subfield of $\overline{\mathbb{Q}}$ and have three automorphisms. On the other hand, non-Galois cubic fields appear three times in $\overline{\mathbb{Q}}$ and have only 1 automorphism.

Example 3.9. Say we want to construct a group of order n. We can try to write down an $n \times n$ multiplication table, and ask if it is a group. Assuming it is a group, how many multiplication tables will describe this group?

Answer: $\frac{n!}{|\mathrm{Aut}(G)|}$ multiplication tables. The reason is that there are $n!$ ways to permute the elements, but the table won't change if the permutation is via an automorphism. So we get this answer by looking at the action of S_n on the set of multiplication tables and the stabilizer of this action corresponds to the automorphism group of the corresponding group.

Another example is when counting stacky points, where you should think of a stacky point as a fractional point, with proportion 1 over the size of the automorphisms of that point.

3.2. **Motivations for Cohen-Lenstra's conjecture.** As discussed above, $\frac{1}{\mathrm{Aut}(G)}$ is the most natural measure on finite abelian groups. On the other hand, $\mathrm{Cl}_K^{\mathrm{odd}}$ is so random and unpredictable, it should basically be a random group. This gives some motivation for their conjecture.

Remark 3.10. One should probably also count quadratic fields on the left hand side of Conjecture 3.2 inversely proportional to their automorphisms. But every quadratic field has 2 automorphisms, so both the numerator and denominator of the left hand side would be multiplied by $1/2$ and they would then cancel.

Remark 3.11. The Cohen Lenstra heuristics have been generalized by Cohen Martinet to arbitrary degree fields, and there one wishes to count inversely proportional to automorphisms. I.e., one would examine sums like $\sum_{K \in \mathscr{F}} \frac{1}{\mathrm{Aut}(K)} f(\mathrm{Cl}_K)$. Here are two caveats.

However, if we count by discriminant, 100% of cubic fields are not Galois, so only have 1 automorphism. Of course f could be unbounded, but morally this suggests we should only see fields with 1 automorphism.

If K is Galois, then Cl_K is a $\mathbb{Z}[C_3]$ module, for C_3 the cyclic group. This has a C_3 action, and so should be considered something totally different. We need to keep track of this additional data and shouldn't really be combining with with non-Galois cubic fields.

Question 3.12. Why do the heuristics for quadratic fields not incorporate the fact that they are $\mathbb{Z}[C_2]$ modules?

Indeed, Cl_K for K a quadratic field is a $\mathbb{Z}[C_2]$ module. Cohen-Lenstra knew this, but we will know see why this adds no additional data. Namely, the automorphism of K acts by sending an ideal I to its conjugate $\overline{I}$. Then, $I \cdot \overline{I}$ is the norm of I, which is trivial in the class group. Therefore C_2 acts on the

class group by inversion, and hence poses no additional data. In the degree 3 cyclic case, there are multiple possibilities (though still some constraints) for what the C_3 action is, and that needs to be kept track of.

Question 3.13. Why do we take the odd part of the class group?

The reason is that by genus theory, $\mathrm{Cl}_K[2] \simeq (\mathbb{Z}/2\mathbb{Z})^{\text{number of primes dividing } \operatorname{disc} K}$. Therefore, it is not random and given by a very simple formula. We expect the rest to be a complete mess. Gerth suggested an updated version of Conjecture 3.2 where one gets rid of the 2-torsion, but keeps the rest of the 2^∞ torsion.

Here are three motivations for the Cohen-Lenstra's conjecture.

(1) We believe that groups should be counted with weight $\frac{1}{|\operatorname{Aut}(G)|}$, as discussed above.
(2) There is a lot of empirical data supporting it
(3) It was known in the case that $f(A) = \#\mathrm{Surj}(A, \mathbb{Z}/3\mathbb{Z}) = |A[3]| - 1$. In this case, the class group average size proven to be 1, which agrees with the conjecture, as the right hand side of Conjecture 3.2 can be computed for this (and most) specific choice(s) of f using the techniques developed on Cohen-Lenstra's paper where they made this conjecture.

It is natural to restrict to the p-part of the class group. In this case, the conjecture simplifies because

$$\sum_{G \text{ finite abelian groups}} \frac{1}{|\operatorname{Aut}(G)|} < \infty$$

Definition 3.14. Let c be the value of the above sum, depending on p. Let ν be the measure on p-power order finite abelian groups sending A to $\frac{c}{|\operatorname{Aut}(A)|}$.

Remark 3.15. If our function $f(A)$ only depends on the p-part of A, then the right hand side of Conjecture 3.2 becomes $\mathbb{E}_\nu(f)$.

Here is yet another motivation:

Remark 3.16. Friedman and Washington were thinking about the function field analog of Conjecture 3.2. The found the following remarkable fact. Let $M \in M_{n\times n}(\mathbb{Z}_p)$ be the random variable drawn randomly from $n \times n$ matrices with entries in $\mathbb{Z}_p$, taken with respect to additive Haar measure. We can view $M : \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ which has a cokernel that is a finite abelian group. It turns out that

$$\lim_{n\to\infty} \text{Prob}\left(\operatorname{coker} M \simeq A\right) = \nu(A) = \frac{c}{|\operatorname{Aut}(A)|}.$$

One should think about these matrices over $\mathbb{Z}$ with coefficients up to X, but the sum does not converge, so to formulate it precisely they worked over $\mathbb{Z}_p$.

Remark 3.17. Take S to be a large set of prime ideals in K. Then $\mathrm{Cl}_K = I^S/\mathscr{O}_S^\times$, where I^S means ideals with valuation 0 outside of S, and $\mathscr{O}_S^\times = H^0(S, \mathbb{G}_m)$. More precisely,

$$\mathrm{Cl}_K = \mathrm{coker}\left(\mathscr{O}_S^\times/\mu(\mathscr{O}_K) \to I^S\right)$$

if S is large enough. There are explicit bounds on the size of S, using, for example, Minkowski's bound on the size of the class group.

One can also think about this for many different large S. In this way, $\mathrm{Cl}_K[p^\infty] = \mathrm{coker}\left(\mathbb{Z}_p^{|S|} \to \mathbb{Z}_p^{|S|}\right)$. Here, $\mathrm{Cl}_K[p^\infty] = \mathrm{Cl}_K \otimes \mathbb{Z}_p$.

As a teaser for next time, one might guess one could enrich the conjecture to say that maps $\mathbb{Z}_p^{|S|} \to \mathbb{Z}_p^{|S|}$ are equidistributed for the natural Haar measure. However, it now seems this is probably not so in any interesting case.

Remark 3.18. If we want to make predictions for non-maximal orders in quadratic fields, we can use an exact sequence relating them to maximal orders, see [CL84, §10, (C'2)]. However, Ila Varma and Manjul Bhargava have some results showing the result is different from that predicted by the Cohen-Lenstra conjectures for 3-torsion in quadratic fields and 2-torsion in cubic fields.

4. 9/11/20

Recall at the end of last time we identified the class group of K as the cokernel of a matrix

$$\mathscr{O}_S^\times/\mu_K \to I^S$$

for S a suitably large set of primes in K. We tensored this map with $\mathbb{Z}_p$ to obtain an element of $M_{n\times n}(\mathbb{Z}_p)$. When we chose the matrix randomly from the additive Haar measure, we obtained that the cokernel was distributed as a random abelian group appearing with measure inversely proportional to its automorphisms. This allows us to rephrase the Cohen Lenstra heuristics for imaginary quadratic fields as a question of equidistribution of the cokernels of these matrices.

4.1. **Universality.** We start by reviewing some probability. Let $N(0,1)$ denote the normal distribution of mean 0 and variance 1 and let $X \in N(0,1)$ be a random variable with that distribution. Let X_i denote iid (independent identically distributed) copies of X. It is not hard to compute that

$$\frac{X_1 + \cdots + X_n}{\sqrt{n}} = N(0,1)$$

Now, let Y be a mystery random variable and let Y_i be iid copies of Y. Suppose we find that for large n,

$$\frac{Y_1 + \cdots + Y_n}{\sqrt{n}} \sim N(0,1).$$

Question 4.1. Should we conjecture that Y is close to $N(0,1)$?

Answer: no, by the central limit theorem.

Recall first the law of large numbers.

Theorem 4.2 (Law of large numbers)**.**

$$\frac{Y_1 + \cdots + Y_n}{n} \to 0.$$

as $n \to \infty$*.*

The central limit theorem is a refinement of the law of large numbers.

Theorem 4.3 (Central limit theorem)**.** *If* Y *has mean* 0 *and variance* 1 *then*

$$\frac{Y_1 + \cdots + Y_n}{\sqrt{n}} \to N(0,1).$$

as $n \to \infty$*.*

Remark 4.4. This is an example of a common theme. We start with many random inputs into a process, and the output doesn't depend on the inputs. This is the theme of universality.

Here is another instance of universality, this time for random integral matrices.

Theorem 4.5 (Wood)**.** *For each integer* n*, choose* n^2 *random variables* X_{ij}^n *with outputs in* $\mathbb{Z}_p$ *and let* $B_{ij}^n \in M_{n\times n}(\mathbb{Z}_p)$ *denote a random matrix with the* ij*th entry is drawn from* X_{ij}^n*. Suppose there exists* $\varepsilon > 0$ *so that for all* a, n, i, j*,*

$$\text{Prob}(B_{ij}^n \equiv a (\text{mod}\, p)) \leq 1 - \varepsilon.$$

Then, for any finite abelian p*-group,*

$$\lim_{n\to\infty} \text{Prob}\left(\text{coker}\, B^n \simeq A\right) = \frac{\prod_{i\geq 1} 1 - p^{-i}}{|\,\text{Aut}\, A|}$$

Remark 4.6. You might think that ε is about $1/100$, and then we are saying that B_{ij}^n takes on any value no more than 99% of the time. Also note that ε does not depend on n.

A reasonable example is that the B_{ij}^n may take on two residues $\bmod p$, each 50% of the time.

Remark 4.7. Another way to phrase this theorem is that as long as there is no conspiracy, your random $n \times n$ matrices tends have cokernel distributed according to the $\frac{c}{\mathrm{Aut}}$ measure. By $\frac{c}{\mathrm{Aut}}$ measure, we mean the measure where a given p-group appears inversely proportional to its automorphisms.

There are two types of conspiracies

(1) B is the 0 matrix (or too many of the values of B lie in a single residue class).
(2) The entries of B are not independent.

Remark 4.8. If A is a symmetric matrix with the upper triangular entries appearing independently, there will be a different distribution for the cokernel of A. Wood has a similar universality theorem characterizing the cokernels of symmetric matrices. We should expect this to be different because the cokernel would then have a symmetric pairing, and so we should expect to get these cokernels distributed among abelian groups with the extra structure of a symmetric pairing, not equidistributed among all abelian p-groups.

However, this is no contradiction because the entries of a symmetric matrix are not independent. The upper right corner is the same as the lower left corner.

Remark 4.9. The matrices $\mathcal{O}_S^\times / \mu_K \to I^S$ do not seem to be Haar random, but probably do satisfy the universality theorem. This gives more support to the cohen lenstra conjectures, so long as there isn't a conspiracy.

Remark 4.10. There are lots of interesting open questions relating to these sort of universality theorems, which might be good project or paper topics for the course.

4.2. **Analytic and measure theoretic issues.** Recall that $\sum_{G \text{ a finite abelian group}} \frac{1}{|\mathrm{Aut}(G)|} = \infty$. We saw one way to deal with this by passing to p-sylow subgroups. Here is another way to deal with this.

Definition 4.11. For G a profinite abelian group, we let $G_p = G \otimes_{\mathbb{Z}} \mathbb{Z}_p$ denote its p-sylow subgroup.

Exercise 4.12. Check that this is a reasonable definition of p-sylow subgroup for a profinite group.

Definition 4.13. Let $\mathscr{A}$ denote the set of isomorphism classes of profinite abelian groups G such that all the p-sylow subgroups of G, G_p are finite and $G_2 = 1$.

Lemma 4.14. *We have* $\mathscr{A} = \prod_{\text{primes } p>2} \{ \text{finite abelian } p\text{-groups} \}$.

Proof. The bijection is given by sending $G \mapsto (G_p)_p$ with inverse sending $(G_p)_p \mapsto \prod_p G_p = \lim \prod_{p \leq X} G_p$. □

Suppose ν_p denotes the $\frac{c}{\text{Aut}}$ measure on finite abelian p groups. Then, we give $\mathscr{A}$ the product measure ν.

The Cohen Lenstra conjecture Conjecture 3.2 can then be approximately restated as follows:

Conjecture 4.15. For "reasonable" functions f,

$$\lim_{X \to \infty} \mathbb{E} \mu_X(f(\mathscr{O}_K)) = \mathbb{E}_\nu(f(G)).$$

Remark 4.16. For many f as discussed in previous classes, the right hand side of Conjecture 4.15 agrees with the right hand side of Conjecture 3.2. However, this is not true for all f. In particular, it fails when f is the indicator that a group is finite, as we now verify.

Lemma 4.17. *For f The indicator function 1_{finite} we have* $\text{Prob}_\nu(f(G)) = 0$ *but* $\lim_{X \to \infty} \text{Prob}_{\mu_X}(|\text{Cl}_K| < \infty) = 1$.

Proof. Because there are only countably many finite abelian groups and ν is a measure, it is enough to check that $\text{Prob}_\nu(G \simeq A) = 0$ for any finite abelian group A. This holds because A has no p-component for sufficiently large p, say for $p > n$. Therefore, since ν is the product measure, the probability $\text{Prob}_\nu(G \simeq A) = 0$ is bounded above by $\prod_{p>X \text{ prime}} \frac{\prod_{i \geq 1}(1-p^{-i})}{1}$, where the 1 in the denominator indicates that the automorphism of the identity group are trivial. This product converges to 0 because we even have that $\prod_{p \geq X}(1 - \frac{1}{p})$ tends to 0. □

Remark 4.18. The set $\mathscr{A}$ is uncountable. This suggests that perhaps the natural measure of distributions in the limit is best understood as a distribution on a bigger space.

4.3. **Test functions.** There are various notions of convergence in measure. For us, we will not be able to use all test functions. This is underscored by the following result:

Theorem 4.19 (Poonen, in a paper of Bartel and Lenstra)**.** *If π is a discrete probability measure on the set of finite odd abelian groups that is not supported on a*

finite set and $Y_1, Y_2, \ldots$ are random iid finite abelian groups drawn from π then

$$\text{Prob}(\exists f \text{ such that } E_\pi(f(A)) < \infty \text{ and } \lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} f(Y_i) \text{ does not exist }) = 1.$$

The above probability is in terms of the choice of the Y_i.

Remark 4.20. The law of large numbers implies that for all test functions f, we have $E_\pi(f(A)) = \lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} f(Y_i)$ with probability 1. The problem is that there are too many test functions, so even though any given one works with probability 1, there will always be one that fails.

The moral is that we don't expect to be able to use all test functions.

Question 4.21. Which test functions should we use? I.e., which functions are the reasonable ones?

Remark 4.22. Here is one popular choice for the possible test functions. We can take those giving weak $(*)$ convergence. By a theorem of Portmanteau, this is equivalent to f being bounded and continuous, though there are many other equivalent definitions.

That is, for all bounded continuous functions f, if we have

$$\lim_{X\to\infty} \mathbb{E}_{\mu_X}(f(Y)) = \mathbb{E}_{\mu}(f(Y))$$

then $\mu_X \to \mu$ converges weakly in measure.

Exercise 4.23. Show that the indicator function that a group is finite is not continuous. *Loose hint:* This essentially follows from unwinding the definitions. That is, we defined the product measure with the product topology, and the characteristic function of a set being finite is not continuous because the basic open sets defining the product topology are products of open sets in finitely many of the components, and the whole space in the remaining components.

Remark 4.24. Note that the indicator function that a group is cyclic and the indicator function that a group is squarefree actually turn out also not to be continuous in the above topology. However, Melanie recommends taking a finer topology than the product topology (which we will not go into now). This will make these functions continuous, though the indicator function that a group is finite will still fail to be continuous.

Remark 4.25. The Cramer model for primes says to take P_n to be the Bernoulli random variable which is 0 with probability $1 - \frac{1}{\log n}$ and 1 otherwise. This simulates the chance that n is prime. One can then study the statistical behavior of P_n to try to understand that of primes. For example, things

which are true about P_n may be true about primes. If we randomly decide whether n is prime with chance $\frac{1}{\log n}$, then many things true about P_n may also be true about primes. This lets one predict asymptotics for things like the number of twin primes.

Similarly, even if we pretend class groups are drawn from a fixed distribution (though we have no reason to expect that they are) Theorem 4.19 shows that we can't use all test functions f. Here, it may not really be that they are drawn from a distribution, but that only makes things worse.

5. 9/16/20

Today we will discuss genus theory, and why Cohen Lenstra needed to take the odd part of the class group. We will approach this via class field theory.

Question 5.1. Let $p \equiv 1 \bmod 4$ be a prime. Let $K = \mathbb{Q}\left(\sqrt{-4p}\right)$. This is ramified at 2 and p. What is a degree 2 extension of K which is unramified.

Answer: $L := K\left(\sqrt{p}\right)$ is unramified over K. To check this is unramified, since $\mathbb{Q}\left(\sqrt{p}\right)$ is unramified away from p, L/K can only be ramified at p. To understand ramification, look at the Galois diagram

(5.1)
$$\begin{array}{ccccc} & & L & & \\ & \swarrow & & \searrow & \\ K & & & & \mathbb{Q}\left(\sqrt{p}\right) \\ & \searrow & & \swarrow & \\ & & \mathbb{Q} & & \end{array}$$

which has corresponding Galois groups

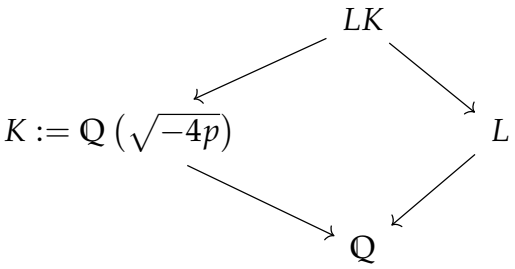
(5.2)
$$\begin{array}{ccccc} & & 1 & & \\ & \swarrow & & \searrow & \\ \mathbb{Z}/2 \times 1 & & & & 1 \times \mathbb{Z}/2 \\ & \searrow & & \swarrow & \\ & & \mathbb{Z}/2 \times \mathbb{Z}/2 & & \end{array}$$

Because tame inertia is cyclic, the inertia of L over $\mathbb{Q}$ at p must be $\mathbb{Z}/2$. Its projection to both factors is nontrivial, so it must map into the diagonal $\mathbb{Z}/2 \subset \mathbb{Z}/2 \times \mathbb{Z}/2$. This implies L/K is unramified, since it intersects the diagonal subgroup trivially. The point here is that inertia in $\mathrm{Gal}(L/K)$ is the inertia in $\mathrm{Gal}(L/\mathbb{Q})$ intersected with $\mathrm{Gal}(L/K)$.

Remark 5.2. So above we had a neat construction. Does this work in other settings?

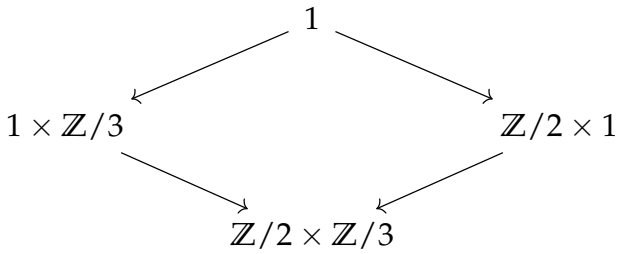
Example 5.3 (Non-example)**.** Suppose we take a cyclic cubic extension L over $\mathbb{Q}$ which is ramified only at p. We have

(5.3)



This corresponds to the diagram of Galois groups

(5.4)



The problem now is that inertia at p can be generated by $(1,1) \subset \mathbb{Z}/2 \times \mathbb{Z}/3$, but this now generates the full group $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2 \times \mathbb{Z}/3$, and therefore its intersection with $1 \times \mathbb{Z}/3$ is nontrivial.

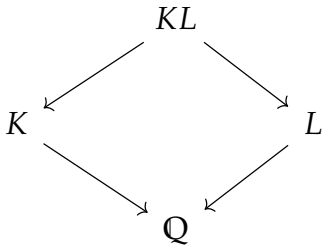
So, the above trick is somewhat limited. Let's now see how far we can push it. Note that because we are working with abelian extensions, we have a well defined inertia subgroup. In general, it is only a conjugacy class of subgroups.

Fact 5.4. The inertia group in the Galois group of the maximal tame extension of K at p over K is pro-cyclic. In fact, when K is a local field (as we may assume if we wish to understand the inertia at p, we know the structure of the Galois group of the maximal tame extension.

Proposition 5.5. *Let K over $\mathbb{Q}$ be a degree 2 extension and $L/\mathbb{Q}$ be an abelian extension not containing K. If LK/K is unramified then $\mathrm{Gal}(L/\mathbb{Q})$ is 2-torsion and the set of places ramified in $L/\mathbb{Q}$ is contained in the set of places ramified in $K/\mathbb{Q}$.*

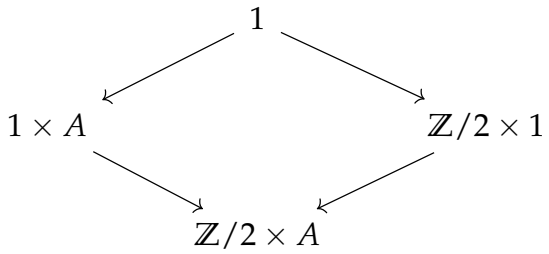
Proof. We have

(5.5)



and corresponding Galois diagram

(5.6)

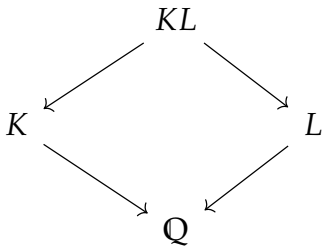


What can elements in the inertia group of $KL/\mathbb{Q}$ look like? We can't have $(0,a)$ for $a \neq 0$ because LK/K is unramified. So, all inertia elements are $(0,0)$ or $(1,a)$. If $(1,a)$ is inertia so is $(0,2a)$ so $2a = 0$. Therefore, inertia is contained in $\mathbb{Z}/2 \times A[2]$. Since there are no nontrivial unramified extensions of $\mathbb{Q}$¡ we find $A = A[2]$. □

Remark 5.6. So, for our trick to work, we can only build unramified extensions of degree 2 extensions K of $\mathbb{Q}$ using other degree 2 extensions which ramify in a subset of the primes that K ramifies in.

Suppose we have a Galois diagram

(5.7)



with $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/2)^k$ and $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2$. Let H be the Hilbert class field of K so that $\mathrm{Gal}(H/K) \simeq \mathrm{Cl}_K$. Let $K \subset M \subset H$ be the intermediate extension with $\mathrm{Gal}(H/M) \simeq \mathrm{Cl}_K/2\,\mathrm{Cl}_K$. We obtain a surjection $\mathrm{Cl}_K \to (\mathbb{Z}/2)^k$

Warning 5.7. So, the above diagram tells us about $\mathrm{Cl}_K/2\,\mathrm{Cl}_K$. However, it does not tell us directly about $\mathrm{Cl}_K[2]$, except for the fact that this has the same size as $\mathrm{Cl}_K/2\,\mathrm{Cl}_K$.

Further, because $\mathrm{Gal}(K/\mathbb{Q})$ acts as inversion on Cl_K, it acts trivially on $\mathrm{Cl}_K/2\,\mathrm{Cl}_K$, and so M/K is the base change of an extension L of $\mathbb{Q}$.

5.1. **Review of the idele class group.** Recall that for K a number field the idele class group is

$$C_K := \prod_{v \text{ places of } K} K_v^\times / K.$$

We have that $\widehat{C_K}$, the profinite completion of C_K is the quotient of C_K by the connected component of the identity, which is just a collection of all $\mathbb{R}_{>0}$ factors corresponding to real places of K. There is an isomorphism $\widehat{C_K} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ coming from the Artin map in class field theory. We have an exact sequence

$$1 \longrightarrow \mathscr{O}_K^\times \longrightarrow \textstyle\prod_v \mathscr{O}_v^\times \xrightarrow{\phi} \widehat{C_K} \longrightarrow \mathrm{Cl}_K \longrightarrow 1. \tag{5.8}$$

The last map sends $(\alpha_v) \mapsto v^{\mathrm{ord}_v(\alpha_v)}$, but with no real places in the target. Here, $\mathscr{O}_v^\times$ is $\mathscr{O}_v^\times$ if v is finite but is $\{\pm 1\}$ if v is real and 1 if v is complex.

Further, Cl_K is finite and $\mathscr{O}_K^\times$ is finitely generated, so they are only "finite level obstructions" to ϕ being an isomorphism to ϕ being an isomorphism.

Corollary 5.8. *We have an isomorphism $\prod_p \mathbb{Z}_p^\times \simeq \widehat{C}_{\mathbb{Q}}$. Here, $\mathbb{Z}_p^\times$ is the tame inertia group at p.*

Remark 5.9. If we have $p \equiv 1 \bmod 3$ we can construct nontrivial maps $\mathbb{Z}_p^\times \to \mathbb{Z}/3$. This is necessarily trivial on $\mathbb{Z}_p^\times$ for $p \equiv 2 \bmod 3$. One can make it trivial or not at $p \equiv 1 \bmod 3$. In this way, one can specify any collection of primes which are 1 mod 3 which one desires, and construct an extension of $\mathbb{Q}$ which is ramified at that collection of primes.

Proposition 5.10. *If K is an imaginary quadratic field then*

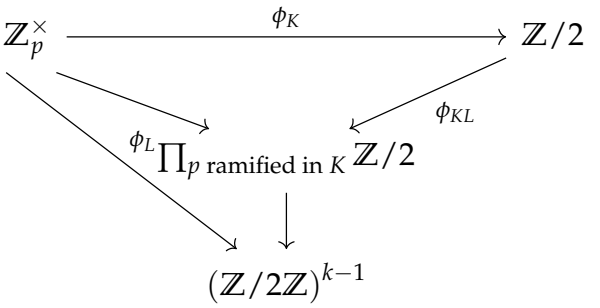
$$|\mathrm{Cl}_K/2\,\mathrm{Cl}_K| = 2^{\omega(\mathrm{disc}(K)-1)}$$

where $\omega(n)$ is the number of distinct prime factors of n.

Proof. By the above it remains to find the largest $(\mathbb{Z}/2)^k$ extension $L/\mathbb{Q}$ such that KL/K is unramified.

We have a diagram

(5.9)



where the bottom vertical map is the projection onto the first $k-1$ coordinates.

Goal 5.11. We want to show no inertia lies in $(\mathbb{Z}/2\mathbb{Z})^{k-1} \times 1$, as this will show KL/L is unramified.

Because $\ker(\phi_{K,p}) \subset \ker(\phi_{L,p})$ we can't have inertia which is trivial in the last coordinate, which shows KL/K is unramified. Alternatively, L was built so that at each prime p, ϕ_K factors through ϕ_{KL} which implies KL/K is unramified.

Exercise 5.12. Complete the proof by showing the constructed L provides the maximal unramified extension of K.

□

Remark 5.13. We saw that genus theory told us $\mathrm{Cl}_K/2\,\mathrm{Cl}_K$ is not random. However, we have an exact sequence

$$0 \longrightarrow 2\,\mathrm{Cl}_K \longrightarrow \mathrm{Cl}_K \longrightarrow \mathrm{Cl}_K/2\,\mathrm{Cl}_K \longrightarrow 0 \tag{5.10}$$

and $2\,\mathrm{Cl}_K$ is the remaining part not described by genus theory. In fact, Gerth generalized the Cohen-Lenstra heuristics from the odd part of Cl_K to $2\,\mathrm{Cl}_K$. Here, he treats all abelian groups the same, and essentially conjectures that $2\,\mathrm{Cl}_K$ appears inversely proportional the the automorphisms of the given abelian group.

5.2. **Preview of next class.** So far, we have discussed the Cohen-Lenstra conjecture for imaginary quadratic fields. Next time, we'll discuss real quadratic fields. Class groups of real quadratic fields are much smaller, so something should definitely be different. There are three equivalent descriptions.

(1) Take $\frac{c}{\mathrm{Aut}\,G}$ and take the quotient by a random element, uniform for Haar measure on G.
(2) Take G with probability $\frac{c}{|\mathrm{Aut}\,G||G|}$.

(3) Take the cokernel of a random matrix $\widehat{\mathbb{Z}}^{n+1} \to \widehat{\mathbb{Z}}^{n+1}$ for a Haar random matrix and let $n \to \infty$.

6. 9/18/20

Today we'll discuss the Cohen Lenstra heuristics for real quadratic fields. Here are some motivations for their heuristics, which are somewhat different in the real quadratic case than the imaginary quadratic case we have been studying so far.

(1) Cohen and Lenstra said that Dick Gross observed the following: Take a fixed prime $p \in \mathbb{Q}$ and look at the imaginary quadratic fields K where p splits as $\mathfrak{p}\overline{\mathfrak{p}}$. Then if one investigates tables of $\mathrm{Cl}_K / [\mathfrak{p}]$ these look very similar to tables of real quadratic class groups. So, we might expect the measure to be the $\frac{c}{|\operatorname{Aut} A|}$ measure quotiented by a uniform random element.
(2) Davenport and Heilbronn's theorem on counting cubic extensions shows that $\lim_{X\to\infty} \mathbb{E}_{\mu_X} \#\operatorname{Surj}(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z}) = 1/3$. This is consistent with the prediction.
(3) If we let $h = \#\mathrm{Cl}_K$ denote the class number and R be the size of the regulator, then we can think of $h = hR/R$, and so we can think of the class group as quotient of some mystery group of size hR by the regulator, corresponding to a generator for the units. Note that when h is imaginary quadratic, the regulator is 1.

Remark 6.1. There is a function field analog to this story which we will discuss in the future. The real quadratic case corresponds to removing 2 points from a proper curve (the points are the infinite places) while the imaginary quadratic case corresponds to removing one degree 2 point.

One student asked:

Question 6.2. Should we think about automorphisms of the pair (field, element) or just automorphisms of the field?

Answer: For K imaginary quadratic split at the prime p, we could ask how $(\mathrm{Cl}_K, [p])$ is distributed in the class group. Wood, Klagsburn, and others have thought about this, and we expect $\frac{1}{|\operatorname{Aut}(\text{ pointed abelian group })|}$ as the measure. Relatedly, we have the following exercise:

Exercise 6.3. Show that the average size of $\frac{1}{|\operatorname{Aut}(\text{ pointed abelian group })|}$ over all finite abelian p-groups agrees with the average size of $\frac{1}{|\operatorname{Aut}(G)|\cdot|G|}$. [Note: I tried to work this out, and it wasn't working for me, but maybe I am misunderstanding the definition of something here.] *Hint:* Use the orbit stabilizer theorem.

Now, we discuss and state the heuristic for real quadratic fields in some more detail.

Recall that in the imaginary quadratic case, $\mathrm{Cl}_K[p^\infty]$ is the cokernel of a map

$$\mathscr{O}_S \otimes \mathbb{Z}_p \to I^S \otimes \mathbb{Z}_p$$

for large enough subsets S of the primes of $\mathscr{O}_K$.

In the real quadratic case, we have the same map, where the former is $\mathbb{Z}_p^{n+1} \to \mathbb{Z}_p^n$. (In the imaginary quadratic case, the ranks of the source and target were the same.) So, we might think $\mathrm{Cl}_K[p^\infty]$ is like the cokernel of a Haar random $n \times (n+1)$ matrix with $\mathbb{Z}_p$ entries. Melanie's universality results still apply to this.

6.1. **Analyzing Haar random matrices.** Let's now try to derive

$$\lim_{n\to\infty} \mathrm{Prob}\left(\mathrm{coker}\left(M : \mathbb{Z}_p^{n+1} \xrightarrow{M} \mathbb{Z}_p^n\right) \simeq A\right)$$

for A a fixed finite abelian group. We first note that the cokernel is finite with probability 1 because the condition for the minors to vanish is given by the vanishing of an equation which has p-adic measure 0.

Now,

$$\lim_{n\to\infty} \mathrm{Prob}\left(\mathrm{coker}\left(M : \mathbb{Z}_p^{n+1} \xrightarrow{M} \mathbb{Z}_p^n\right) \simeq A\right) \simeq \mathbb{E}\left(\#\mathrm{isom}\left(\mathrm{coker}(M), A\right)\right) \frac{1}{|\operatorname{Aut}(A)|}.$$

This is because the set of isomorphism is a torsor under $\operatorname{Aut}(A)$. Another way to say this is that if we believe the average number of isomorphism should be constant, we obtain the same $\frac{1}{|\operatorname{Aut}(A)|}$ distribution. Now, we want to analyze $\mathbb{E}\left(\#\mathrm{isom}\left(\mathrm{coker}\, M, A\right)\right)$. Because maps $\mathbb{Z}_p^n/M(\mathbb{Z}_p^{n+1}) \to A$ lift to $\mathbb{Z}_p^n$, we have

$$\mathbb{E}\left(\#\mathrm{isom}\left(\mathrm{coker}\, M, A\right)\right) = \sum_{f \in \mathrm{Surj}\left(\mathbb{Z}_p^n, A\right)} \mathrm{Prob}\left(\ker f = M\mathbb{Z}_p^{n+1}\right).$$

It will turn out that all such functions f have the same associated probability, as we will soon see. For now, fix one f. We can choose a basis $e_1, \ldots, e_n$ of $\mathbb{Z}_p^n$ so that $A = \langle f(e_i) : p^{\lambda_i} f(e_i) = 0\rangle$ where $A = \prod_{i=1}^n \mathbb{Z}/p^{\lambda_i}\mathbb{Z}$. In other words, there are no "mixed relations" between the generators. Also, since A is fixed and finite, eventually we have $\lambda_i = 0$ as $n \to \infty$. Then,

$$\ker f = \begin{pmatrix} p^{\lambda_1}\mathbb{Z}_p \\ p^{\lambda_2}\mathbb{Z}_p \\ \vdots \end{pmatrix} \subset \mathbb{Z}_p^n.$$

Now, take M a Haar random $n \times (n+1)$ matrix. We want to compute the chance the kernel of f is $M\mathbb{Z}_p^{n+1}$. We will need the ith row to be divisible by p^{λ_i}. Altogether, the chance this happens is $p^{-(n+1)\sum_i \lambda_i} = \text{Prob}\left(M\mathbb{Z}_p^{n+1} \subset \ker f\right)$. This simplifies to $|A|^{-(n+1)}$. Summing this up, we have proven the following:

Lemma 6.4. *We have $M\mathbb{Z}_p^{n+1} = \ker f$ if and only if, when you divide the ith row by p^{λ_i} you get a rank n matrix* $\bmod p$.

Observe that the above happens when each row is independent with the following probabilities: The chance the 1st row is nonzero, which is $1 - p^{-n-1}$, the chance the 2nd row is not a multiple of the first, which is $1 - p^{-n}$. In general, we need the ith row to be independent of the previous ones, which is $1 - p^{-n-2+i}$.

Putting together everything coming earlier in this subsection yields

Corollary 6.5.

$$\text{Prob}\left(\text{coker}\, M \simeq A\right) = \frac{\#\,\text{Surj}(\mathbb{Z}_p^n, A)}{|\,\text{Aut}(A)| \cdot |A|^{n+1}} \prod_{i=2}^{n+1} \left(1 - p^{-i}\right). \tag{6.1}$$

Here, we used the Haar measure, but it is quite non obvious if the entries in this matrix are uniformly distributed. However, this is what Melanie's universality theorem says.

Now, as $n \to \infty$,

$$\frac{\#\,\text{Surj}\left(\mathbb{Z}_p^n, A\right)}{\#\text{Hom}\left(\mathbb{Z}_p^n, A\right)} \to 1$$

and so $\#\,\text{Surj}\left(\mathbb{Z}_p^n, A\right)$ tends to $|A|^n$. It follows that the above (6.1) tends to

$$\frac{1}{|\,\text{Aut}(A)| \cdot |A|} \prod_{i \geq 2} \left(1 - p^{-i}\right).$$

In fact, we have

Theorem 6.6.

$$\lim_{n \to \infty} \text{Prob}\left(\text{coker}\, M \simeq A\right) = \frac{1}{|\,\text{Aut}(A)| \cdot |A|} \prod_{i \geq 2} \left(1 - p^{-i}\right).$$

We have essentially shown the above theorem, modulo two analytic issues, which we now discuss. Here they are:

(1) Is

$$\sum_A \frac{1}{|\operatorname{Aut} A||A|} \prod_{i\geq 2} \left(1-p^{-i}\right) = 1?$$

So far we only know it is at most 1, since there could be escape of mass.

(2) How does this relate to the $\frac{1}{|\operatorname{Aut}(A)|}$ measure after quotienting by a random element? If $X_n = \operatorname{coker}(\mathbb{Z}_p^n \to \mathbb{Z}_p^n)$ for a Haar random such map and $Y_n = \operatorname{coker}\left(\mathbb{Z}_p^{n+1} \to \mathbb{Z}_p^n\right)$, can we get from X_n to Y_n by quotienting by a uniform random element. Note that these random variables X_n and Y_n are finite groups with probability 1. This was mentioned above, and follows from the fact that the minors define hypersurfaces which have vanishing p-adic volume.

In other words, we want to know whether certain limits commute with quotienting by a random element. That is, do we have

$$\lim_{n\to\infty} X_n/ \text{ uniform random element } = \lim_{n\to\infty} (X_n/ \text{ uniform random element }) = \lim_{n\to\infty} Y_n.$$

Remark 6.7. These are real issues and things can sometimes fail to commute with limits. That is, in general, limits may fail to commute with quotienting by a uniform random element.

We will now deal with these two analytic issues simultaneously, essentially using the monotone convergence theorem. We'll actually describe how to deal with them in a slightly different case. We'll focus on the variant of (1) where the matrix is $n \times n$.

In this case, we want to know whether

$$\sum_A \frac{\prod_{i\geq 2}\left(1-p^{-i}\right)}{|\operatorname{Aut}(A)|A|} = 1.$$

We will check

$$\sum_G \lim_{n\to\infty} \operatorname{Prob}(X_n \simeq G) = \lim_{n\to\infty} \sum_G \operatorname{Prob}(X_n \simeq G).$$

Note that $\frac{\#\operatorname{Surj}(\mathbb{Z}_p^n, A)}{A^n}$ is increasing, but $\prod\left(1-p^{-i}\right)$ is decreasing. We want to use the monotone convergence theorem, but it is a minor annoyance that the second factor is decreasing. Fortunately, it does not depend on G so we can factor it out. The key observation is that $\operatorname{Prob}(X_n \simeq G)$ is an increasing

function of n. Therefore, using the monotone convergence theorem, we have

$$\begin{aligned}\sum_G \frac{\lim_{n\to\infty} \operatorname{Prob}(X_n \simeq G)}{\prod_{i\geq 1}(1-p^{-i})} &= \sum_G \lim_{n\to\infty} \frac{\operatorname{Prob}(X_n \simeq G)}{\prod_{i=1}^n (1-p^{-i})} \\ &= \lim_{n\to\infty} \sum_G \frac{\operatorname{Prob}(X_n \simeq G)}{\prod_{i=1}^n (1-p^{-i})} \\ &= \prod_{i\geq 1} \left(1-p^{-i}\right)^{-1}.\end{aligned}$$

Dealing with quotients by a random element is similar: Let Y denote a $\frac{1}{|\operatorname{Aut}|}$ random group quotiented by a random element. Then,

$$\begin{aligned}\frac{\operatorname{Prob}(Y \simeq G_2)}{\prod_{i=1}^n (1-p^{-i})} &= \sum_{G_1,G_2} \lim_{n\to\infty} \frac{\operatorname{Prob}(X_n \simeq G_1)}{\prod_{i=1}^n (1-p^{-i}) \operatorname{Prob}(G_1/\langle g\rangle \simeq G_2)} \\ &= \lim_{n\to\infty} \sum_{G_1,G_2} \frac{\operatorname{Prob}(X_n \simeq G) \operatorname{Prob}(G_1/\langle g\rangle \simeq G_2)}{\prod_{i=1}^n (1-p^{-i})} \\ &= \lim_{n\to\infty} \frac{\operatorname{Prob}(Y_n \simeq G_2)}{\prod_{i=1}^n (1-p^{-i})}.\end{aligned}$$

The final Y has the $\frac{1}{|\operatorname{Aut}(G)||G|}$ distribution. Here, we used the monotone convergence theorem.

Question 6.8. Why do we not just take the cokernel of $\mathscr{O}_S^\times/\mathscr{O}_K^\times \to I^S$ where both have rank n in the real quadratic case?

Indeed, the above question may seem reasonable, and would suggest that the imaginary quadratic and real quadratic fields should have identically distributed class groups. However, empirically this cannot be. But it seems reasonable given that any map $\mathbb{Z}_p^{n+1} \to \mathbb{Z}_p^n$ factors through $\mathbb{Z}_p^n$. This seems like a legitimate concern. However, according to the data, it seems we should take the cokernel of a map $\mathscr{O}_S^\times \to I^S$ and not $\mathscr{O}_S^\times/\mathscr{O}_K^\times \to I^S$. Also, there is no good basis for $\mathscr{O}_S^\times$ and the quotient $\mathscr{O}_S^\times/\mathscr{O}_K^\times$ does not have a splitting.

Remark 6.9. One possible project for the course is to make computations of $\mathscr{O}_S^\times/\mathscr{O}_K^\times$ for various quadratic fields K, looking at a basis and counting maps to I_S.

Hence, in the case of the real quadratic Cohen Lenstra distribution, we get an actual distribution on class groups.

Remark 6.10. Let $\mathscr{A}$ denote the set of profinite abelian groups with finite p-sylow subgroups. On $\mathscr{A}$, for μ_{imag} Cohen-Lenstra's measure for imaginary

quadratic fields, we find $\mu_{\text{imag}}(\text{ finite groups }) = 0$ and $\mu_{\text{imag}}(\mathscr{A}) = 1$. But when we take μ_{real} the $\frac{c}{|A||\operatorname{Aut}(A)|}$ measure, we find $\mu_{\text{real}}(\text{ finite groups }) = 1$. This follows from convergence of $\sum_{G \text{ p-groups}} \frac{1}{|G||\operatorname{Aut}(G)|}$.

6.2. **Function field analogs.** Is number theory about $\mathbb{Z}$ or $\mathbb{Q}$? If it is about $\mathbb{Q}$, why do we study $\mathbb{Z}$ and not $\mathbb{Z}[1/2]$?

Observe that open subschemes of $\mathbb{Z}$ obtained by localizing correspond to smaller geometric spaces.

Remark 6.11. For any (nonzero) subring $R \subset \mathbb{Q}$ we have $\mathbb{Z} \subset R$. In the function field setting, the analogous question would be what subrings of $\mathbb{F}_q(t)$ there are, and if they need to contained $\mathbb{F}_q[t]$.

Question 6.12. What are the subrings of $\mathbb{F}_q(t)$ not containing $\mathbb{F}_q[t]$?

Some examples are $\mathbb{F}_q, \mathbb{F}_p, \mathbb{F}_q[t^k], \mathbb{F}_q[t^2, t^3]$,.

Fact 6.13. $\mathbb{F}_q[t]$ is minimal in the sense that there is no proper integrally closed subring with fraction field $\mathbb{F}_q(t)$. However, there are many other such minimal subfields such as $\mathbb{F}_q[1/t], \mathbb{F}_q[1/(t-a)], \mathbb{F}_q[1/p(t)]$ for $p(t)$ an irreducible polynomial.

Really, what is going on here is that $\mathbb{P}^1_{\mathbb{F}_q}$ is the unique regular proper curve with function field $\mathbb{F}_q(t)$.

Remark 6.14. Rings only see affine pieces of $\mathbb{P}^1_{\mathbb{F}_q}$. We have the analogy, $\operatorname{Spec}\mathbb{Z}$ is to $\operatorname{Spec}\mathbb{Q}$ as $\mathbb{P}^1_{\mathbb{F}_q}$ is to $\operatorname{Spec}\mathbb{F}_q(t)$ The places of $\mathbb{Q}$ are the infinite place and the primes while the places of $\mathbb{F}_q(t)$ correspond to closed points of $\mathbb{P}^1_{\mathbb{F}_q}$.

There are some subtleties in the number field and function field analogy. In the function field setting, say we have K a degree 2 extension of $\mathbb{F}_q(t)$ with ring of integers $\mathscr{O}_K$, the integral closure of $\mathbb{F}_q[t]$ in K. Then, we have $\operatorname{Cl}(\mathscr{O}_K) = \operatorname{Pic}(\mathscr{O}_K)$ is a finite abelian group, as in the number field case.

Let C be the proper regular curve associated to K. We can either discuss $\operatorname{Cl}(\mathscr{O}_K)$ or $\operatorname{Pic}(C)$, which are in general quite different. There is a sequence

$$0 \longrightarrow \operatorname{Pic}^0(C) \longrightarrow \operatorname{Pic}(C) \longrightarrow \mathbb{Z}. \tag{6.2}$$

where the last map is given by degree. It is not obvious this map is surjective, but it turns out to be by Lang's theorem.

Then, $\operatorname{Pic}(\operatorname{Spec}\mathscr{O}_K) = \operatorname{Pic}(C)/\langle \mathscr{L}(p) \rangle$ for p a point over ∞. the imaginary quadratic field case corresponds to the hyperelliptic curve being ramified over ∞ and the real quadratic field corresponds to being unramified over ∞.

In the imaginary quadratic field case, $\mathscr{L}(\mathscr{O}_K) \simeq \mathrm{Pic}(C)/\mathscr{L}(\infty_1)$, for ∞_1 the unique point over ∞ in $\mathbb{P}^1$.

In the real quadratic field case, we have two points ∞_1, ∞_2 over ∞ in $\mathbb{P}61$ and we have $\mathrm{Pic}^0(C) \simeq \mathrm{Pic}(C)/\mathscr{L}(\infty_1)$. Then, $\mathrm{Cl}(\mathscr{O}_K) = \mathrm{Pic}^0(C)/\mathscr{L}(\infty_1 - \infty_2)$.

For $\mathbb{F}_q(t)$, there is nothing special about ∞. Rather, $\mathrm{Pic}(C)$ or $\mathrm{Pic}^0(C)$ is the more natural object to think about. It is natural to guess that $\mathrm{Pic}^0(C)$ should be distributed like a $\frac{1}{|\mathrm{Aut}(A)}$ measure for the odd part.

Remark 6.15. When C is split at ∞ with fiber $\infty_1 + \infty_2$, then $\mathscr{L}(\infty_1 - \infty_2)$ behaves like a uniformly random element of $\mathrm{Pic}^0(C)$. Therefore, for K real quadratic, we find their class groups should be distributed according to the $\frac{c}{|A||\mathrm{Aut}(A)|}$ measure.

Remark 6.16. This is reminiscent of Gross' remark in Cohen-Lenstra's paper that the table of sizes of real fields look like $\mathrm{Cl}_K / < A\mathfrak{p} >$

Remark 6.17. In $\mathbb{F}_q(t)$, ∞ is not special. To understand why, see Wood's paper on cohen lenstra and local conditions. There is the guess that the left naturally extends to any point of $\mathbb{F}^1_{\mathbb{F}_q}$ and any place of $\mathbb{F}_q(t)$ can replace ∞.

Next time, we'll see another perspective in the function field case. Then, $\mathrm{Pic}^0(C)$ is the Frobenius fixed points of a variety, and so we can try to understand how Frobenius acts on the Jacobian. This will give another motivation for the Cohen-Lenstra heuristics

7. 9/25/20

For today, we will work over $\mathbb{F}_q(t)$ and let $p = \mathrm{char}\,\mathbb{F}_q$ and ℓ be a prime not equal to p and ℓ be a prime not equal to p

Take $K = \mathbb{F}_q(t)[y]/(y^2 = a(t)y + f(t)$ with $a(t), f(t) \in \mathbb{F}_q[t]$. Then, K is the function field of a smooth projective curve over $\mathbb{F}_q$. There is a projection $\pi : C \to \mathbb{P}^1_{\mathbb{F}_q}$. Let $J := \mathrm{Jac}(C)$, which is an abelian variety over $\mathbb{F}_q$ of dimension g.

Using that the Brauer group of $\mathbb{F}_q$ is trivial and the Leray spectral sequence, one can deduce the following:

Fact 7.1. $J(\mathbb{F}_q) = \mathrm{Pic}^0(C)$.

Remark 7.2. The dimension g is a good analog of the discriminant in the function field setting.

When $p \nmid m$ it follows from the theory of abelian varieties that $J(\overline{\mathbb{F}}_q)[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}$. We also have an isomorphism $\mathrm{Pic}^0(C)[m] \simeq J(\mathbb{F}_q)[m]$ as abelian

groups, where the $\mathbb{F}_q$ points of J are the Frobenius fixed points of $J(\overline{\mathbb{F}}_q)[m]$. Moreover, $\mathrm{Jac}(\overline{\mathbb{F}}_q)[\ell^\infty] = (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$ and Frobenius acts on this. We next want to use this to obtain a model for the Cohen Lenstra heuristics in the function field setting.

Let D be a divisible group such that $D[\ell^k]$ is finite for $k \geq 0$.

Definition 7.3. The *Tate module* $T_\ell D := \lim D[\ell^k]$ along the maps

$$D[\ell^{k+1}] \xrightarrow{\times \ell} D[\ell^k].$$

Remark 7.4. We have $D[\ell^k] = T_\ell D / \ell^k T_\ell D$.

We now wish to apply this to $T_\ell J := \mathrm{Jac}(\overline{\mathbb{F}}_q)[\ell^\infty] \simeq \mathbb{Z}_\ell^{2g}$. The key fact here is that $\mathrm{Pic}^0(C)[\ell^\infty] = \ker(\mathrm{Frob} - \mathrm{id})$.

The following lemma lets us compare this to the cokernel of $\mathrm{Frob} - \mathrm{id}$.

Lemma 7.5 (Friedman-Washington, 1989)**.** *Let D be as above and $\phi : D \to D$ a surjective homomorphism. Then, we have $T_\ell \phi : T_\ell D \to T_\ell D$. If $\ker \phi$ is a finite ℓ group then* $\ker \phi \simeq \mathrm{coker}\,(T_\ell \phi)$.

Proof. There is a map

$$\begin{aligned} \ker \phi &\to \mathrm{coker}\, T_\ell \phi \\ \alpha &\mapsto \left\{ \phi\left(\ell^{-n}\right) \alpha \right\}_n \end{aligned}$$

where $\ell^{-n}\alpha$ is really shorthand for a choice of element x so that $\ell^n x = \alpha$. By construction, $\phi(\ell^{-n}\alpha) \in D[\ell^n]$. Further, there are difference possible choices of $\ell^{-n}\alpha$, but they differ by an element in $\phi(T_\ell D)$, i.e., by an element in the image of ϕ. Therefore, we obtain a well defined element in $\mathrm{coker}(\phi)$. Since the kernel is finite, the map is injective. The map is surjective because a limit of finite sets is compact by Tychonoff's theorem, and so we can make choices at each level to form a compatible system of lifts. □

Now, we may apply the above lemma to $\phi = \mathrm{Frob} - \mathrm{id}$ acting on $J(\overline{\mathbb{F}}_q)$. This is justified because $J(\mathbb{F}_q)$ is a finite group, and so the kernel of ϕ is finite which implies ϕ is surjective, since the only way a self map from $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$ to itself can fail to be surjective is if it does not surject onto $(\mathbb{Z}_\ell/p\mathbb{Z}_\ell)^{2g}$ and hence has some subgroup isomorphic to $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ in the kernel. This crucially uses divisibility of $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$.

We can identify

$$\mathrm{Frob} \in \mathrm{Hom}\left((\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}, (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}\right) \simeq M_{2g\times 2g}(\mathbb{Z}_\ell)$$

and

$$\text{Frob} \in \text{Hom}\left((\mathbb{Z}_\ell)^{2g}, (\mathbb{Z}_\ell)^{2g}\right) \simeq M_{2g\times 2g}(\mathbb{Z}_\ell)$$

Under this identification, $\phi \mapsto T_\ell\phi$ is given by the same matrix. So, $\ker\phi$ on $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$ is identified with $\operatorname{coker}\phi$ on $\mathbb{Z}_\ell^{2g}$ Applying this to $\phi = \text{Frob} - 1$ we get

$$\text{Pic}^0(C)[\ell^\infty] = \operatorname{coker}(\text{Frob} - 1)\,|_{\mathbb{Z}_\ell^{2g}}.$$

Our next model is given by taking Frob to be a random element of $\text{GL}_{2g}(\mathbb{Z}_\ell)$. One might guess that Frobenius equidistributed with respect to Haar measure on $\text{GL}_{2g}(\mathbb{Z}_\ell)$. Friedman and Washington made this into a precise conjecture as $g \to \infty$.

Question 7.6. If $M \in \text{GL}_{2g}(\mathbb{Z}_\ell)$ is drawn randomly from the Haar measure on $\text{GL}_{2g}(\mathbb{Z}_\ell)$, what is the distribution of $\operatorname{coker}(M - \text{id})$?

To make this precise, one needs to specify a collection of test functions, but let's not worry about this for now.

Theorem 7.7 (Friedman-Washington)**.** *For A a finite abelian ℓ group*

$$\lim_{n\to\infty} \text{Prob}\left(\operatorname{coker}(F-1) \simeq A\right) = \frac{c}{|\operatorname{Aut}(A)|},$$

for F a random matrix from Haar measure on $\text{GL}_n(\mathbb{Z}_\ell)$.

Friedman and Washington had a fairly involved proof of this, though one can also give a fairly simple proof using moments.

Remark 7.8. This gives another kind of universality. Before we saw the cokernel of a random matrix has the Cohen-Lenstra distribution. Now, it turns out that $F - 1$ also has this distribution when F is drawn randomly from invertible matrices. Note that the entries of F are certainly not random, since F must be invertible, but it still has this universality and the cokernel distribution still tends to the $\frac{c}{|\operatorname{Aut}|}$ measure.

Friedman and Washington called this fact that $\operatorname{coker}(F-1)$ has the same distribution of the cokernel of a random matrix "blurring."

Example 7.9. As an example of something failing universality, if we just take F Haar random in $\text{GL}_n(\mathbb{Z}_\ell)$ and don't subtract the identity, the cokernel of F always is trivial, and so the distribution is the point mass supported at the trivial group.

Remark 7.10. One interesting project could be to try to find a bigger universality class interpolating between $F - 1$ for $F \in \text{GL}_n(\mathbb{Z}_\ell)$ and $M \in M_{n\times n}(\mathbb{Z}_\ell)$ random.

We now want to refine our model.

Question 7.11. Why is Frob not general in $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$?

The answer is that there is a Weil pairing on the Jacobian which is a perfect alternating pairing

$$J\left(\overline{\mathbb{F}}_q\right)[\ell^k] \times J\left(\overline{\mathbb{F}}_q\right)[\ell^k] \to \mu_{\ell^k}(\overline{\mathbb{F}}_q).$$

This is compatible between different values of k and gives a map

$$\begin{array}{ccc} T_\ell J\left(\overline{\mathbb{F}}_q\right) \times T_\ell J\left(\overline{\mathbb{F}}_q\right) & \xrightarrow{W} & \mathbb{Z}_\ell(1) \\ \downarrow \simeq & & \downarrow \simeq \\ \mathbb{Z}_\ell^{2g} \times \mathbb{Z}_\ell^{2g} & \longrightarrow & \mathbb{Z}_\ell \end{array} \tag{7.1}$$

where we can choose a basis so that

$$W = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

Question 7.12. How does this interact with Frobenius?

We find

$$W(\mathrm{Frob}\, x, \mathrm{Frob}\, y) = qW(x,y).$$

This factor of q is because Frob sends $x \mapsto x^q$ and taking the map $\mu_\ell^k \to \mathbb{Z}_\ell$ turns this multiplicative operation into an additive one, so raising to the qth power corresponds to multiplying by q. Altogether, we find $F^t W F = qW$ so $F \in \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}_\ell)$.

Our next model is then to take a Haar random matrix from $\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}_\ell)$.

Question 7.13. What is the cokernel distribution of $F - 1$ for $F \in \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}_\ell)$ Haar random?

Garton computed the moments, and by a result of Wood, this determines the distribution. When $\ell \nmid q - 1$, as $g \to \infty$,

$$\mathrm{Prob}\left(\mathrm{coker}\,(F - I) \simeq A\right) \to \frac{c}{|\mathrm{Aut}(A)|}$$

for $F \in \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}_\ell)$. This is not true for any particular g but does hold in the $g \to \infty$ limit. When $\ell \mid q - 1$, we get a different cokernel distribution, as was observed by Achter, and also investigating in a recent paper of Lipnowski, Tsimerman, and Sawin. They give a formula for this distribution. Garton found the moments of this distribution.

Question 7.14. What is going on?

If $\ell \mid q-1$ then $\mathbb{F}_q(t)$ has ℓth roots of unity. When ℓ is odd, $\mathbb{Q}$ has no ℓth roots of unity. So, in this way, $\ell \mid q-1$ implies that $\mathbb{F}_q(t)$ is not like $\mathbb{Q}$.

Remark 7.15. We expect that $\mathrm{Pic}^0(C)[\ell^\infty]$ should be differently distributed when $\ell \mid q-1$. We expect this is more similar to the case when $\mathbb{Q}$ is replace by a number field K with $\mu_\ell(K) \neq 1$. What exactly we expect is at the current edge of research, and Melanie is on the case! In the function field setting, $F \in \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}_\ell)$ gives a good reason that this should have a different distribution when $\ell \mid q-1$, since this is different in the function field case when $\ell \mid q-1$

In future lectures, we'll investigate the following:

(1) Moments, how they are more accessible, when they determine the distribution
(2) How to compute moments in the GL and $\mathrm{GSp}^{(q)}$ cases
(3) Function field theorems (due to JK Yu, Jeff Achter, and others)

Remark 7.16. What about the case when $\ell = p$. This is not at all like the number field case. There is some work of Ellenberg, and Zureick-Brown. They suggest one should really work with the whole p-divisible group scheme and ask about its distribution, not just the distribution of $\mathbb{F}_q$ points.

8. 9/30/20

Remark 8.1. There was a homework problem to find $\#\mathrm{Surj}(\mathbb{Z}_p^n, A)$. We know $\#\mathrm{Hom}(\mathbb{Z}_p^n, A) = |A|^n$. To check $\phi \in \mathrm{Hom}(\mathbb{Z}_p^n, A)$ is a surjection, it is equivalent to check it is a surjection mod p by Nakayama's lemma. So, the question reduces to finding the proportion of homomorphisms which are surjections. That is, if $r = \mathrm{rk}_p A$, we want to find the proportion of $n \times r$ matrices which have rank r, assuming $r < n$. This is $\prod_{i=0}^{r-1}\left(1 - p^{-(n-i)}\right)$ and so

$$\#\mathrm{Surj}\left(\mathbb{Z}_p^n, A\right) = |A|^n \prod_{i=0}^{r-1}\left(1 - p^{-(n-i)}\right).$$

Today, we'll discuss moments of class groups and their relation to counting number fields. Let $\mathscr{F}$ denote a set of number fields and let $I : \mathscr{F} \to \mathbb{R}_{>0}$ denote an invariant, i.e., a map. We will want that there are only finitely many elements of $\mathscr{F}$ with bounded invariant. Define

$$N_{\mathscr{F},I}(X) := \#\{K \in \mathscr{F} : I(K) < X\}.$$

Question 8.2. What are the asymptotics in X of $N_{\mathscr{F},I}(X)$? What families of $\mathscr{F}$ are of most interest?

Usually we will take families of fixed degree and fixed Galois structure. By Galois structure we mean the following: Let $K/\mathbb{Q}$ be a number field and let $\widetilde{K}$ denote the Galois closure of K. Then $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ permutes the embeddings $K \to \widetilde{K}$. Therefore, $\mathrm{Gal}\left(\widetilde{K}/\mathbb{Q}\right)$ can be realized as a permutation group on these embeddings, and it is this permutation group we refer to as the Galois structure.

Here are some further conditions we may want to impose while counting:

(1) Local conditions (like splitting types, ramification). We may want to impose finitely many or impose conditions everywhere (like having a squarefree discriminant).
(2) Fixed class group
(3) Shape (of the lattice of the ring of integers)

Here are some invariants we may want to count by:

(1) Discriminant
(2) The radical of the discriminant (the product of the ramified primes)
(3) Other products of local invariants (like the conductor in the class field theory sense, or the Artin conductor)

Remark 8.3. Malle's conjecture and the Malle-Bhargava principle give a baseline conjecture for many of these counts, but these conjectures are known to be sometimes wrong, so it is more of a guiding principal.

We now want to relate class group moments to counting number fields. Suppose we have

$$\begin{array}{c} H \\ \big\downarrow \mathrm{Cl}_K \\ K \\ \big\downarrow \text{degree 2} \\ \mathbb{Q}. \end{array} \tag{8.1}$$

Let A be a finite odd order abelian group. Then, there is a bijection between surjections $\mathrm{Surj}(\mathrm{Cl}_K, A)$ and

$$\{(L, \phi) : L/K \text{ Galois and unramified over } K, \phi : \mathrm{Gal}(L/K) \simeq A\}.$$

It is crucial here that we specify the isomorphism ϕ, and not just state that one exists.

Question 8.4. Is $L/\mathbb{Q}$ Galois?

It does indeed turn out to be Galois, let's see why.

Proposition 8.5. *$L/\mathbb{Q}$ is Galois.*

Proof. First, $H/\mathbb{Q}$ since the Hilbert Class field is characteristic (so preserved by automorphisms) and therefore the question of $L/\mathbb{Q}$ being Galois boils down to whether $\mathrm{Gal}(H/L)$ is normal in $\mathrm{Gal}(H/\mathbb{Q})$. We have an exact sequence

$$1 \longrightarrow \mathrm{Gal}(H/K) \longrightarrow \mathrm{Gal}(H/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow 1 \tag{8.2}$$

and we want to know if H/L is normal. It is certainly preserved by the conjugation action of the abelian group $\mathrm{Gal}(H/K)$ so we want to know if it is also preserved by the action of $\mathrm{Gal}(K/\mathbb{Q})$ which acts by lifting to an element of $\mathrm{Gal}(H/\mathbb{Q})$ and then conjugating (this is well defined because $\mathrm{Gal}(H/K)$ is abelian, but in general it is only an outer action. So, it suffices to show

Lemma 8.6. $\mathrm{Gal}(H/L)$ *is fixed by the* $\mathrm{Gal}(K/\mathbb{Q})$ *action?*

Proof. To see this, note that from class field theory, we have the Artin map

$$\mathrm{Gal}(H/K) \to \mathrm{Cl}(K)$$

which is equivariant for the action of $\mathrm{Gal}(K/\mathbb{Z})$ on both sides. It is therefore enough to check the subgroup of $\mathrm{Cl}(K)$ corresponding to L is fixed by the $\mathrm{Gal}(K/\mathbb{Q})$ action. However, since this action acts as -1 on the class group, and $\mathrm{Gal}(H/L)$ is a subgroup of $\mathrm{Gal}(H/K)$, it is indeed closed under inversion, and hence fixed by this -1 action. □

Altogether, we have now shown that $L/\mathbb{Q}$ is Galois. □

Let's try to understand more explicitly what $\mathrm{Gal}(L/\mathbb{Q})$ is. We have

$$1 \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow 1. \tag{8.3}$$

We choose isomorphisms $\mathrm{Gal}(L/K) \simeq A$ and $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}$, though there isn't any choice in the latter isomorphism. We are assuming $|A|$ is odd. Therefore by Schur Zassenhaus, the above exact sequence splits and

$$\mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\tau} A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}.$$

Further, again by Schur Zassenhaus, any two such splittings are conjugate and if we choose a different splitting we get a different isomorphism τ. The -1 in the semidirect product indicates that the generator of $\mathbb{Z}/2\mathbb{Z}$ acts by inversion on A.

Remark 8.7. We didn't really need Schur Zassenhaus. There are a number of other ways to see this. One is that there are elements of order 2 in $\mathrm{Gal}(L/\mathbb{Q})$, another is that it has 2-Sylow subgroups. You can also see it from the fact that $H^2(\mathbb{Z}/2\mathbb{Z}, A) = 0$ (which is essentially the proof of Schur Zassenhaus in this case) or by analyzing how inertia acts and how primes ramify.

The above establishes a bijection between

$$\{ (K, \psi, L, \phi) : \psi : \mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}, \phi : \mathrm{Gal}(L/K) \simeq A, \\ L/K \text{ unramified with a choice of splitting } \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})\}$$

and

$$\left\{ (L, \theta) : \theta : \mathrm{Gal}(L/\mathbb{Q}) \simeq A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z} \text{ such that } \mathrm{Gal}(L/L^A) \text{ is unramified.} \right\}$$

Remark 8.8. The above discussion shows that the question of counting $\sum_K \#\mathrm{Surj}(\mathrm{Cl}_K, A)$ is equivalent to counting certain $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ fields where $\mathrm{Gal}(L/L^A)$ is unramified. So, there is no more sum over K in the latter formulation, we are just counting field extensions L which have their own associated fields K.

Question 8.9. When can we count $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ extensions?

Remark 8.10. Essentially all the cases we know how to compute moments of class groups are via counting these extensions.

For $K/\mathbb{Q}$ quadratic, so far we only know the case $A = \mathbb{Z}/3\mathbb{Z}$ when A is odd (and technically $A = \mathrm{id}$). In this case $\mathbb{Z}/3\mathbb{Z} \rtimes_{-1} \mathbb{Z}/2\mathbb{Z} \simeq S_3$.

8.1. **Davenport Heilbronn and counting S_3 extensions.** Counting S_3 extensions is roughly the same as counting non-Galois cubics.

Remark 8.11. In order to get the right count, one needs to be careful about exactly which isomorphism classes of objects one is counting. I.e., you need to be careful about whether you count things like $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$ where the specify the isomorphism or where you don't specify the isomorphism, as they will be off by a factor of 2. In the end, computing this moment is a specific number, and it is important to get the actual value of the moment, not just compute the moment "up to a constant." These constants could come from choices of splittings of exact sequences, or choices of isomorphisms, or choices of conjugate extensions, etc. Of course, just to see whether a problem is doable, one doesn't have to worry about these constants.

Remark 8.12. Cohn counted cyclic cubic fields, which asymptotically account for 0% of cubic extensions by discriminant. We will also see how to approach this on the homework.

Let $N_3(X)$ denote the number of cubic fields with $|\operatorname{disc}_K| < X$.

Theorem 8.13 (Davenport-Heilbronn)**.** *There is a constant $c_3 \in \mathbb{R}$ so that*

$$N_3(X) \sim c_3 X.$$

In other words,

$$\lim_{X\to\infty} \frac{N_3(X)}{X} = c_3.$$

Let's now describe how one can deduce the class group moment from this result. To compute the class group moment, (i.e., the average number of 3-torsion elements in quadratic fields) we need to count nowhere totally ramified cubic fields. In general, this is an infinite collection of conditions on the inertia, with a certain condition at each place.

Let S be a finite set of places and let Σ_p denote a local condition at the prime p (i.e., a specification of what possibilities we allow for the completion of the cubic algebra at p). Define

$$N_{3,(\Sigma_p)_{p\in S}}(X)$$

to be the number of cubic number fields of discriminant at most X whose ring of integers lies in Σ_p at p. Then,

$$N_{3,(\Sigma_p)_{p\in S}}(X) \sim \prod_p \delta(\Sigma_p) c_3 X.$$

One can deduce this fairly easily from the arguments used to prove Theorem 8.13 and the Chinese remainder theorem. Unfortunately, to compute the desired moment, we will need infinitely many conditions, as we want the cubic algebra to be nowhere totally ramified. It follows formally from the above that

$$\limsup_{X\to\infty} \frac{N_{3,(\Sigma_p)_{\text{all } p}}(X)}{X} \leq c_3 \prod_p \delta\left(\Sigma_p\right).$$

However, the reverse inequality is not formal, and requires some more work. Let's see a somewhat contrived example where the reverse inequality would not hold.

Example 8.14. Let $N(X)$ denote the number of positive integers $m \leq X$. Let Σ_p denote the set of m with $p^2 \nmid m$ and $m > p$. For any give p, note that 100% of integers m are $> p$. Then, for any finite set S,

$$N_{(\Sigma_p)_{p\in S}}(X) = \prod_{p\in S} \left(1 - p^{-2}\right) X.$$

However, the set of integers satisfying Σ_p for all primes p is empty, because no integers are larger than all primes.

In general, the further input sufficient to obtain the reverse inequality is the following:

Lemma 8.15. *Suppose* $\frac{N_{(\Sigma_p)_{all\ p}}(X)}{X} \leq c_p$ *with* $\sum_p c_p < \infty$. *Here,* $N_{(\Sigma_p)_{all\ p}}$ *counts number fields satisfying* Σ_p *at all primes* p. *Then,* $N_{(\Sigma_p)_{all\ p}}(X) \sim c\prod_p \delta(p)X$, *for some constant* c *and* $\delta(p)$ *the density of number fields satisfying* Σ_p.

Davenport-Heilbronn proved this when $c_p = \frac{c}{p^2}$, and so this infinite sum certainly converges.

Remark 8.16. The above is quite reminiscent of the dominated convergence theorem. That was about interchanging limits when functions were bounded, and here we are interchanging the limit in X and the infinite product over all primes, which is itself a limit.

Next time, we will see how Datskovsky and Wright proved this, thus relating class group averages to counting number fields. Also, see Tanaguchi-Thorne for an analytic proof of the above results, and Bhargava-Shankar-Tsimerman for a geometry of numbers proof.

9. 10/2/20

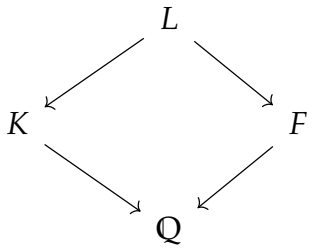
Recall that we are using $N_{3,\overline{\Sigma}_p}(X)$ to denote the number of cubic fields with total ramification p whose discriminant has absolute value at most X.

Goal 9.1. Show $N_{3,\overline{\Sigma}_p}(X) = O(X/p^2)$.

Recall we began discussing this last time, and we saw this was needed in the sieve to count 3-torsion in quadratic fields. Last time, we reduced the question of determining $\mathbb{E}(\#\mathrm{Surj}(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z})$ for K a quadratic field, to counting nowhere totally ramified cubic extensions.

9.1. **Tangent: Why can't we use class field theory to count cubic fields?** Let's take some time to go on a tangent about why we can't use class field theory to count cubic fields. We begin with the setup

(9.1)



where $K/\mathbb{Q}$ is a non-Galois cubic extension, L/K is its Galois closure, $F/\mathbb{Q}$ is a quadratic field, and L/F is a C_3 cyclic Galois extension. For any given F, we can count C_3 extensions of F. However, the issue is we can't easily sum over F. By elementary means, we have an exact sequence

$$1 \longrightarrow \mathscr{O}_F^\times \longrightarrow \prod_v \mathscr{O}_v^\times \longrightarrow \widehat{C}_F \longrightarrow \mathrm{Cl}_F \longrightarrow 1. \tag{9.2}$$

Cutting this off, we get the sequence

$$0 \longrightarrow \prod_v \mathscr{O}_v^\times / \mathscr{O}_F^\times \longrightarrow \widehat{C}_F \longrightarrow \mathrm{Cl}_F \longrightarrow 0 \tag{9.3}$$

We now take hom of this sequence into $\mathbb{Z}/3\mathbb{Z}$ to get

(9.4)

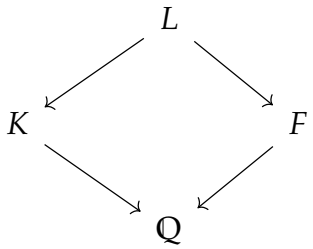
$$0 \longrightarrow \mathrm{Hom}(\mathrm{Cl}_F, \mathbb{Z}/3\mathbb{Z}) \longrightarrow \mathrm{Hom}(\widehat{C}_F, \mathbb{Z}/3\mathbb{Z}) \longrightarrow$$

$$\longrightarrow \mathrm{Hom}(\textstyle\prod_v \mathscr{O}_V^\times / \mathscr{O}_F^\times, \mathbb{Z}/3\mathbb{Z}) \longrightarrow \mathrm{Ext}^1(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z}).$$

We then find that the first and last nonzero terms are identified with $\mathrm{Cl}_K/3\,\mathrm{Cl}_K$ and $\mathrm{Cl}_K[3]$ (which are abstractly isomorphic), the latter follows by computing Ext^1 via the projective resolution $\mathbb{Z} \xrightarrow{\times 3} \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$. Of course, $\mathrm{Hom}(\prod_v \mathscr{O}_V^\times / \mathscr{O}_F^\times, \mathbb{Z}/3\mathbb{Z})$ is typically fairly easy to analyze, but we don't understand the kernel and cokernel of this map very well. In this way, $\mathrm{Cl}_K[3]$ is precisely the obstruction to understanding the number of surjections from $\widehat{C}_F$ onto $\mathbb{Z}/3\mathbb{Z}$.

9.2. **Computing $\mathbb{Z}/3\mathbb{Z}$ moment.** Keeping the setup as in (9.1),

(9.5)



we let $D_K = |\operatorname{disc} K|, D_F = |\operatorname{disc} F|$. Recall now that Davenport Heilbronn counted cubic fields and found the upper bound

$$\sum_{D_F \leq X} |\mathrm{Cl}_F[3]| = O(X).$$

Let $H \subset \widehat{C}_F$ be the index 3 subgroup corresponding to L over F. Let f denote the conductor of L/F.

Fact 9.2. (1) $f \in \mathbb{Z}_{>0}$
(2) f is the product of the primes where $K/\mathbb{Q}$ is totally ramified
(3) $D_K = f^2 D_F$ (which is true when localizing at 2 and 3)

Let $w(f)$ denote the number of prime divisors of f.

Lemma 9.3.

$$\#\left\{H \subset \widehat{C}_F : H \textit{ is closed of index } 3 \textit{ with conductor } f\right\} = O\left(9^{w(f)} \cdot |\operatorname{Cl}_F[3]|\right)$$

Proof. Using the exact sequence, (9.4) we find

$$|\operatorname{Hom}\left(\widehat{C}_F, \mathbb{Z}/3\mathbb{Z}\right)^f| \leq \left|\operatorname{Hom}\left(\operatorname{Cl}_F, \mathbb{Z}/3\mathbb{Z}\right)^f\right| \cdot \left|\operatorname{Hom}\left(\prod_v \mathscr{O}_v^\times, \mathbb{Z}/3\mathbb{Z}\right)^f\right|$$

where the f superscripts indicate that it is those homs corresponding to field extensions of conductor f. It is enough to show

$$\left|\operatorname{Hom}\left(\prod_v \mathscr{O}_v^\times, \mathbb{Z}/3\mathbb{Z}\right)^f\right| = O\left(9^{w(f)}\right).$$

Each prime $p \mid f$ has at most 2 places in F over it. Therefore,

$$\#\operatorname{Hom}\left(\mathscr{O}_v^\times, \mathbb{Z}/3\mathbb{Z}\right) \leq 3$$

except in the cases $v \mid 3$. Indeed, when $v \nmid 3$, then $\mathscr{O}_v^\times$ is the product of the unites in a finite field with an ℓ group where ℓ is the residue characteristic at v. When v does not divide 3, we are then counting $\mathbb{F}_{\ell^k}^\times \to \mathbb{Z}/3\mathbb{Z}$ of which there are at most 3 because this unit group is cyclic. When $v \mid 3$, there may be more homomorphisms, but there are only finitely many degree 2 extensions of $\mathbb{Q}_3$, and hence their number of homs to $\mathbb{Z}/3\mathbb{Z}$ is uniformly bounded, independent of K. Altogether, we indeed obtain

$$\left|\operatorname{Hom}\left(\prod_v \mathscr{O}_v^\times, \mathbb{Z}/3\mathbb{Z}\right)^f\right| = O\left(3^{2w(f)}\right).$$

□

Proposition 9.4. *We have*

$$N_{3,\overline{\Sigma}_p}(X) = O\left(X/p^2\right).$$

Proof. Indeed, we know

$$N_{3,\overline{\Sigma}_p}(X) = O\left(\sum_{f, p \mid f} \sum_{F \text{ quadratic}, D_F \leq X/f^2} 9^{\omega(f)} |\operatorname{Cl}_F[3]|\right)$$

using that $D_K = f^2 D_F$ from our facts above. Simplifying the inner summation, we find

$$\sum_{F \text{ quadratic}, D_F \leq X/f^2} |\mathrm{Cl}_F[3]| = O(X/f^2)$$

as follows from Davenport Heilbronn's theorem on counting cubic fields.

Remark 9.5. It may be confusing at first that we need Davenport-Heilbronn's upper bound in order to obtain the lower bound on counting cubic fields. However, we are using it because we need to upper bound the type of cubic fields we are throwing away.

Now, using this to simplify the sum, we find

$$\begin{aligned} N_{3,\overline{\Sigma}_p}(X) &= O\left(\sum_{f, p|f} \sum_{F \text{ quadratic}, D_F \leq X/f^2} 9^{\omega(f)} |\mathrm{Cl}_F[3]|\right) \\ &= O\left(\sum_m 9^{\omega(m)} \left(\frac{X}{p^2 m^2}\right)\right) \\ &= O\left(\frac{X}{p^2} \sum_{m \geq 1} \frac{9^{\omega(m)}}{m^2}\right). \end{aligned}$$

To conclude, it is enough to show $\sum_m \frac{9^{\omega(m)}}{m^2}$ converges. This holds because

$$\begin{aligned} \sum_{m \geq 1} \frac{9^{\omega(m)}}{m^2} &= \prod_\ell \left(1 + \frac{9}{\ell^2} + \frac{9}{\ell^4} + \cdots\right) \\ &\leq \prod_\ell \left(1 - \frac{9}{\ell^2}\right)^{-1} < \infty. \end{aligned}$$

Since $\prod_\ell \left(1 - \frac{9}{\ell^2}\right) \neq 0$ as $\sum_\ell \frac{9}{\ell^2} < \infty$. □

The moral is that $\sum_F |\mathrm{Cl}_F[3]|$ or $\sum_F \#\mathrm{Surj}\left(\mathrm{Cl}_F, \mathbb{Z}/3\mathbb{Z}\right)$ are both hard to compute, but the difference between Cl_F and $\widehat{C}_F$ is much easier to compute from the exact sequence (9.2). We saw that $\mathbb{E}\left(\#\mathrm{Surj}\left(\mathrm{Cl}_K, A\right)\right)$ was related to counting $A \rtimes \mathbb{Z}/2\mathbb{Z}$ extensions. If $A = \mathbb{Z}/\ell\mathbb{Z}$, then this is related to counting D_ℓ extensions. However, when ℓ is odd, this is only known for $\ell \leq 3$. However, when $\ell > 3$ we can still say something:

Theorem 9.6 (Klüners)**.** *The Cohen-Lenstra conjecture for* $\mathbb{E}\left(\#\mathrm{Surj}\left(\mathrm{Cl}_K, \mathbb{Z}/\ell\mathbb{Z}\right)\right)$ *implies the conjectured upper bound for* D_ℓ *extensions.*

We won't prove this here, but briefly mention the idea: If you know the average of $\mathbb{E}\left(\mathrm{Cl}_F[\ell]\right)$ then you can sum over F and obtain things that are D_ℓ extensions. There are some D_ℓ extensions not corresponding to this, but as in the case $\ell = 3$, there aren't too many others.

Remark 9.7. Further, Klüners also proves the conjectured lower bound on the number of D_ℓ extensions, though for the moment, the conjectured lower bound on $\mathrm{Cl}_F[\ell]$ seems quite out of reach. In other words, although you can deduce upper bounds for D_ℓ extensions and $\mathrm{Cl}_F[\ell]$ from one another, we have no idea ho to deduce a lower bound for the average size of $\mathrm{Cl}_F[\ell]$ from one on D_ℓ.

That is, there are no good lower bounds for $\mathbb{E}\left(\#\mathrm{Surj}\left(\mathrm{Cl}_K, \mathbb{Z}/\ell\mathbb{Z}\right)\right)$ and the lower bound for D_ℓ extensions is not closely tied to class group moments, even though the upper bound is.

Lemma 9.8. *There are at least $O(X)$ D_ℓ extensions.*

Proof. We only give a sketch of his idea. We only need to product on average one D_ℓ extension per quadratic field. For a quadratic field F, if $\mathrm{Cl}_F[\ell]$ *neq*1 then there exists an unramified degree ℓ extension of F, so we get a D_ℓ extension unramified over F. On the other hand, if $\mathrm{Cl}_F[\ell] = 1$ we can use the exact sequence (9.4) to deduce

$$\mathrm{Hom}\left(\widehat{C}_F, \mathbb{Z}/3\mathbb{Z}\right) \simeq \mathrm{Hom}\left(\prod_v \mathscr{O}_v^\times / \mathscr{O}_F^\times, \mathbb{Z}/3\mathbb{Z}\right)$$

and we can then directly count the latter and show it is $O(X)$ as we vary over quadratic fields F of discriminant up to X. □

Next time, we'll discuss moments of random groups. We'll see how moments are often more accessible than the distribution, but how we can often use moments to determine the distribution.

10. 10/7/20

Today we'll discuss moments and random groups. Let X be a random real number.

Definition 10.1. The kth moment of X for k a positive integer is $\mathbb{E}\left(X^k\right)$, the average value of X^k.

Example 10.2. If X takes countably many values then $\mathbb{E}(X^k) = \sum_\lambda \mathrm{Prob}(X = \lambda)\lambda^k$. If X takes values from a probability distribution μ on $\mathbb{R}$ then $\mathbb{E}(X^k) = \int_{\mathbb{R}} x^k d\mu$.

Remark 10.3. If X and Y have the same distribution then $\mathbb{E}(X^k) = \mathbb{E}(Y^k)$.

The moment problem asks whether these moments determine a unique distribution. That is, given $m_1, m_2, \ldots \in \mathbb{R}$ does there exist a unique X (up to having the same distribution) such that for all k, $m_k = \mathbb{E}(X^k)$. In this class, we will focus on uniqueness. The reason for this is that we will want to be able to determine a distribution by its moments. This will let us check some distribution is what we want by just computing its moments, which may be more accessible.

Remark 10.4. Melanie was recently working on a problem where one knows what the moments should be, but doesn't know if there exists a distribution having those moments. So sometimes the existence part of the moment problem is also interesting in arithmetic statistics.

Here is an example of the sort of results we have about a distribution being determined by its moments

Theorem 10.5 (Carleman's condition)**.** *Suppose* $\sum_{n\geq 1} m_{2n}^{-1/2n} = \infty$. *Then uniqueness in the moment problem holds, though not necessarily existence.*

Remark 10.6. The idea is that moments should be relatively small to obtain uniqueness. We want the sum to diverge, and so we want $m_{2n}^{1/2n}$ to be small.

Example 10.7. Suppose $m_{2n} = c$ for some constant c. Then $\sum_n c^{-1/2n}$ diverges because it fails the term test (i.e., the terms to not tend to 0). Therefore, there is at most one distribution with this collection of moments by Carleman's condition.

Example 10.8. Say $m_{2n} = c^{2n}$. Then $\sum_n m_{2n}^{-1/2n} = \sum_n \frac{1}{c} = \infty$. Therefore, there is at most one distribution with this collection of moments.

Example 10.9. Say $m_{2n} = c^{2n^2}$. Then $\sum_n m_{2n}^{-1/2n} = \sum_n c^{-n} < \infty$. Therefore, this fails Carleman's condition, and it is possible there are multiple distributions with this collection of moments.

Remark 10.10. The log normal distribution is a counterexample to the moments problem. That is, the moments $m_n = e^{n^2}$ are moments of more than one distribution.

Remark 10.11. Moments are often more accessible because they satisfy linearity.

Remark 10.12. When we say moments determine a distribution, we mean they determine a measure on the real line, where the measure of $S \subset \mathbb{R}$ is the probability that $X \in S$.

There are two other kinds of moments we will consider: factorial moments and mixed moments.

Definition 10.13. The *factorial moments* of X, denoted $\mathbb{E}((X)_r) := \mathbb{E}\left(X(X-1)\cdots(X-r+1)\right)$, where the right hand side has r factors.

Example 10.14. We have $\mathbb{E}\left((X)_1\right) = \mathbb{E}(X) = \mathbb{E}(X^1)$. Also,

$$\mathbb{E}\left((X)_2\right) = \mathbb{E}\left(X(X-1)\right) = \mathbb{E}(X^2) - \mathbb{E}(X).$$

Remark 10.15. We have that $\mathbb{E}\left((X)_r\right)$ is a precise linear combination of $\mathbb{E}\left(X^1\right), \ldots, \mathbb{E}\left(X^r\right)$.

Remark 10.16. In terms of the moment problem, knowing the factorial moments is equivalent data to knowing the moments. One should just use whichever is easier to work with for the relevant question.

Example 10.17. If X is Poisson with parameter λ then $\mathbb{E}\left((X)_r\right) = \lambda$ for all r while $\mathbb{E}(X^r)$ is some awful polynomial in λ. So in this case, the factorial moments are much nicer. However, for Gaussian distributions, $\mathbb{E}\left(X^r\right)$ are much nicer to work with. If one had some other bijective function f, one could equally well work with $\mathbb{E}\left(f\left(X^k\right)\right)$ instead and use these as your moments.

Definition 10.18. If $X = (X_1, \ldots, X_n) \in \mathbb{R}^n$ then the *mixed moment* indexed by $k_1, \ldots, k_n \in \mathbb{N}^n$ is $\mathbb{E}\left(X_1^{k_1} \cdots X_n^{k_n}\right)$.

10.1. **Moments of random groups.** Now let X be a random group. This could mean a random finite abelian ℓ group, or a random abelian group, or a random group (always drawn from a distribution on isomorphism classes of groups).

Definition 10.19. The *sur moments* are $\mathbb{E}\left(\mathrm{Surj}(X, A)\right)$.

Example 10.20. If X is a random elementary abelian ℓ group (such as $\mathrm{Cl}_K[\ell]$) meaning $X = (\mathbb{Z}/\ell\mathbb{Z})^m$ for some random $m \in \mathbb{N}$, the sur moments are then indexed by $(\mathbb{Z}/\ell\mathbb{Z})^k$. That is, they are given by $\mathbb{E}\left(\#\mathrm{Surj}\left(X, (\mathbb{Z}/\ell\mathbb{Z})^k\right)\right)$.

Remark 10.21. Instead of Sur moments, one can also consider the hom moments $\mathbb{E}\left(\#\mathrm{Hom}\left(X, B\right)\right)$. Hom moments are to sur moments as regular moments are to factorial moments.

Exercise 10.22. We have the following relations between Hom and Sur moments:

$$\#hom\left(X, B\right) = \sum_{A \subset B} \#\mathrm{Surj}(X, A).$$

Find a function $\mu(A, B)$ such that

$$\#\mathrm{Surj}(X, A) = \sum_{B \subset A} \mu(A, B) \#\mathrm{Hom}(X, B).$$

This μ is a type of mobius inversion.

As with the case of regular moments and factorial moments, we just use whichever of hom or sur moments are simpler.

Question 10.23. Why would we call these hom and sur functions the moments?

We have

$$\mathrm{Hom}\left(\left(\mathbb{Z}/\ell\mathbb{Z}\right)^m, \left(\mathbb{Z}/\ell\mathbb{Z}\right)^k\right) = \left(\ell^m\right)^k.$$

Therefore, for X an elementary abelian ℓ group,

$$\#\mathrm{Hom}\left(X, \left(\mathbb{Z}/\ell\mathbb{Z}\right)^k\right) = |X|^k.$$

Therefore, we conclude the following.

Lemma 10.24.

$$We have \mathbb{E}\left(\#\mathrm{Hom}\left(X, \left(\mathbb{Z}/\ell\mathbb{Z}\right)^k\right)\right) = \mathbb{E}\left(|X|^k\right).$$

More generally, we can describe moments for finite abelian ℓ groups. Suppose λ is a partition with λ given by $\lambda_1 \geq \lambda_2 \geq \cdots \geq 0$ with $\lambda_i \in \mathbb{Z}_{\geq 0}$. Let λ' denote the conjugate partition, so that when drawn as a young diagram it is the transpose of λ. Explicitly, $\lambda_i' = \#\left\{j : \lambda_j \geq i\right\}$. Let $G_\lambda := \oplus_i \mathbb{Z}/\ell^{\lambda_i}\mathbb{Z}$.

Exercise 10.25. Show

$$\#\mathrm{Hom}\left(G_\lambda, G_\mu\right) = \ell^{\sum_i \lambda_i' \mu_i'}.$$

If $F_{\lambda'} = G_\lambda$, we get

$$\#\mathrm{Hom}\left(F_\lambda, F_\mu\right) = \left(\ell^{\lambda_1}\right)^{\mu_1}\left(\ell^{\lambda_2}\right)^{\mu_2}\cdots.$$

Here, we see these averages are mixed moments of $\ell^{\lambda_1}, \ell^{\lambda_2}, \cdots$. This is actually a little different than the mixed moments because we could have an infinite sequence of λ_i.

Remark 10.26. Let the dual group $A^\vee := \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ for A a finite abelian group. Then, $A \simeq \left(A^\vee\right)^\vee$ so

$$\mathrm{Hom}\left(A, B\right) \simeq \mathrm{Hom}(B^\vee, A^\vee).$$

Unnaturally, by working out duals of finite abelian groups, we find $A \simeq A^\vee$. This is analogous to the way a finite dimensional vector space is isomorphic to its dual, but not in a natural way.

Using this, we have

$$\mathrm{Hom}(A, B) \simeq \mathrm{Hom}(B^\vee, A^\vee) \simeq \mathrm{Hom}(B, A),$$

We find that always $\mathrm{Surj}(X, B) \simeq \mathrm{Inj}(B^\vee, X^\vee)$. and this has the same size as $\mathrm{Inj}(B, X)$.

Question 10.27. Why do we work with Hom and Surj moments?

If we encode $(\mathbb{Z}/\ell\mathbb{Z})^k$ As k as opposed to ℓ^k then these are not literally the moments. Though if we encode these as ℓ^k we do obtain the usual moments from Hom, as mentioned above. The only theorem we have on these objects is due to Davenport and Heilbronn, which computes

$$\mathbb{E}\left(\#\mathrm{Surj}\left(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z}\right)\right), \mathbb{E}\left(\#\mathrm{Hom}\left(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z}\right)\right), \mathbb{E}\left(\mathrm{Cl}_K[3]\right).$$

However, it does not compute $\mathbb{E}\left(\mathrm{rk}_3(\mathrm{Cl}_K)\right)$.

Remark 10.28. In the function field analog over $\mathbb{F}_q(t)$, there are many theorems about taking a $q \to \infty$ limit calculating $\mathbb{E}\left(\#\mathrm{Surj}\left(\mathrm{Cl}_K, A\right)\right)$ for all A. We will discuss this more in future classes.

Remark 10.29. Empirically, $\mathbb{E}\left(\#\mathrm{Surj}\left(\mathrm{Cl}_K, A\right)\right)$ converge in X (the discriminant of K) much faster than $\mathrm{Prob}(X \simeq A)$ converges.

Remark 10.30. On the random group side, these moments are also nice. As noted in homework 3, if $X = \mathrm{coker}\, M$ for M a random $n \times n$ matrix with entries in $\mathbb{Z}_\ell$ distributed according to Haar measure, we have

$$\mathbb{E}\left(\#\mathrm{Surj}(X, A)\right) = \sum_{f \in \mathrm{Surj}\left(\mathbb{Z}_\ell^n, A\right)} \mathrm{Prob}\left(f\left(M\mathbb{Z}_\ell^n\right) = 0\right) = \frac{\#\mathrm{Surj}\left(\mathbb{Z}_\ell^n, A\right)}{|A|^n} \to_{n\to\infty} 1.$$

We saw as a corollary, using the monotone convergence theorem:

Corollary 10.31. *If X is the Cohen-Lenstra distribution for imaginary quadratic fields i.e.,* $\mathrm{Prob}(X \simeq A) = \frac{c}{|\mathrm{Aut}(A)|}$, *then* $\mathbb{E}\left(\#\mathrm{Surj}(X, A)\right) = 1$. *Therefore, we must have picked the correct moments for this problem.*

Next time, we will discuss random group models and the uniqueness of the moments problem.

11. 10/9/20

Today we'll discuss moments of random groups.

Example 11.1. Take X from $\mathrm{Prob}\left(X \simeq A\right) = \frac{c}{|A|^u |\mathrm{Aut}(A)|}$ for $u \geq 0$ an integer. (One can also consider non integer u, but it rarely comes up, except sometimes $u = 1/2$.) We calculated $\mathbb{E}\left(\#\mathrm{Surj}\left(X, A\right)\right) = \frac{1}{|A|^u}$.

Example 11.2. Take X_n to be the cokernel of a symmetric random matrix from $\mathrm{Sym}_{n\times n}(\mathbb{Z}_\ell)$. The Haar measure is given by collections of $\mathbb{Z}_\ell$ Haar random elements to fill in the upper triangular part of the matrix. One then fills in the lower triangular part to make the matrix symmetric. This is not the definition of Haar measure, but one can check this measure is a Haar measure because it is translation invariant. On the homework we found

$$\lim_{n\to\infty} \mathbb{E}\left(\#\mathrm{Surj}\left(X_n, A\right)\right) = \left|\wedge^2 A\right| = A\otimes A/\langle a\otimes a\rangle_{a\in A}.$$

For example, when $A = (\mathbb{Z}/\ell\mathbb{Z})^k$ we have $|\wedge^2 A| = \ell^{\frac{k(k-1)}{2}}$.

Example 11.3. Take X_n to be Haar random matrix from $\mathrm{Alt}_{n\times n}(\mathbb{Z}_\ell)$. Then it turns out

$$\lim_{n\to\infty} \mathbb{E}\left(\#\mathrm{Surj}\left(X_n, A\right)\right) = \left|\mathrm{Sym}^2 A\right|.$$

So, for example $A = (\mathbb{Z}/\ell\mathbb{Z})^k$ then $|\mathrm{Sym}^2 A| = \ell^{\frac{k(k+1)}{2}}$.

In principle, these moments wouldn't have to be so nice. But perhaps it's not so surprising that these very natural distributions have nice moments.

We'll next do a more involved example.

11.1. **Analyzing cokernels of $1-g$ for g from a coset of the general symplectic group.** Consider $F \in \mathrm{GSp}_{2n}^{(q)}(\mathbb{Z}_\ell)$ a Haar random matrix. Recall that in the function field case, with respect to the Weil pairing, we had $\mathrm{Frob} \in \mathrm{GSp}_{2n}^{(q)}(\mathbb{Z}_\ell)$. That is, for W an alternating perfect pairing we have

$$\phi \in \mathrm{GSp}_{2n}^{(q)}(\mathbb{Z}_\ell) \iff W\left(\phi(x), \phi(y)\right) = qW(x,y).$$

This may not be the most natural matrix group one would come up with, but we saw that in the function field case, Frobenius acts in this way on the Weil pairing.

When we say Haar random above, we must note that $\mathrm{GSp}_{2n}^{(q)}(\mathbb{Z}_\ell)$ is not actually a group, but rather a coset of $\mathrm{Sp}_{2n}(\mathbb{Z}_\ell)$. The latter has a Haar measure, so we can just translate it by any element of $\mathrm{GSp}_{2n}^{(q)}(\mathbb{Z}_\ell)$ to get a measure on $\mathrm{GSp}_{2n}^{(q)}(\mathbb{Z}_\ell)$. And this resulting measure is independent of choice of element because we started with a Haar measure on $\mathrm{Sp}_{2n}(\mathbb{Z}_\ell)$. Note that this Haar measure is just the uniform measure $\bmod \ell^k$ for each k.

We then considered the random variable $X = \mathrm{coker}\left(1-F\right)$. On this divisible group, the class group is the kernel of $1-F$, but on the Tate module, we can identify Pic^0 in the function field case with the cokernel of $1-F$ on the Tate module.

We will now analyze the moments of this model. This will take us some time in this class, in the overall scope of things, this is relatively easy.

As usual, we can use linearity of expectation to write these moments as a sum over surjections $\mathbb{Z}_\ell^{2n} \to A$.

$$\mathbb{E}\left(\#\operatorname{Surj}(X, A)\right) = \sum_{f \in \operatorname{Surj}\left(\mathbb{Z}_\ell^{2n} \to A\right)} \mathbb{P}\left(f\left((1-F)\,\mathbb{Z}_\ell^{2n}\right) = 0\right)$$

Then,

$$f \circ (1-F) = 0 \iff f = fF.$$

Here, $\mathrm{GSp}_{2n}(\mathbb{Z}_\ell)$ is acting on the surjections $\operatorname{Surj}\left(\mathbb{Z}_\ell^{2n}, A\right)$. Therefore, the above says that f is a fixed point of the above action. Hence, we want to determine the expected number of fixed points is.

So, we want to find the number of fixed points of this action. To this end, we'll recall a general fact about the expected number of fixed points.

Fact 11.4. The spirit of this fact is that the expect number of fixed points is the number of orbits. Let's now be more precise.

Let G be a group with a Haar probability measure acting on a finite set S. Let $g \in G$ be a random element drawn from Haar measure. Let $s \in S$. What is the probability that g fixes s?

$$\operatorname{Prob}(gs = s) = \operatorname{Prob}\left(g \in \operatorname{Stab} s\right)$$

Note that $\operatorname{Stab} s \subset G$ is a subgroup and we can partition $G = \cup_{\tau_i} \tau_i \operatorname{Stab} s$ for τ_i representatives of cosets for $\operatorname{Stab} s$ in G. Then, since there are $\#\operatorname{Orbit} s$ many such cosets, we have

$$\operatorname{Prob}(gs = s) = \operatorname{Prob}\left(g \in \operatorname{Stab} s\right) = \frac{1}{\#\operatorname{Orbit} s}.$$

Therefore,

$$\mathbb{E}\left(\#s \in S \text{ fixed by } g\right) = \sum_s \frac{1}{\#\operatorname{Orbit} s} = \#\left(\text{orbits of } G \text{ on } S\right).$$

To be really precise, we will need to work with closed subgroups and have some compatibility between the sigma algebra we are working with on G and the measure on S. But for now we'll just sweep these issues under the rug, but remain aware that they exist.

Now, let G and S as be as above and let $H \subset G$ a subgroup. Fix $g_0 \in G$. We would like to understand

$$\mu_{\mathrm{Haar}, g_0 H}(\operatorname{Stab} s \cap g_0 H) := \mu_{\mathrm{Haar}, H}(g_0^{-1} \operatorname{Stab} s \cap H).$$

Let $s' = g_0^{-1} s$. Then $g_0^{-1} \operatorname{Stab} s$ correspond to elements that take s to s'.

Lemma 11.5. *We have*

$$\mathbb{E}\left(\#\left(\text{ fixed points of } g_0 h \in S\right)\right) = \#\left(\text{ orbits of } H \text{ on } S \text{ that are fixed by } g_0\right).$$

Proof. There are two cases.

(1) If there exists $h \in H$ with $hs = s'$ then $g_0^{-1} \operatorname{Stab} s = h \operatorname{Stab} s$. In this case,
$$\mu\left(h \operatorname{Stab} s \cap H\right) = \mu\left(\operatorname{Stab} s \cap H\right) = \frac{1}{\#\operatorname{Orbit}_H s}.$$
(2) If there is no $h \in H$ with $hs = s'$ then
$$g_0^{-1} \operatorname{Stab} s \cap H = \emptyset.$$

Therefore, the second case does not contribute, and if we add up the first case as above, we obtain the lemma. □

Using the above lemma, we find

$$\begin{aligned}
&\mathbb{E}\left(\#\operatorname{Surj}\left(\operatorname{coker}\left(1-F\right), A\right)\right) \\
&= \mathbb{E}\left(\#F \text{ fixed } \operatorname{Surj}\left(\mathbb{Z}_\ell^{2n}, A\right)\right) \\
&= \#\left(\text{ orbits of } \operatorname{Sp}_{2n}(\mathbb{Z}_\ell) \text{ on } \operatorname{Surj}\left(\mathbb{Z}_\ell^{2n}, A\right) \text{ fixed by } g_0 \in \mathrm{GSp}^{(q)}\right).
\end{aligned}$$

The first equality holds because $\phi \in \operatorname{Surj}\left(\operatorname{coker}(1-F), A\right) = \mathbb{Z}_\ell^{2n}/(1-F)\mathbb{Z}_\ell^{2n}$ if and only if $\phi \in \operatorname{Surj}\left(\mathbb{Z}_\ell^{2n}, A\right)$ with $\phi(1-F) = 0 \iff \phi = \phi F$.

So, we want to understand the following question.

Question 11.6. What are the orbits of $\operatorname{Sp}_{2n}(\mathbb{Z}_\ell)$ on $\operatorname{Surj}\left(\mathbb{Z}_\ell^{2n}, A\right)$.

As a preliminary question we have the following:

Question 11.7. What are the orbits of $\mathrm{GL}_n(\mathbb{Z}_\ell)$ on $\operatorname{Surj}\left(\mathbb{Z}_\ell^{2n}, A\right)$?

For this latter question, there is only a single orbit because for any two such surjections, we can change basis to go from one to the other. We can rephrase this as follows.

Corollary 11.8. *We have*

$$\mathbb{E}\left(\#\operatorname{Surj}\left(\operatorname{coker}\left(1-G\right), A\right)\right) = 1$$

whenever $n \geq \mathrm{rk}_\ell A$ *for* G *Haar random from* $\mathrm{GL}_n(\mathbb{Z}_\ell)$.

Note that this recovers the Cohen-Lenstra distribution as all moments are 1.

Note that the moments above are 0 for groups A not generated by n elements.

We can now wonder whether there will only be a single orbit of the symplectic group, or whether the orbits from GL split into multiple orbits. There will in fact be a certain invariant that is preserved, which we will now discuss. Let $V = \mathbb{Z}_\ell^{2n}$. We can choose $W \in V \otimes V$ thought of as an alternating element.

Remark 11.9. Strictly speaking, $W \in V \otimes V \to \mathbb{Z}_\ell$, and this is a perfect pairing yielding an isomorphism $V \simeq V^\vee$, so we obtain an element of $V^\vee \otimes V^\vee \to \mathbb{Z}_\ell$, or equivalently an element of $V \otimes V$.

Now for $f : V \to A$ we get a map $V \otimes V \to A \otimes A$.
This construction then gives a map

$$\mathrm{Surj}\,(V, A) \to A \otimes A$$

by sending f to the evaluation of $f \otimes f$ on $W \in V \otimes V$. Because W is alternating, the image lands in alternating elements. By alternating elements, we mean the subgroup of $A \otimes A$ generated by $x \otimes y - y \otimes x$. If $\phi \in \mathrm{Sp}(V)$, then $(\phi \otimes \phi)(W) = W$. Therefore, the above map $\mathrm{Surj}(V, A) \to A \otimes A$ is constant on $\mathrm{Sp}(V)$ orbits. Hence, we have an orbit invariant

$$\wedge_2 A \subset A \otimes A$$

which we define as the alternating elements of $A \otimes A$. It turns out that there is an isomorphism $\wedge_2 A \simeq \wedge^2 A$ given by

$$\begin{aligned} \wedge_2 A &\to \wedge^2 A \\ x \otimes y - y \otimes x &\mapsto x \wedge y. \end{aligned}$$

Proposition 11.10. *This invariant exactly distinguishes orbits.*

We omit the proof. This is somewhat like the proof that there is one isomorphism class of symplectic form. You can prove this concretely by choosing bases and changing one to the other.

Corollary 11.11. *We have*

$$\mathbb{E}\left(\#\,\mathrm{Surj}\,(1 - \mathrm{coker}\,G, A)\right) = \left|\wedge^2 A\right|$$

for $2n \geq \mathrm{rk}_\ell\, A$ (so that there are some surjections).

Remark 11.12. These are the same moments as if one takes the cokernel of a symmetric matrix, even though $1 - G$ for G symplectic is not a symmetric matrix.

We wanted to know about the orbits of $\mathrm{Sp}(V)$ fixed by an element of $\mathrm{GSp}^{(q)}$. We have $g_0 \in \mathrm{GSp}^{(q)}$ exactly when $g_0 \otimes g_0(W) = qW$.

So, the orbits fixed by g_0 are exactly in bijection with the elements of $\wedge^2 A$ fixed by q.

That is, they are in bijection with $b \in \wedge^2 A$ such that $qb = b$. In other words, we have $b \in \wedge^2 A[q-1]$.

Corollary 11.13. *We have*

$$\mathbb{E}\left(\#\mathrm{Surj}\left(1-G, A\right)\right) = \left|\wedge^2 A\left[q-1\right]\right|$$

when $2n \geq \mathrm{rk}_\ell A$. *If* $\ell \nmid q-1$, *this is* 1.

12. 10/14/20

We have several random matrix models with

$$\lim_{n\to\infty} \mathbb{E}\left(\#\mathrm{Surj}\left(\mathrm{coker}\left(M_n, A\right)\right)\right) = 1$$

for all A finite abelian ℓ-groups.

(1) We can take $M_n \in M_{n\times n}(\mathbb{Z}_\ell)$ Haar random
(2) We can take $M_n \in I - \mathrm{GSp}_{2n}^{(q)}(\mathbb{Z}_\ell)$ Haar random when $\ell \nmid q-1$.
(3) We can take $M_n \in M_{n\times n}(\mathbb{Z}_\ell)$ with independent entries not too concentrated.
(4) We can take $M_n \in I - \mathrm{GL}_n(\mathbb{Z}_\ell)$ Haar random.

Note that the differences between these models is not completely trivial. For example, there are many matrices (and even a locus with positive measure) that arise in the first case but do not arise in the last. Even though we have quite different sets of matrices, their cokernels do have the same moments. This brings us back to the moment question:

Question 12.1. Is $\mathrm{coker}\, M_n$ as $n \to \infty$ the same distribution for the above models?

We'll ignore analytic issues relating to the limit $n \to \infty$. We want to understand:

Question 12.2. If X is a random finite abelian ℓ-group with $\mathbb{E}\left(\#\mathrm{Surj}\left(X, A\right)\right) = 1$ for all finite abelian ℓ groups, is $\mathbb{P}\left(X \simeq A\right) = \frac{c}{|\mathrm{Aut}\, A|}$?

For simplicity, let's stick with elementary ℓ groups to start. That is, we replace X by $X/\ell X$. We have

$$\#\mathrm{Surj}\left(X, (\mathbb{Z}/\ell\mathbb{Z})^k\right) = \#\mathrm{Surj}\left(X/\ell X, (\mathbb{Z}/\ell\mathbb{Z})^k\right).$$

Recall, for X a random elementary ℓ-group,

$$\mathbb{E}\left(\#\mathrm{Hom}\left(X,(\mathbb{Z}/\ell\mathbb{Z})^k\right)\right)=\mathbb{E}\left(|X|^k\right).$$

If $\mathbb{E}\left(\#\mathrm{Surj}\left(X,A\right)\right)=1$ for all A, then

$$\mathbb{E}\left(\#\mathrm{Hom}\left(X,A\right)\right)=\#\text{subgroups of A.}$$

This number of subgroups are counted by q-binomial coefficients. That is, $\mathbb{E}\left(|X|^k\right)$ is the number of subspaces of $(\mathbb{Z}/\ell\mathbb{Z})^k$. These are most concentrated in the middle, just like for the usual binomial coefficients.

Example 12.3. How many dimension $k/2$ subspaces of $(\mathbb{Z}/\ell\mathbb{Z})^k$ are there? We can count these by looking at $(k/2)\times k$ matrices, which is $q^{k^2/2}\left(1-q^{-k}\right)\left(1-q^{-(k-1)}\right)\cdots$ and then divide by $\#\mathrm{GL}_{k/2}\left(\mathbb{Z}/\ell\mathbb{Z}\right)=\ell^{k^2/4}(1-\ell^{-k})\cdots$. This ration is approximately $\ell^{k^2/4}$.

Unfortunately, this is precisely too big to apply Carleman's condition for the moments to determine the distribution.

In fact, it is not just that Carleman's condition fails, but moreover, there are random real numbers $Y\in\mathbb{R}$ with different distributions such that $\mathbb{E}\left(Y^k\right)$ equal to the number of subspaces of $(\mathbb{Z}/\ell\mathbb{Z})^k$.

Does this mean we are doomed in our moments problem? Does that necessarily mean there are multiple different distributions of elementary abelian ℓ-groups with number of surjections 1?

We can observe that our distributions are necessarily supported on powers of ℓ. This gives some more constraints, so we are not necessarily doomed. In fact, we can rephrase this question as a linear algebra problem:

Choose a random $n\in\mathbb{Z}_{\geq 0}$ such that

$$\mathbb{E}\left(\#\mathrm{Surj}\left(\mathbb{F}_{\ell}{}^n,\mathbb{F}_{\ell}{}^k\right)\right)=1.$$

We can write the left hand side as

$$\sum_{a\geq 0}\mathrm{Prob}\left(n=a\right)\#\mathrm{Surj}\left(\mathbb{F}_{\ell}{}^a,\mathbb{F}_{\ell}{}^k\right).$$

We can express our conditions as follows. Let

$$M:=\begin{pmatrix}m_{00} & m_{01} & \cdots\\ m_{10} & m_{11} & \cdots\\ \vdots & \vdots & \ddots\end{pmatrix}$$

in $\mathbb{R}^{\mathbb{N}\times\mathbb{N}}$ and

$$b := \begin{pmatrix} b_0 \\ b_1 \\ \cdots \end{pmatrix}$$

in $\mathbb{R}^{\mathbb{N}}$. Given M and b, is there a unique x such that $Mx = b$.

Warning 12.4. We have to beware of two things:

(1) First, Mx or MN (for $x \in \mathbb{R}^{\mathbb{N}}$, $N \in \mathbb{R}^{\mathbb{N}\times\mathbb{N}}$) may not exist, because the products may not have finite entries.
(2) Even if these products exist, $M(NP)$ may not equal $(MN)P$ because we may not be able to change the order of summation in infinite sums.

We will have to deal with these difficulties. Suppose we are in a case where M is invertible. That is, there exists $N \in \mathbb{R}^{\mathbb{N}\times\mathbb{N}}$ such that $NM = MN = \mathrm{id}$. If all of

(1) Nb exists
(2) $M(Nb)$ exists
(3) $(MN)b = M(Nb)$

then xNb is a solution to $Mx = b$.

So this would give existence. But what about uniqueness (which is what we were primarily interested in)?

If all of

(1) $Mx = b$ is a solution
(2) Nb exists
(3) $(NM)x = N(Mx)$

then $x = Nb$, so we would have uniqueness.

In summary, for M invertible, for "small enough" b, there exists a solution. By small enough, we mean

$$\sum_k |N_{jk}||b_k| < \infty, \sum_{j,k} |M_{ij}||N_{jk}||b_k| < \infty.$$

The absolute convergence is used to exchange the order of summation.

In general, there may not be uniqueness, since if $Mx_1 = Mx_2 = b$, for b not small, then subtracting $M(x_1 - x_2) = 0$ and if $Mx = b$ implies $M(x + x_1 - x_2) = b$. Instead of asking for uniqueness in terms of b, we could ask for uniqueness of small solutions. That is:

Definition 12.5. Say x is small if

$$\sum_k |N_{jk}||x_k| < \infty, \sum_{j,k} |M_{ij}||N_{jk}||x_k| < \infty.$$

which guarantees $Mx = b$ and $(NM)x = N(Mx)$.

Then, by the definition of smallness, we have uniqueness of small solutions.

Let's now return to our problem at hand. A summary of the above discussion is:

Lemma 12.6. *If M is invertible, we have uniqueness of small solutions.*

This leads us to ask:

Question 12.7. Is our matrix M invertible?

Our matrix M is upper triangular because

$$\#\text{Surj}\left(\mathbb{F}_\ell{}^n, \mathbb{F}_\ell{}^k\right) = 0 \text{ if } n < k$$

We get equations of the form

$$\begin{array}{lll} m_{00}x_0 + m_{01}x_1 & +m_{02}x_2 + \cdots & = b_0 \\ m_{11}x_1 & +m_{12}x_2 + \cdots & = b_0 \end{array}$$

Remark 12.8. If the matrix were instead lower triangular $m_{00}x_0 = b_0, m_{10}x_0 + m_{11}x_1 = b_1$. Equations of this form are easy to solve if $m_{ii} \neq 0$ since we can recursively solve the equations. Unfortunately, we have upper triangular matrices, not lower triangular matrices, so we will have to work harder.

Let's assume $m_{ii} \neq 0$ so that our matrix has a chance of being invertible. We can scale each row to assume $m_{ii} = 1$.

Proposition 12.9. *For M upper triangular with all $m_{ii} = 1$ there exists a matrix N such that $NM = MN = 1$.*

Proof. We can take $N = 1 + (1 - M) + (1 - M)^2 + (1 - M)^3 + \cdots$. We need to check this exists. But any matrix times an upper triangular matrix exists because the entry sums are all finite sums. Since $(1 - M)$ is upper triangular, we can take arbitrary powers of it. We next check the infinite sum exists. Observe $1 - M$ is strictly upper triangular. This implies $(1 - M)^n$ is n-strictly upper triangular, meaning the i, j entry is 0 whenever (i, j) is n steps above the diagonal. That is $j \geq i + n$. So, each entries only sees finitely many summands.

To conclude, we want to see $NM = MN = \text{id}$. One can multiply and telescope the sum, using the above idea that each entry sees only finitely many summands. □

Corollary 12.10. *For our matrix M given by*

$$M_{ij} = \frac{\#\mathrm{Surj}\left(\mathbb{F}_\ell{}^j, \mathbb{F}_\ell{}^i\right)}{\#\mathrm{Surj}\left(\mathbb{F}_\ell{}^i, \mathbb{F}_\ell{}^i\right)}$$

we have invertibility of this matrix, so we do obtain uniqueness of small solutions.

We wanted uniqueness of non-negative solutions x, i.e., solutions with $x_k \geq 0$, because we wanted probability distributions. Fortunately, we have the following lemma.

Lemma 12.11. *When M is invertible with non-negative entries, for small enough b, we have uniqueness of non-negative solutions.*

Proof. Since our $M_{ij} \geq 0$, if b is our unique small solution, and x is our given positive solution with all $x_k \geq 0$, then we find $|x_k| \leq b_k$ and so x is in fact small.

Therefore, when there is a small solution b, nonnegative solutions have to be small solutions. □

Already, this may help us understand morally what is going on with the moment problem. When moments are small, we expect there exist solutions, and in the space of nonnegative solutions, that they are unique. However, when moments are big, the solutions may not be unique.

Question 12.12. What exactly is small enough?

Of course, the answer to the above question depends on M. A priori, it may also depend on $N = M^{-1}$, but in our upper triangular case N is described in terms of M as $1 + (1 - M) + (1 - M)^2 + \cdots$. The condition of being small is of the form $\sum_k c_k |b_k| < \infty$ where the c_k are non-negative coefficients given as a function of M.

Let c_A denote the scaled version of the b_A, where we take M to be the matrix

$$M_{ij} = \frac{\#\mathrm{Surj}\left(\mathbb{F}_\ell{}^j, \mathbb{F}_\ell{}^i\right)}{\#\mathrm{Surj}\left(\mathbb{F}_\ell{}^i, \mathbb{F}_\ell{}^i\right)}$$

Suppose we started with a matrix $Sx = d$ for $S_{ij} = \#\mathrm{Surj}\left(\mathbb{F}_\ell{}^j, \mathbb{F}_\ell{}^i\right)$. Let M be the normalized matrix $Mx = b$ with $M_{ij} = \frac{\#\mathrm{Surj}\left(\mathbb{F}_\ell{}^j, \mathbb{F}_\ell{}^i\right)}{\#\mathrm{Surj}\left(\mathbb{F}_\ell{}^i, \mathbb{F}_\ell{}^j\right)}$. Then

Theorem 12.13 (Wood, paper on sandpile groups)**.** *There is at most one distribution on random elementary ℓ-groups such that $\mathbb{E}\left(\#\mathrm{Surj}\left(X, A\right)\right) = d_A$ for $|d_A| = O\left(\wedge^2 A\right)$. That is, when $A = \#\mathbb{F}_\ell{}^k$, $|d_k| = O\left(\ell^{\frac{k(k-1)}{2}}\right)$, or equivalently when $b_k = O\left(\ell^{\frac{-k(k+1)}{2}}\right)$.*

In our case, our #Surj moments are 1, so $d_k = 1$ and the above theorem definitely applies.

Remark 12.14. Heath-Brown and Fouvry-Klüners have proven slightly weaker versions of this requiring stricter smallness hypotheses.

Next time, we'll discuss distributions on finite abelian ℓ groups where the moments are a little bigger than this, and there are multiple different (even natural and important) distributions. However, the Cohen-Lenstra distribution does satisfy the above theorem as the moments there are 1. This means, we expect that all the distributions of matrices from the beginning of class have the same cokernel distribution. However, we still have to address one issue: how does all this interact with the analytic issue of taking a limit in n.

13. 10/21/20

Let's review where we were. We were discussing the moment problem. We found several different distributions of matrices whose cokernels all had the same moments.

Theorem 13.1. *If X and Y are random finite abelian groups so that for all finite abelian groups A,*

$$\mathbb{E}\left(\#\mathrm{Surj}(X,A)\right) = \mathbb{E}\left(\#\mathrm{Surj}(Y,A)\right) \leq \left|\wedge^2 A\right|$$

then X and Y have the same distribution.

In particular, this applies to the case that all the Surj moments are 1. Note that the classical (Hom) moments are too big to apply the classical probability theorem. But, we can still apply the above theorem to conclude the distribution was uniquely determined.

Remark 13.2. We can extend the above theorem to profinite abelian groups with finite Sylow-p subgroups. That is, groups of the form $\prod_p G_p$ where each G_p is a finite abelian p-group.

We saw a few cases where this holds:

(1) X is the $\frac{c}{|\#\operatorname{Aut} A|}$ distribution which has $\mathbb{E}\left(\#\mathrm{Surj}(X,A)\right) = 1$
(2) X is the $\frac{|c|}{|A||\#\operatorname{Aut} A|}$ distribution we have $\mathbb{E}\left(\#\mathrm{Surj}(X,A)\right) = \frac{1}{|A|}$.
(3) Take $X_n = \operatorname{coker} S_n$ for $S_n \in \mathrm{Sym}_{n\times n}(\mathbb{Z}_\ell)$ Haar random, has $\lim_{n\to\infty} X_n$ has moments $|\wedge^2 A|$.
(4) Take $X_n = \operatorname{coker}(1 - G_n)$ for $G_n \in \mathrm{GSp}_{2n}^{(q)}(\mathbb{Z}_\ell)$ Haar random. This has Ath moment tending to $\left|\wedge^2 A[q-1]\right|$. When $q = 1$, this corresponds to $\mathrm{Sp}_{2n}(\mathbb{Z}_\ell)$ which has Ath moment $\left|\wedge^2 A\right|$.

Note the last two only agree in the limit $n \to \infty$. Symmetric matrices have Ath moment

$$\frac{\#\operatorname{Surj}\left(\mathbb{Z}_\ell^n, A\right)}{|A|^n}\left|\wedge^2 A\right|$$

while cokernels of id $-G$ for G symplectic has moments $\left|\wedge^2 A\right|$ as n is large, though it approaches it from below along integer values, since it is counting orbits.

Remark 13.3. We might expect symmetric matrices to have bigger moments. Indeed, when there are more entries divisible by ℓ there will tend to be larger cokernels. For symmetric matrices, when there is a single entry divisible by ℓ, there is necessarily another entry divisible by ℓ. So this tends to increase the moments.

From another perspective, we can identify the moments with orbits. Because the symplectic group is smaller than the general linear group, we expect there to be more orbits.

Now we will discuss what happens just past the bound, and then discuss how to deal with the $n \to \infty$ limit.

13.1. **Going past the bound.** Let $A_n \in \operatorname{Alt}_{n\times n}(\mathbb{Z}_\ell)$ to be a Haar random skew symmetric matrix.

Remark 13.4. Note that skew symmetric matrices do not depend on a choice of basis because skew symmetry can be expressed as saying $x \otimes x \mapsto 0$ which can be viewed as a map $\mathbb{Z}_\ell^n \otimes \mathbb{Z}_\ell^n \to \mathbb{Z}_\ell$ after choosing a basis.

Let's outline how to compute the moments of coker A_n.

(1) The moments can be described as

$$\sum_{f \in \operatorname{Surj}(\mathbb{Z}_\ell^n, A)} \operatorname{Prob}\left(f(A_n) = 0\right).$$

(2) Choose a basis for $\ker f$ of the form

$$\ker f = \begin{pmatrix} (\ell)^{a_1} \\ (\ell)^{a_2} \\ (\ell)^{a_3} \\ \vdots \end{pmatrix} \subset \mathbb{Z}_\ell^n$$

with $a_1 \geq a_2 \geq \cdots$. Note that Haar measure is the same as picking upper triangular entries independently from the Haar measure for $\mathbb{Z}_\ell$.

(3) Then Prob $(f(A_n) = 0)$ occurs with probability

$$\begin{aligned}&\left(\ell^{a_1}\right)^n \left(\ell^{-a_2}\right)^n \cdots \left(\ell^{-a_n}\right)^n \cdots \ell^{a_1}\ell^{2a_2}\ell^{3a_3}\\ &= \left(\ell^{-a_1}\right)^{n-1} \left(\ell^{-a_2}\right)^{n-2} \cdots \\ &= \frac{\left|\mathrm{Sym}^2 A\right|}{|A|^n}\end{aligned}$$

where $A = \mathbb{Z}/\ell^{a_1}\mathbb{Z} \times \mathbb{Z}/\ell^{a_2}\mathbb{Z} \times \mathbb{Z}/\ell^{a_3}\mathbb{Z} \cdots$.

(4) Then,

$$\sum_{f \in \mathrm{Surj}(\mathbb{Z}_\ell^n, A)} \mathrm{Prob}\left(f(A_n) = 0\right). = \frac{\#\mathrm{Surj}(\mathbb{Z}_\ell^n, A)}{|A|^n} \left|\mathrm{Sym}^2 A\right|$$

Example 13.5. If $A = (\mathbb{Z}/\ell\mathbb{Z})^k$ then $\left|\wedge^2 A\right| = \ell^{\frac{k(k-1)}{2}}$ while

$$\left|\#\mathrm{Sym}^2 A\right| = \ell^{\frac{k(k+1)}{2}}$$

Fact 13.6. The rank of an alternating matrix is always even.

Further, we can put an alternating form always in the standard block form

$$\begin{pmatrix} 0 & \mathrm{id} & 0 \\ -\mathrm{id} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

by change of basis.

Now, observe that

$$\mathrm{rk}_\ell \operatorname{coker} A_n = n - \mathrm{rk}\, A_n.$$

where $\mathrm{rk}_\ell = \dim_{\mathbb{F}_\ell} A_n/\ell A_n$. Therefore, $n - \mathrm{rk}_\ell \operatorname{coker} A_n$ is always even.

Hence, when n is even, the cokernel of id $-A_n$ for A_n a random alternating matrix, we obtain all even rank groups while for n odd, we obtain all odd rank groups. Additionally, the A_n are singular over $\mathbb{Q}_\ell$ for n odd. That is, we always have $\det A_n = 0$. Then, $\operatorname{coker} A_n = \mathbb{Z}_\ell \times T$ for T some abelian group of even rank. In particular, the even and odd case will necessarily have different distributions because their matrices always have different $\mathbb{Z}_\ell$ ranks. As $n \to \infty$, we have

$$\lim_{n\to\infty} \mathbb{E}\left(\#\mathrm{Surj}\left(\operatorname{coker} A_n, A\right)\right) = \left|\mathrm{Sym}^2 A\right|.$$

As $n \to \infty$, there is certainly not a limit distribution of $\operatorname{coker} A_n$.

However, one can show there are two limit distributions here by just writing down explicit formulas. That is,

$$\lim_{\substack{n\to\infty \\ n \text{ even}}} \text{Prob}\left(\text{coker } A_n \simeq A\right) \text{ exists}$$
$$\lim_{\substack{n\to\infty \\ n \text{ odd}}} \text{Prob}\left(\text{coker } A_n \simeq A\right) \text{ exists}$$

Remark 13.7. These are the predicted distributions for Sel_{ℓ^∞} of elliptic curves over $\mathbb{Q}$ for rank 0 and rank 1 elliptic curves, as the conjectures of Poonen-Rains and Bhargava-Kane-Lenstra-Poonen-Rains.

To see where the infinite part above is coming from, we have $\text{rk}_\ell \text{Sel} = \text{rk}_\ell E + \text{rk}_\ell Ш$. Here, note also that Ш has an alternating pairing (since it is an elliptic curve, not a higher dimensional abelian variety), the Cassels-Tate pairing and so this always has even rank.

Remark 13.8. It turns out the above distributions have the same moments, which are $\left|\text{Sym}^2 A\right|$. Therefore, those moments are not enough to determine the distribution. However, it turns out one can add "an extra moment" keeping track of the parity of the rank, and then the distributions will be determined by the moments plus this extra information, at least in the mod ℓ (as opposed to ℓ^∞) case.

The following remark is not written down anywhere, but turns out to hold.

Remark 13.9. One can prove uniqueness right up to the $\left|\text{Sym}^2 A\right|$ boundary for elementary ℓ-groups. That is

$$\#\text{Surj}(X, (\mathbb{Z}/\ell\mathbb{Z})^k) \leq \ell^{k^2/2} + \frac{(1-\varepsilon)k}{2}$$

for some $\varepsilon > 0$, we still have uniqueness.

Question 13.10. If we have a sequence X_n where

$$\lim_{n\to\infty} \mathbb{E}\left(\#\text{Surj}\left(X_n, A\right)\right)$$

is known (e.g., if it is 1), does this imply $\lim_{n\to\infty} X_n$. I.e., does $\lim_{n\to\infty} \text{Prob}(X_n \simeq A)$ exist? Further, is the distribution the one with those moments?

Above, the limit moments exist does not imply the limit distributions exist.

Remark 13.11. Whenever there are multiple distributions with the same moments, then there are two distributions having the same limiting moments but not the same limiting distributions

For example, we can take $X_n = Y_0$ for n even and Y_1 for n odd. If Y_0 and Y_1 have the same moments, then the moments of X_n are independent of n, but the limiting distribution does not exist if Y_0 and Y_1 have different distributions.

Remark 13.12. We are interested in X_Z to be the distribution of the class group of a uniform random K with $|\operatorname{disc} K| \leq Z$ in the limit $Z \to \infty$.

So, suppose we have a collection of distributions which are determined by their moments. We might still wonder if the limiting distribution is determined by its moments. There is a further unfortunate phenomenon which we will see in the following example.

Example 13.13. Take X to be a real quadratic Cohen-Lenstra group. That is, take

$$\operatorname{Prob}(X \simeq A) = \frac{c}{|A|\,|\operatorname{Aut} A|}$$

so

$$\mathbb{E}\left(\#\operatorname{Surj}(X, A)\right) = \frac{1}{|A|}.$$

Now, take $X_n = \mathbb{Z}/p_n\mathbb{Z}$ where p_n is the nth prime. Then, we claim

$$\lim_{n\to\infty} \mathbb{E}\left(\#\operatorname{Surj}(X_n, A) = \frac{1}{|A|}.\right.$$

for A a fixed finite abelian group. Indeed, once p_n is larger than any prime dividing $|A|$, $\operatorname{Surj}(X, A) \to \operatorname{Surj}(X_n, A)$ is a bijection.

However, for any B,

$$\lim_{n\to\infty} \operatorname{Prob}\left(X_n \simeq B\right) = 0$$

because X_n always has larger and larger cyclic factors. In this example, one does not have a limiting distribution and we have total escape of mass.

Here, uniqueness sin the moment problem, plus having the same limiting moments does not imply that the limiting distribution is as expected. Indeed, there may be escape of mass.

Question 13.14. What if one also requires that the limiting distribution exists and is a probability distribution? I.e., it has no escape of mass. Does the limiting distribution still exist?

Remark 13.15. In practice, we often don't know whether the limiting distribution exists. So the above question is often not so relevant to arithmetic statistics questions.

However, we do have the following result when we stay in the regime of finite abelian ℓ-groups with limiting moments that are not too big.

Theorem 13.16. *For X, Y_n random finite abelian ℓ-groups, If for all A (or all finite abelian ℓ groups A)*

$$\mathbb{E}\left(\#\operatorname{Surj}\left(X, A\right)\right) = \lim_{n\to\infty} \mathbb{E}\left(\#\operatorname{Surj}\left(Y_n, A\right)\right) \leq \left|\wedge^2 A\right|,$$

then

$$\lim_{n\to\infty} \operatorname{Prob}\left(Y_n = B\right) Y_n = \operatorname{Prob}(X \simeq B)$$

and the limit above exists.

Example 13.17. If $\lim_{n\to\infty} \mathbb{E}\left(\#\operatorname{Surj}\left(Y_n, A\right)\right) = 1$ for finite abelian ℓ-groups A then $\lim_{n\to\infty} \operatorname{Prob}\left(Y_n \simeq B\right) = \frac{c}{|\operatorname{Aut} B|}$ for finite abelian ℓ-groups B.

In practice, the above type of result has been used a lot in arithmetic statistics, such as in Heath-Brown's work on statistics of Selmer groups and Fouvry and Klüners' work on ranks of 4-torsion in class groups. That is, one may compute the moments, and use this to determine the distribution.

This will close our discussion of moments. Let us now summarize the key points:

(1) We can conveniently access distributions by their moments
(2) We can conveniently access limit distributions from limit moments
(3) Moments are number theoretically meaningful. For example, for A abelian, $\operatorname{Surj}(\operatorname{Cl}_K, A)$ correspond to unramified A-extensions of K.
(4) When we have $K/\mathbb{Q}$ of degree 2 and L/K an unramified A extension, the data of $(K, \phi \in \operatorname{Surj}\left(\operatorname{Cl}_K, A\right))$ are in correspondence with $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ extensions $L/\mathbb{Q}$ which are unramified above L^A, the fixed field of A.

We will next return to the case of arithmetic statistics over function fields, and for the next several weeks we will discuss work proving limits of moments existing the function field setting. That is, we will work over $\mathbb{F}_q(t)$ instead of $\mathbb{Q}$.

14. 10/23/20

Today, we will transition to discuss the function field case using algebraic geometry over $\mathbb{F}_q$. Recall, $\operatorname{Pic}^0(C) = \operatorname{coker}\left(1 - \operatorname{Frob}|_{T_\ell \operatorname{Pic}^0(C)}\right) \in \operatorname{GSp}_{2g}^{(q)}(\mathbb{Z}_\ell)$. We spent a class discussing the moments of this model in the function field case. Today, we will discuss the function field setting and what changes from the number field setting. If K is finite over $\mathbb{F}_q(t)$ is the function

field of a smooth projective irreducible curve (i.e., 1-dimensional) over $\mathbb{F}_q$. Additionally, this curve comes with a map to $\mathbb{P}^1_{\mathbb{F}_q}$.

Remark 14.1. We have an equivalence of categories between smooth projective irreducible curves over $\mathbb{Q}$ and finitely generated fields $K/\mathbb{F}_q$ finitely generated of transcendence degree 1. Specifying K additionally as an extension of $\mathbb{F}_q(t)$ corresponds to giving a map $C_K \to \mathbb{P}^1_{\mathbb{Q}}$ for C_K the curve corresponding to K under the above correspondence.

Let us briefly recall how abelian extension of K work.

Remark 14.2 (Class field theory over global function fields)**.** Let $J_K := \prod_v K_v^\times / K^\times$. We have an Artin map

$$J_K \to \mathrm{Gal}\left(K^{\mathrm{ab}}/K^\times\right)$$

that yields an isomorphism on profinite completions

$$\widehat{J_K} \simeq \mathrm{Gal}\left(K^{\mathrm{ab}}/K^\times\right).$$

Recall that places v of K correspond to closed points of C_K as a scheme, or equivalently $\overline{\mathbb{F}}_q/\mathbb{F}_q$ orbits of $\overline{\mathbb{F}}_q$ points of C_K. Then, $\deg v$ is the degree of the residue field over $\mathbb{F}_q$ which is the size of the $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ orbit.

Abelian extensions correspond to surjections

$$\prod_v K_v^\times / K^\times \to A.$$

If the extension is unramified, the above map factors

$$\begin{array}{ccc} \prod_v K_v^\times/K^\times & \longrightarrow & \left(\prod_v K_v^\times/\mathscr{O}_v^\times\right)/K^\times \\ & \searrow \quad \swarrow & \\ & A & \end{array} \tag{14.1}$$

We can write

$$\left(\prod_v K_v^\times/\mathscr{O}_v^\times\right)/K^\times = \prod_v \langle \pi_v \rangle / K^\times$$

for π_v a uniformizer at v. This is exactly the divisor class group $\mathrm{Pic}(C)$.

Summarizing, abelian unramified A-extensions of K, or equivalently finite étale connected A-covers of C correspond to surjections $\mathrm{Pic}(C) \to A$.

Remark 14.3 (The degree map and geometric irreducibility)**.** Recall we have a degree map $\mathrm{Pic}(C) \to \mathbb{Z}$ which sends $\pi_v \mapsto \deg v$. Note this map is not in general surjective; it is surjective if and only if C is geometrically

irreducible. This is well defined because elements of $K^\times$ have degree 0. We obtain surjections $\mathrm{Pic}(C) \to \mathbb{Z}/n\mathbb{Z}$. Using class field theory as described in the above remark, we obtain degree n $\mathbb{Z}/n\mathbb{Z}$ extensions of C, which are $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$. Geometrically, this corresponds to $C_{\mathbb{F}_{q^r}}$. Algebraically, we have $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r} = K[s]/f(s)$ where $f(s)$ is the minimal polynomial of some generator of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ with coefficients in $\mathbb{F}_q$. Note that $C_{\mathbb{F}_{q^r}}$ has no $\mathbb{F}_q$ points. Further, these are irreducible but are not geometrically irreducible.

Recall we want to study

$$\mathrm{Pic}^0(C) := \ker\left(\mathrm{Pic}(C) \xrightarrow{\deg} \mathbb{Z}\right).$$

Or, in the imaginary quadratic case, we have a point ∞ in $\mathbb{P}^1$ and we have a unique point $\infty \in C$ over $\infty \in \mathbb{P}^1$. We might be interested in studying $\mathrm{Pic}^0(C) \to \mathrm{Pic}(C)/\infty$. In the real quadratic case, we have ∞_1 and $\infty_2 \in C$ over $\infty \in \mathbb{P}^1$ and in the real quadratic case, we may be interested in studying $\mathrm{Pic}^0(C)/\langle \infty_1 - \infty_2 \rangle \simeq \mathrm{Pic}(C)/\langle \infty_1, \infty_2 \rangle$. So, the theory might be that $\mathrm{Pic}^0(C)$ is equidistributed in some way and $\mathrm{Pic}^0(C)/\langle \infty_1 - \infty_2 \rangle$ may be viewed as a quotient of $\mathrm{Pic}^0(C)$ by a random element.

Using class field theory, quotients of $\mathrm{Pic}(C)$ are more natural, since they correspond to certain abelian unramified extensions.

Example 14.4. Given a surjection $\mathrm{Pic}(C)/v_0 \to A$, we must have that the uniformizer at v_0 is trivial. That is, this must send $\mathrm{Frob}(v_0)$ to 0 so v_0 must be split completely.

Now, $\mathrm{Pic}(C)/\infty$ or $\mathrm{Pic}(C)/\langle \infty_1, \infty_2 \rangle$ for C hyperelliptic are finite groups. Additionally, these characterize extensions which split completely over ∞ or ∞_1 and ∞_2. In particular, these extensions have $\mathbb{F}_q$ points.

Question 14.5. How can one study $\mathrm{Pic}(C)/\infty$ using geometry over $\mathbb{F}_q$.

This is a tool that is not at all available in the number field case. We will talk about multiple ways we can do this. However, all of them are built on étale cohomology. In this class we will use étale cohomology as a black box.

There are two main tools from étale cohomology we will use are

(1) Deligne-Katz equidistribution
(2) Grothendieck-Lefschetz trace formula

We'll next give an introduction to what each of these are about and next class we'll give an introduction to étale cohomology and the étale fundamental group. In the following classes, we will use this to discuss how these approaches play out.

14.1. **Deligne-Katz equidistribution.** Recall that if $C/\mathbb{F}_q$ is a curve, we have Frob acting on $T_\ell(\mathrm{Jac}(C)) \simeq \mathbb{Z}_\ell^{2g}$. Then, we can view Frob $\in \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}_\ell)$. If Frob were Haar random in $\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}_\ell)$ and $\ell \nmid q-1$, we get the Cohen-Lenstra distribution. Strictly speaking, Frob really only determines a conjugacy class, but two elements in the same conjugacy class will have isomorphic 1-eigenspaces, and hence the resulting distribution of $\mathrm{id} - \mathrm{coker}\,\mathrm{Frob}$ will not depend on the choice of value of Frobenius in this conjugacy class.

We'd like to describe a concrete notation of equidistribution of $F_1, F_2, \ldots \in \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}_\ell)$. For each k, we can look at $\overline{F}_1, \overline{F}_2, \ldots \in \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/\ell^k\mathbb{Z})$. Then, for all $h \in \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/\ell^k\mathbb{Z})$,

$$\lim_{X\to\infty} \frac{\#\left\{i \le X : \overline{F}_i = h\right\}}{X} = \frac{1}{\#\,\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)} \tag{14.2}$$

For all k, (14.2) implies that $\mathrm{coker}(\mathrm{id} - F_n)$ have the Cohen-Lenstra limit distribution.

Deligne-Katz equidistribution will give us (14.2) for F_i's Frobenius on $T_\ell(\mathrm{Jac}(C_i))$ where C_i's are in certain families over $\mathbb{F}_q$ with $q \to \infty$.

What we wanted was the following: Fix q. We wanted to look at C_i varying over $\mathbb{F}_q$ of varying genera. Admittedly, this doesn't make sense because for varying g, the group is changing. We actually wanted equidistribution of $\mathrm{id} - \mathrm{coker}$, but strictly speaking, equidistribution of varying moving targets in this case would need to be made sense of.

What we get from Deligne-Katz equidistribution, as in work of Achter, is the following. Fix g. Let the C_i vary over genus g hyperelliptic curves over varying $\mathbb{F}_q$. This either varies over all q or arbitrarily large q with $\ell \nmid q-1$. Note that one can relate $\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}_\ell)$ and $\mathrm{GSp}_{2g}^{(q')}(\mathbb{Z}_\ell)$ for $1-q = u(1-q')$ with $u \in \mathbb{Z}_\ell^\times$.

14.2. **Grothendieck Lefschetz trace formula.** This lets us count $\mathbb{F}_q$ points on X by knowing enough about the étale cohomology of X. For example, even knowing the 0th étale cohomology of X (which has to do with knowing about the components of X and geometric components of X. This approach was pioneered by Ellenberg-Venkatesh-Westerland. The moments correspond to certain $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ extensions, i.e., covers of $\mathbb{P}^1_{\mathbb{F}_q}$. Those are $\mathbb{F}_q$ points on a moduli space of such covers.

15. 10/28/20

Today we'll have a crash course on étale fundamental group and étale cohomology. The goal is mostly to orient us to what the definitions might be.

15.1. **The étale fundamental group.** This is motivated by the analog in topology.

15.1.1. *The topological fundamental group.* When we have a nice topological space X, we have a universal covering space $U \to X$. Then, $\pi_1(X) = \mathrm{Aut}(U/X)$. Technically, we need base points to be precise, but we will ignore that level of detail today. The cover is universal in the sense that all connected covering spaces $Y \to X$ receive maps from the universal cover U, so we have

(15.1)
$$\begin{array}{ccc} U & \longrightarrow & Y \\ & \searrow \quad \swarrow & \\ & X & \end{array}$$

and $\pi_1(X) = \mathrm{Aut}(U/X)$. Then, subgroups of $\pi_1(X)$ correspond to connected covering spaces $Y \to X$. Then $Y \to X$ is a normal covering space (or equivalently Galois in this case) if and only if the corresponding subgroup of $\pi_1(X)$ is normal. Then, for G a group, normal connected G covers of X are in bijection with surjections $\pi_1(X) \to G$.

Remark 15.1. What we will use below is that there is an equivalence of categories between finite quotients of $\pi_1(X)$ onto G and finite normal connected G-covers.

15.1.2. *The algebraic setting.* We now move into the world of algebraic geometry. We only consider finite covers, and essentially take the topological covering space construction as the definition of $\pi_1^{\text{ét}}(X)$.

Let X be a connected scheme. We should technically choose a base point, which will need to be a geometric point in this case. Though again, we won't worry about base points. Covers correspond to finite étale maps with connected source. If you haven't seen étale morphisms before, there are at least 2 equivalent definitions. One is that it is smooth of relative dimension 0. Another definition is that they satisfy a lifting property: it is formally étale and of finite presentation.

one defines $\pi_1^{\text{ét}}(X)$ so that finite quotients of $\pi_1(X)$ correspond to connected finite étale morphisms to X.

Example 15.2. The map

$$\mathbb{A}^1 \to \mathbb{A}^1$$
$$x \mapsto x^2$$

is not étale over the origin, but it is étale when you remove the origin in the source and target.

Topologically, we might think of a punctured copy of $\mathbb{A}^1$ as the circle, via looking at its complex points. So its fundamental group should be $\mathbb{Z}$, or $\widehat{\mathbb{Z}}$ when we take the profinite completion and only see finite covers.

Example 15.3. If k is a perfect field, and finite extension is étale so $\pi_1(\operatorname{Spec} k) = \operatorname{Gal}(\overline{k}/k)$.

Remark 15.4. The following is often a point of confusion for number theorists. When number theorists say $\mathbb{Q}(i)/\mathbb{Q}$ is ramified, it really means $\operatorname{Spec}\mathbb{Z}[i]$ over $\operatorname{Spec}\mathbb{Z}$ is ramified, hence not étale, at the point $(i) \in \operatorname{Spec}\mathbb{Z}[i]$. However, $\operatorname{Spec}\mathbb{Q}(i)$ over $\operatorname{Spec}\mathbb{Q}$ is étale. Then, $\pi_1(\operatorname{Spec}\mathscr{O}_K) = \operatorname{Gal}(K^{\mathrm{un}}/K)$ for K^{un} the maximal unramified extension of K.

In general, finite étale $Y \to \operatorname{Spec}\mathscr{O}_K$ correspond to rings of integers in unramified extensions L over K.

15.2. **Étale cohomology.** Take X to be a nice scheme over $\mathbb{C}$. Let $X(\mathbb{C})^{\mathrm{an}}$ denote the corresponding space with the analytic topology. We can look at $H^*(X(\mathbb{C})^{\mathrm{an}}, \mathbb{Z})$.

Example 15.5. Take $X = \mathbb{P}^1$. Then $\mathbb{P}^1(\mathbb{C})^{\mathrm{an}}$ is also notated as $\mathbb{C}\mathbb{P}^1$. Then,

$$H^*\left(\mathbb{P}(\mathbb{C})^{\mathrm{an}}, \mathbb{Z}\right) = \begin{cases} \mathbb{Z} & \text{if } * = 0 \\ 0 & \text{if } * = 1 \\ \mathbb{Z} & \text{if } * = 2 \\ 0 & \text{if } * > 2. \end{cases}$$

We have two goals for generalizing this:

(1) We want invariants like this form general base schemes like $\mathbb{Q}, \mathbb{F}_p, \overline{\mathbb{F}}_q, \overline{\mathbb{Q}}, \mathbb{Z}$ instead of just over $\mathbb{C}$.
(2) We would like to keep track of the relevant Galois action over general base fields. That is, $\sigma \in \operatorname{Gal}(\overline{K}/K)$ should act on $H^*(X_{\overline{K}})$.

In fact, étale cohomology accomplishes these goals. For X a nice scheme over a field K and $\ell \neq \operatorname{char} K$, we typically take coefficients in $\mathbb{Z}/\ell^n\mathbb{Z}$. Then, one can extend the definition to $\mathbb{Z}_\ell$ and $\mathbb{Q}_\ell$ coefficients. One can construct étale cohomology groups $H^*_{\text{ét}}(X, \mathscr{F})$ for $\mathscr{F}$ one of the above mentioned types of coefficients. These groups satisfy the following properties.

(1) They are functorial in X.
(2) They vanish for $* > 2\dim(X)$.
(3) There is also a compactly supported version of étale cohomology.

15.2.1. *Ideas in the definition of étale cohomology.* One useful property of covering spaces is that they, locally on the base, disjoint unions of copies of the base. However, this is in general quite false for maps of schemes in the Zariski topology. This is because Zariski open sets are way too big. For example, in the map $\mathbb{A}^1 - 0 \to \mathbb{A}^1 - 0$ by $x \mapsto x^2$, every nonempty open set is the complement of a finite number of points. In particular, there is no open set on the target over which the preimage is disconnected.

One needs "smaller" neighborhoods to get this property. In the end, one uses "larger" neighborhood. Really, what we mean is that we want a finer topology. However, we will work with neighborhoods so large that they don't even fit in the space. Instead of a usual topology where opens are subsets of the space, we use a *Grothendieck topology*, where opens are certain spaces that map to your space. This will let us define the étale topology, where the above desired disjoint union property does hold. There are similar axioms for Grothendieck topologies, analogous to the axioms that unions of opens are open, and finite intersections of open are open. In the étale topology, one declares étale morphisms to be open.

With the étale topology, we have the property that étale morphisms can be locally written as a disjoint union of copies. More precisely, given $X \to Y$ étale, every point $p \in Y$ is contained in an (étale) open $x \in U$ such that the preimage of U in X is a disjoint union of copies of U.

One defines $H^*_{\text{ét}}(X, \mathbb{Z}/\ell^n\mathbb{Z})$ with the above idea and then the analog of a classical definition of cohomology groups.

15.2.2. *More high-brow properties.* Let's discuss some additional properties.

(1) There is a cup product on cohomology.
(2) There is Poincaré duality. Suppose X is smooth. Then there is a perfect pairing induced by the cup product $H^i(X) \times H_c^{2r-i}(X) \to H_c^{2r}(X)$. (We are being a bit loose with coefficients here.) This $H_c^{2r}(X)$ is a free module over the coefficients of rank 1.
(3) If X is proper, $H_c^i = H^i$.

One of the key properties we will need is the Grothendieck-Lefschetz Trace formula. This is the analog of the Lefschetz fixed point theorem. For $K = \mathbb{F}_q$, this gives

$$\#X(\mathbb{F}_q) = \sum (-1)^i \operatorname{tr}\left(\text{Frob} \,|\, H_c^i(X_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_\ell)\right).$$

Note here that $\#X(\mathbb{F}_q)$ is counting the fixed points of Frobenius. The usual Lefschetz fixed points theorem counts fixed points of a nice topological map in terms of alternating sums of its action on cohomology of the space.

Remark 15.6. So, the Grothendieck-Lefschetz trace formula lets us count $\mathbb{F}_q$ points by understanding the cohomology and Galois action on the cohomology groups.

To better understand this, we will need to understand the cohomology groups and the action of Frobenius.

There are two things we will need to know about cohomology groups. One is smooth an proper base change. A consequence of this is the following.

Example 15.7. Suppose $X \to \operatorname{Spec} \mathbb{Z}$ is a proper smooth scheme. Then, we can relate $H^i_{\text{ét},c}(X_{\mathbb{C}}, \overline{\mathbb{Q}}_\ell = H^i_{\text{ét},c}(X_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_\ell)$.

So, we can relate questions over $\overline{\mathbb{F}}_q$ to a question over $\mathbb{C}$. Moreover, we will need Artin's comparison theorem.

Theorem 15.8 (Artin comparison)**.** *We have*

$$H^i_{\text{ét},c}(X_{\mathbb{C}}, \overline{\mathbb{Q}}_\ell) \simeq H^i_c(X(\mathbb{C})^{\text{an}}, \overline{\mathbb{Q}}_\ell)$$

where the latter cohomology is the usual topological cohomology.

Additionally, we need to understand the action of Frobenius. Fortunately, Deligne has proven the Riemann hypothesis over finite fields.

Theorem 15.9. *Let X be smooth and proper over $\mathbb{F}_q$. The eigenvalues of Frobenius on H^i_c lie in $\overline{\mathbb{Q}}$. Additionally, if one eigenvalue appears, all its conjugates appear as well. Moreover, any eigenvalue α and all their conjugates have size $q^{i/2}$.*

Remark 15.10. One can drop properness and smoothness, but there is still an extension of these facts. For example if one drops properness, the above holds where instead the eigenvalues have norm $q^{w/2}$ for some $w \leq i$.

Example 15.11. Let's use the Grothendieck Lefschetz trace formula to count $\#\mathbb{P}^1(\mathbb{F}_q)$. Note

$$\#\mathbb{P}^1(\mathbb{F}_q) = \operatorname{tr} \operatorname{Frob} H^0(\mathbb{P}^1) - \operatorname{tr} \operatorname{Frob} H^1(\mathbb{P}^1) + \operatorname{tr} \operatorname{Frob} H^2(\mathbb{P}^1) = \pm 1 \pm q$$

using that the 0th and 2nd cohomology groups are 1-dimensional and the 1st cohomology group is 0 dimensional, we get the above computation.

16. 10/30/20

16.1. **Review and our statistical question.** Last time, we were discussing using algebraic geometry over $\mathbb{F}_q$ to say things about statistics of class groups over function fields.

Last class, we discussed some algebraic geometry tools relating to the étale fundamental group and étale cohomology.

The general problem was to understand quadratic extensions K over $\mathbb{F}_q(t)$, corresponding to hyperelliptic curves C which are degree 2 covers of $\mathbb{P}^1_{\mathbb{F}_q}$. We want to understand $\mathrm{Cl}_{\mathscr{O}_K}$ or $\mathrm{Pic}^0(C_K)$ and more precisely understand $\mathrm{Cl}_{\mathscr{O}_K}[p]$ or $\#\mathrm{Surj}\,(\mathrm{Cl}_{\mathscr{O}_K}, \mathbb{Z}/p\mathbb{Z})$. Alternatively, it may be clarifying to think about understanding $K/\mathbb{F}_q(t)$ when the extension is a Γ extension more generally, where we need not have $\Gamma = \mathbb{Z}/2\mathbb{Z}$. If it helps you, you may think of Γ as $\mathbb{Z}/2\mathbb{Z}$ for the moment.

We then have a counting problem. The denominator is asking about the number of Γ extensions up to some bound. The numerator is asking about the number of element of $\mathrm{Cl}_{\mathscr{O}_K}[p]$ or $\mathrm{Surj}\,(\mathrm{Cl}_{\mathscr{O}_K}, \mathbb{Z}/p\mathbb{Z})$ of some Γ extension. That is, we want to understand either of

$$\frac{\#\text{ of elements of } \mathrm{Cl}_{\mathscr{O}_K}[p] \text{ up to some bound}}{\#\Gamma \text{ extensions of } \mathbb{F}_q(t) \text{ up to some bound}} \tag{16.1}$$

$$\frac{\#\text{ of elements of } \mathrm{Surj}\,(\mathrm{Cl}_{\mathscr{O}_K}, \mathbb{Z}/p\mathbb{Z}) \text{ up to some bound}}{\#\Gamma \text{ extensions of } \mathbb{F}_q(t) \text{ up to some bound}} \tag{16.2}$$

When we mention "numerator and denominator" in what follows, we will always mean the numerator and denominator of (16.1). The idea will be to view the numerator and denominator as counts of $\mathbb{F}_q$ points on some moduli space over $\mathbb{F}_q$. Our tools from last time can tell us about the number of $\mathbb{F}_q$ points on these varieties. There is more than one way one can do this. We will pick the second one relating to the moments $\mathrm{Surj}\,(\mathrm{Cl}_{\mathscr{O}_K}, \mathbb{Z}/p\mathbb{Z})$ though one could do this in a different way relating to subgroups instead of quotient groups.

Then, Γ $K/\mathbb{F}_q(t)$ extensions correspond to Galois Γ covers $\pi : C \to \mathbb{P}^1$. For example, we can take $\Gamma = \mathbb{Z}/2\mathbb{Z}$, in which case we get hyperelliptic curves.

16.2. **Hurwitz spaces.** We next discuss Hurwitz spaces, which will parameterize the above discussed extensions.

Definition 16.1. The Γ-*Hurwitz space* is an algebraic stack over $\mathbb{F}_q$ whose points correspond to the data of Γ extensions $C \to \mathbb{P}^1$.

Remark 16.2. We will not justify why this is an algebraic stack, but one can construct it using standard techniques in algebraic geometry by rigidifying it appropriately and constructing a suitable smooth cover by a scheme.

Recall that elements of $\mathrm{Surj}\,(\mathrm{Cl}_{\mathcal{O}_K}, \mathbb{Z}/p\mathbb{Z})$ correspond to unramified $\mathbb{Z}/p\mathbb{Z}$ extensions of K split completely at ∞ (where ∞ denotes all points of C over a fixed point of $\mathbb{P}^1$).

For $K/\mathbb{F}_q(t)$ a quadratic extension,

$$(K, \phi \in \mathrm{Surj}\,(\mathrm{Cl}_{\mathcal{O}_K}, \mathbb{Z}/p\mathbb{Z}))$$

correspond to $\mathbb{Z}/p\mathbb{Z} \rtimes_{-1} \mathbb{Z}/2\mathbb{Z} := D_p$ (the dihedral group of order $2p$) extensions L of $\mathbb{F}_q(t)$ so that L over $L^{\mathbb{Z}/p\mathbb{Z}}$ is unramified everywhere and split completely over ∞.

Now, the denominator is the number of points in the Hurwitz space for $\mathbb{Z}/2\mathbb{Z}$, $\#H_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)$. The numerator is close to being $H_{D_p}(\mathbb{F}_q)$, but we need to include the additional condition of L being unramified everywhere and split completely over ∞. However, these are conditions one can add to the moduli space. We call this new moduli space H'_{D_p}, where we add in these unramified and split conditions. Then, we want to count

$$\frac{\#H'_{D_p}(\mathbb{F}_q)}{\#H_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}.$$

Remark 16.3. These Hurwitz spaces certainly have many components. For example, there is a discrete invariant of the genus. We notate this genus by including a superscript g. We can use the genus as the bound, so we are looking for

$$\lim_{g\to\infty} \frac{\#H'^{g}_{D_p}(\mathbb{F}_q)}{\#H^{g}_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}.$$

Strictly speaking, one should really add up all genera up to g. However, it turns out that for each genus, the number of points for that genus is so much more than that of the previous genus that it won't matter whether we take the sum over genera up to g, instead of just looking at genus g. If the above terms without the sum have a limit, the same will be true of the corresponding sums up to g.

Goal 16.4. We have two varieties $H'^{g}_{D_p}$ and $H^{g}_{\mathbb{Z}/2\mathbb{Z}}$. We would like to understand how many $\mathbb{F}_q$ points these have.

Suitably motivated, we will next discuss $\mathbb{F}_q$ points on varieties.

16.3. **Counting $\mathbb{F}_q$ Points on varieties.**

Question 16.5. How many points should a variety X over $\mathbb{F}_q$ have?

A very coarse level 0 answer is that you might expect about $q^{\dim X}$ $\mathbb{F}_q$ points. Let's next review the Riemann hypothesis for curves.

Theorem 16.6 (Riemann Hypothesis for curves)**.** *Let X be a smooth projective geometrically integral curve over $\mathbb{F}_q$. Then,*

$$\left|\#X(\mathbb{F}_q) - q - 1\right| < 2gq^{1/2}.$$

This was proven by Weil around 1940, and was a large part of the motivation for the Weil conjectures. This shows that the above answer $X(\mathbb{F}_q) \sim q^{\dim X}$ is somewhat reasonable for curves, at least when q is large relative to the genus. The constant g only depends on the geometry of X and is quite coarse.

Another nice asymptotic result for varieties of arbitrary dimension is due to Lang-Weil.

Theorem 16.7 (Lang-Weil, around 1954)**.** *Let $X \subset \mathbb{P}^n$ be a projective geometrically integral variety of degree d and dimension r. Then*

$$\left|\#X\left(\mathbb{F}_q\right) - q^r\right| \leq \delta_d q^{r-1/2} + A_{n,d,r} q^{r-1}$$

where

$$\delta_d = (d-1)(d-2)$$

and $A_{n,d,r}$ is an explicit constant depending only on n, d, and r.

Once again, the difference between q^r has a power savings of $q^{1/2}$ (i.e., it is $q^{r-1/2}$) and this difference really only depends on combinatorial invariants of X.

Sketch. Start with the Riemann hypothesis for curves. Induct on the dimension of X. Look at a hyperplanes H and we will apply the inductive hypothesis to $X \cap H$. Then, we will sum over hyperplanes $H \in (\mathbb{P}^{n-1})^\vee$ and we have

$$\begin{aligned}\#(\mathbb{P}^{n-1})^\vee \#X(\mathbb{F}_q) &= \sum_{H \in (\mathbb{P}^n)^\vee(\mathbb{F}_q)} (X \cap H)(\mathbb{F}_q) \\ &= \sum_{\substack{H : X \cap H \text{ satisfies the hypotheses of the theorem} \\ \dim X \cap H = \dim X - 1}} (X \cap H)(\mathbb{F}_q) + \sum_{\text{other } H} \#(X \cap H)(\mathbb{F}_q).\end{aligned}$$

The reason for the factor of $\#(\mathbb{P}^{n-1})^\vee$ is that this counts the number of hyperplanes containing any given point. One then can show there aren't too

many bad H in the second term, and can use a crude bound to bound the number of H in the second term. The second term essentially corresponds to hyperplanes whose intersection with X is no longer geometric integral (or hyperplanes containing X in the case X happens to be degenerate).

We then do induction to reduce to the 1-dimensional case, but there is a tiny bit of additional input to deal with the case of singular curves in dimension 1. □

Let's see some examples of varieties where the above bound is quite off (but the variety is not geometrically integral)

Example 16.8. Consider a disjoint union of two copies of $\mathbb{P}^1$ meeting at a point. This has $2q+1$ points.

The disjoint union of two copies of $\mathbb{P}^1$ has $2q+2$ points.

Of course, these varieties are both reducible.

Example 16.9. Consider $f(x,y)$ an homogeneous irreducible cubic over $\mathbb{F}_q$. In $\mathbb{P}^2$, consider the variety given by $f(x) = 0$, where $\mathbb{P}^2$ has coordinates x, y, z. Further, the above variety is smooth and connected, but not geometrically connected. Here, we have $\#X(\mathbb{F}_q) = 0$.

Example 16.10. More generally, given X, consider the number of geometric components of X defined over $\mathbb{F}_q$. That is, the number of components of X which are geometrically integral. Said another way, this is the number of components of $X_{\overline{\mathbb{F}}_q}$ which are fixed by Frobenius Frob_q, which means raising the coordinates of the polynomials defining X to the qth power.

So, the level 1 answer is that

$$\#X(\mathbb{F}_q) \sim q^{\dim X} \cdot \#(\text{irreducible components of } X \text{ which are geometrically irreducible})$$

A level 1.5 answer might be that the error from the level 1 answer is $O(q^{\dim X - 1/2})$ with constants in the O notation depending on coarse geometric invariants of X.

The above also fits in to the picture of étale cohomology. Recall that for X smooth and projective of dimension r, $\#X(\mathbb{F}_q) = \operatorname{tr}\mathrm{Frob}\,|H^{2r} - \operatorname{tr}\mathrm{Frob}\,|H^{2r-1} + \cdots$. On H^{2r}, the eigenvalues have size q^r, on H^{2r-i} they have size $q^{r-i/2}$. In fact, H^{2r} essentially corresponds to H_0 by Poincaré duality, which parameterizes components of X. In fact, H^{2r} parameterizes irreducible components of X. Then, the trace of a permutation representation counting the number of fixed points, which is the number of components which are geometrically irreducible. The factor of q^r comes from Poincaré duality. The error between q^r times the number of irreducible components which are geometrically irreducible components is about $O(q^{r-1/2})$.

Remark 16.11. It seems this version of point counting from étale cohomology is neither strictly stronger or weaker than Lang Weil. The reason is that Lang Weil only depends on relatively coarse invariants, while this version depends on finer invariants such as the cohomology. In any particular case, it may be useful to use one or the other, depending on whether one understands the cohomology of the variety or the degree and the embedding.

Recall we were trying to understand

$$\frac{\#H'(\mathbb{F}_q)}{\#H(\mathbb{F}_q)}.$$

Both the numerator and denominator are about q^r. The approximations are only good when q gets large. But if q is fixed, we don't have much information at all. The original problem is for q fixed and the discriminant, or the genus g, going to infinity. The nature of the kinds of approximations we have discussed so far will not give theorems about the original problem. They only give theorems about the approximation as q gets large. Further, the above approximations assume we have a single geometrically integral component.

Next time, we will discuss how one can get a theorem for the $q \to \infty$ theorem about moments of class groups.

17. 11/4/20

Last time, at least as $q \to \infty$, we saw that for X a variety, $\#X(\mathbb{F}_q)$ was given by the number of Frobenius fixed components of maximal dimension of $X_{\overline{\mathbb{F}}_q}$ times $q^{\dim X}$.

We also saw that

$$\mathbb{E}\left(\#\operatorname{Surj}(\operatorname{Cl}\mathscr{O}_K, A)\right) = \frac{\#H'_{A\rtimes\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}{\#H_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}.$$

Today, we'll discuss the issue of the order of the limits of things going to infinity. We will then discuss understanding the number of components of the space in the numerator of the above fraction.

17.1. **The order of the limits.** Recall that our original problem was over $\mathbb{Q}$ and we were trying to compute the expected number of surjections of the class group of $\mathscr{O}_K$ onto $\mathbb{Z}/n\mathbb{Z}$ over $|\operatorname{disc}(K)| \leq X$ as $X \to \infty$.

In the function field setting, we replace $\mathbb{Q}$ by $\mathbb{F}_q(t)$ and the discriminant corresponds to the genus of C_K, the smooth proper curve associated to K over $\mathbb{F}_q(t)$. However, these genera are discrete, and it turns out that one obtains the same asymptotic if one takes curves of genus exactly g instead of at most g, since each genus has many more curves than the previous genus.

We could image a graph with the genus g positioned vertically and the finite fields size q positioned horizontally. The original question is about taking vertical limits along the g direction, with q fixed.

Example 17.1. We could image in our q, g graph described above, that all the lattice points above the diagonal are 2 and all the points below the diagonal are 1. If we first take a limit in q and then a limit in g, we will get 1. However, if we first take a limit in g and then a limit in q, we will get 2. Therefore, in general, taking limits in g and q do not commute.

However, without further information, knowing the large q limit is still heuristically useful.

Further, it is a perfectly fine question in its own right to ask about the distribution of class groups of Pic^0 of curves over finite fields. That is, the question where one fixes g and lets q go to infinity, it is not a good analog of the original question, but it is already an interesting question.

Remark 17.2. Fixing g and letting q go to infinity is typically the easiest option. Letting q and g go to infinity simultaneously is of intermediate difficulty. Finally, fixing q and letting g go to infinity is typically the most difficult.

Remark 17.3. The discriminant $\mathrm{disc}(K/\mathbb{F}_q(t))$ is an ideal of $\mathbb{F}_q(t)$. If one takes the norm, one gets a number $\mathrm{Nm}(\mathrm{disc}(K/\mathbb{F}_q(t)) = \prod_{\text{ramified places}} q^{\text{ramification degree}}$. So, the norm of the discriminant is q^{ag+b} coming from Riemann Hurwitz where a and b just depend on the degree of the extension and g is the geometric genus.

17.2. **Thinking about components and the $q \to \infty$ limit.** For now, we'll let $q \to \infty$ and then count components.

Remark 17.4. We'll start by describing some of the history. The idea to use this lens to understand the Cohen-Lenstra heuristics over function fields is due to J-K Yu in unpublished notes. This inspired Jeff Achter to work on it. We will discuss a $q \to \infty$ result due to Achter. The next important work along these lines is due to Ellenberg Venkatesh and Westerland. Their breakthrough came from looking not just at components, but instead by thinking about the higher homology of these varieties (the further terms in the Grothendieck-Lefschetz trace formula). We will follow the perspective of Ellenberg Venkatesh and Westerland.

Recall we are trying to understand the ratio

$$\frac{\#H'_{A\times\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}{\#H_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}.$$

This is already interesting to think about the case $A = \mathbb{Z}/3\mathbb{Z}$ so we are counting S_3 covers. We will assume $2 \nmid q$. In this case that the characteristic is not 2, hyperelliptic curves can be written in the form $y^2 = f(x)$. So, the set of hyperelliptic curves can be identified with the set of homogeneous polynomials in 2 variables. If we additionally want the hyperelliptic curves to be smooth, then the polynomials need to have no repeated roots, i.e., be squarefree.

Question 17.5. What does this space of homogeneous polynomials look like over the complex numbers?

A squarefree polynomial over $\mathbb{C}$ is determined, up to scaling, by its roots. Therefore, the genus is determined by the number of roots of $f(x)$, or equivalently the degree of f. (These are not equal, but the number of roots determines the genus using Riemann Hurwitz).

Over the complex numbers, if we fix the number of roots, this space is connected. To stay in the space of squarefree f, the roots may need to be patient as they move, so as not to overlap.

If $H_{\mathbb{Z}/2\mathbb{Z}}$ was smooth and proper, it would be well known that being connected over the complex numbers implies these spaces are also connected over $\overline{\mathbb{F}}_q$. This essentially follows from Stein factorization, and is sometimes called the Enriques-Severi-Zariski connectedness principle. This is not proper because two points can come together. However, one can still use geometry to show that connectedness of these spaces over $\mathbb{C}$ implies it is connected over $\overline{\mathbb{F}}_q$.

The space $H_{\mathbb{Z}/2\mathbb{Z}}$ is closely related to $M_{0,n}$. So, generically, on coarse spaces, $M_{0,n}$ is a degree $n!$ generically étale cover for $n > 3$. We then understand the relation between $M_{0,n}$ and $\overline{M_{0,n}}$ and can use connectedness of $\overline{M_{0,n}}$. Here $M_{g,n}$ denotes the moduli space of smooth genus g curves with n ordered distinct marked points, and $\overline{M_{g,n}}$ is a compactification of this space which is proper, and parameterizes stable curves. Further, $\overline{M_{g,n}}$ includes $M_{g,n}$ as a dense open subset and is modular. There are other compactifications of $M_{g,n}$ and this is an interesting area of current research in algebraic geometry and the minimal model program.

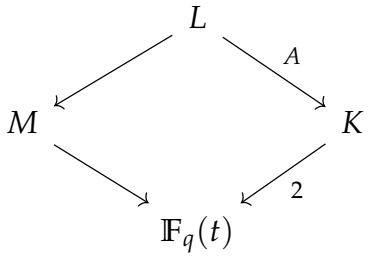
Remark 17.6. It is certainly much easier to see $H_{\mathbb{Z}/2\mathbb{Z}}$ is connected. However, the above description is a path which will work more generally.

Remark 17.7. The general theme we are using here is that often things are nicest when working with proper spaces, and we can often understanding non-proper spaces by understanding the proper space it sits inside of and the boundary you need to add in to compactify your original space.

Question 17.8. What is the fiber of the projection map $H'_{A\times\mathbb{Z}/2\mathbb{Z}} \to H_{\mathbb{Z}/2\mathbb{Z}}$?

We can identify a point $[H]$ in the space of hyperelliptic curves, with the roots x_i of the polynomial $f(x)$. We will call this fixed basepoint $\star$. This projection map comes from the field diagram

(17.1)



A point in $H'_{A\rtimes\mathbb{Z}/2\mathbb{Z}}$ in this fiber corresponds to a curve $\pi : D \to \mathbb{P}^1$ that is ramified only at the x_i. Then, $D - \cup_i \pi^{-1}(x_i) \to \mathbb{P}^1 - \cup_i x_i$ is an unramified map. Equivalently, we get a map

$$\pi_1\left(\mathbb{P}^1 - \cup_i x_i\right) \to A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}.$$

The fundamental group on the left is F_{n-1}, (or its profinite completion if one looks at the étale fundamental group) the free group on $n-1$ generators, where n is the number of roots x_i. One can use this to conclude the same holds for the fundamental group over $\overline{\mathbb{F}}_q$, so long as one stays away from the case that q and $|A|$ share a common factor. Therefore, we also assume $\gcd(q, |A|) = 1$.

Example 17.9. Let's consider the case $|A| = 3$. Then, we have a map from a free group with generators corresponding to loops around $x_1, x_2, \ldots,$ to S_3. The fiber is approximately

$$\{(g_1, \ldots, g_{n-1}) : g_i \in S_3, g_i \text{ generate } S_3\}.$$

However, we need to throw in the conditions that $K/\mathbb{F}_q(t)$ is ramified, which implies the g_i must be nontrivial. Further, the condition that L over K is unramified translates to the g_i being transpositions. Therefore, the fiber is in fact

$$\{(g_1, \ldots, g_{n-1}) : g_i \text{ transpositions in } S_3, g_i \text{ generate } S_3\}.$$

The above easily generalizes to abelian A of larger order. We'll continue analyzing the situation in the special case $|A| = 3$ for concreteness.

The net question is whether $H'_{A\rtimes\mathbb{Z}/2\mathbb{Z}}$ is connected. We now have $H'_{A\rtimes\mathbb{Z}/2\mathbb{Z}} \to H_{\mathbb{Z}/2\mathbb{Z}}$ is a finite étale cover. Just like in topology, when you have a covering space, we can get between points in the fiber if there is loop of $H_{\mathbb{Z}/2\mathbb{Z}}$ which one can lift to a path joining two points in the fiber. In other words, the action

of $\pi_1(H_{\mathbb{Z}/2\mathbb{Z}})$ on points in a fiber determines the connected components of $H'_{A\rtimes\mathbb{Z}/2\mathbb{Z}}$. Summarizing this, we have

$$\text{Connected components of } H'_{A\rtimes\mathbb{Z}/2\mathbb{Z}} \;\leftrightarrow\; \text{orbits of } \pi_1(H_{\mathbb{Z}/2\mathbb{Z}}) \text{ on a fiber}$$

Over the complex numbers, one can draw pictures to see how $\pi_1(H_{\mathbb{Z}/2\mathbb{Z}})$ acts on the fiber. Recall we have fixed a basepoint $\star$. Moving the x_i around starting and ending at $\star$ correspond to a loop in $H_{\mathbb{Z}/2\mathbb{Z}}$, corresponding to an element of $\pi_1(H_{\mathbb{Z}/2\mathbb{Z}}, \star)$. We have a particular loop which corresponds to simply swapping two points x_i and x_{i+1}, corresponding to an "elementary transformation" or "Dehn twist" of the associated complex curve. This takes

$$(g_1, g_2, \ldots, g_i, g_{i+1}, \ldots, g_{n-1}) \mapsto \left(g_1, \ldots, g_{i-1}, g_i g_{i+1} g_i^{-1}, g_i, g_{i+2}, \ldots, g_{n-1}\right).$$

Note that this operation preserves the product of the g_i. These elementary transformations generate the fundamental group. Therefore, we can identify components of $H'_{A\rtimes\mathbb{Z}/2\mathbb{Z}}$ over the complex numbers with equivalence classes of $(g_1, \ldots)$ under the above equivalence relations.

There was a lot of work in understanding these equivalence classes by Conway-Fried-Parker-Volklein.

Remark 17.10. There are many issues above we have not been precise about that one needs to be precise about in order to get an actual number. So far, we have been focusing on what sort of things you need to obtain a number. To be precise, one needs to be precise about how one is counting the following things

(1) Choices of automorphisms of $\mathrm{Gal}(L/\mathbb{F}_q(t))$ with $A \rtimes \mathbb{Z}/2\mathbb{Z}$.
(2) What is going on at infinity
(3) Do we have maps $\pi_1 \to A \rtimes \mathbb{Z}/2\mathbb{Z}$ or only conjugacy classes of such maps.

One can go either way on any of these things, one just needs to make choices to keep track of the relevant data.

Modulo the above issues pertaining to precision, one finds there are $|\wedge^2 A|$ components of this space. So, if $A = \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/\ell\mathbb{Z}$ then $\wedge^2 A = 1$ and so this has 1 component over $\mathbb{C}$. This implies there is 1 component over $\overline{\mathbb{F}}_q$. Frobenius must fix the component. Next time, we'll discuss the higher moments, like when $A = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. This then has 3 components. It is now not automatic what Frobenius does to them. Next time, we will discuss how to analyze these components.

18. 11/6/20

Recall that we were working in the function field case. We were trying to compute

$$\mathbb{E}\left(\#\operatorname{Surj}\left(\operatorname{Cl}\mathscr{O}_K, A\right)\right) = \frac{\#H'_{A\rtimes_{-1}\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}{\#H_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}$$

with appropriate limits. Recall L/K is an A extension and $K/\mathbb{F}_q(t)$ is a $\mathbb{Z}/2\mathbb{Z}$ extension. We said last time that over $\overline{\mathbb{F}}_q$, $H'_{A\rtimes_{-1}\mathbb{Z}/2\mathbb{Z}}$ has $|\wedge^2 A|$ components for sufficiently large genus (or equivalently sufficiently large discriminant).

Today, when $|\wedge^2 A| > 1$, we need to know how Frobenius acts on these $\overline{\mathbb{F}}_q$ components. To get the components over the complex numbers, one can draw pictures using the path interpretation of π_1^{top}

Remark 18.1. Computing the action of Frobenius is somewhat nontrivial, because there is no way to see Frobenius over the complex numbers.

One needs to see these components over $\overline{\mathbb{F}}_q$ using an algebraic definition in terms of the étale fundamental group.

It often happens that one can define some algebraic invariant. that must be constant in families In our case, we will take an invariant associated to curves which is constant on components of moduli spaces of curves.

Example 18.2. For example, the genus of a curve is constant in families.

If we succeed in defining such invariants, we can often obtain a lower bound on the number of components. However, it may be that objects with the same invariant lie in different components. The component count over $\mathbb{C}$ gives the upper bound. We can then hope that the lower bound matches the upper bound, which would allow us to prove we have found all the geometric components.

We will next go into the definition of this component invariant which we will define algebraically.

Let C be a given $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ cover of $\mathbb{P}^1$. Let D be the divisor on $\mathbb{P}^1$ where $C/\mathbb{P}^1$ is branched. Suppose D is supported on n distinct points, and we are working over $\mathbb{C}$. Let $U := \mathbb{P}^1 - D$. Then, this cover corresponds to a map $\pi_1(U) \xrightarrow{\phi} A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$. In this case $\pi_1(U)$ is the free group on $n-1$ generators, F_{n-1}. From that, we obtained a tuple of elements. The generators are loops γ_i around each of the n points of D. Also, we obtain that $\gamma_1 \cdots \gamma_n = 1$ because the composition is the loop around the boundary of the disk. For symmetry reasons even though the group is generated by the first $n-1$ loops, it is simpler to work with tuples $(g_1, \ldots, g_n)$

with $g_i = \phi(\gamma_i)$, for $\phi : C \to \mathbb{P}^1$ the projection. We impose the relation $(g_i, g_{i+1}) \mapsto (g_{i+1}, g_{i+1}^{-1} g_i g_{i+1})$. When we do this algebraically, are these loops around each point.

We now work over $\overline{\mathbb{F}}_q$. We have $(q, |A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}|) = 1$. We can take $\gamma_1, \gamma_2, \ldots, \in \pi_1^{\text{tame}}(U_{\overline{\mathbb{F}}_q})$ as generators of tame inertia. Note here that tame inertia is cyclic. We can take $(\phi(\gamma_1), \ldots, \phi(\gamma_n)) \in |A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}|^n$.

This leads to the following two questions.

Question 18.3. Is this element well defined? Or better, how does this element depend on the choices we have made, such as choosing generators of tame inertia?

Question 18.4. Is this element constant in families?

The first question is more or less a special case of the second question. The choices we have made above are:

(1) The order of the points $1, \ldots, n$
(2) The conjugacy class of the inertia subgroup
(3) The choice of the generator

Remark 18.5. One might wonder why we didn't have to worry about these choices over $\mathbb{C}$. Over the complex numbers, we only defined the invariant like this in a single fiber. We didn't move around and see how this invariant changed in families. So this question never came up topologically because we had a different way around it. We only needed the definition for a single fiber, and we could make these choices uniformly for the fiber associated to our basepoint.

Changing the choices will turn out to change the invariant we defined above in a very reliable way.

18.1. **The local picture of inertia groups.** To see this, we look at the local picture of inertia groups. We have $\mathbb{F}_q((t))^{(q')}$ over $\overline{\mathbb{F}}_q((t))$ over $\mathbb{F}_q((t))$. When we write superscript (q') it means the prime to q part. The first extension has inertia group equal to the Galois group and the second extension is the maximal unramified extension. $\text{Gal}\left(\mathbb{F}_q((t))^{(q')} / \overline{\mathbb{F}}_q((t))\right)$ is a canonical subgroup which is identified with the roots of unity

$$\mu_\infty\left(\overline{\mathbb{F}}_q\right) = \text{colim}_{\gcd(m,q)=1} \mu_m(\overline{\mathbb{F}}_q)$$

and then $\mathbb{F}_q\left((t)\right)^{(q')} = \overline{\mathbb{F}}_q\left(\left(t^{1/n}\right)\right)_{(m,q)=1}$. So, for σ in the Galois group fixing $\overline{\mathbb{F}}_q$ we have

$$\frac{\sigma(t^{1/m})}{t^{1/m}} \in \mu_m(\overline{\mathbb{F}}_q).$$

Over the complex numbers, we chose $\gamma_1, \gamma_2, \dots$ so that $\gamma_1\gamma_2\cdots\gamma_n = 1$. We also required that, in our choice of the inertia generators γ_i over $\overline{\mathbb{F}}_q$, each γ_i is associated to the same generator of $\mu_\infty(\overline{\mathbb{F}}_q)$.

Exercise 18.6. Verify the above directly with étale cohomology or using class field theory using the maximal abelian extension. That is, verify the condition that $\gamma_1\gamma_2\cdots\gamma_n = 1$ imposes the condition that all γ_i are associated to the same generator of $\mu_\infty(\overline{\mathbb{F}}_q)$. *Possible Hint:* Consider the action on $k(t, \sqrt[m]{\frac{t-t_1}{t-t_2}}, \sqrt[m]{\frac{t-t_2}{t-t_3}}, \dots, \sqrt[m]{\frac{t-t_n}{t-t_1}})$ for t_i the points where γ_i generates the inertia. Let ζ_i be the element of $\widehat{\mathbb{Z}}(1)$ corresponding to γ_i. Show that the condition $\gamma_1\gamma_2\cdots\gamma_n = 1$ forces $\zeta_i\zeta_{i+1}^{-1} = 1$

Now, pick a topological generator of $\mu_\infty(\overline{\mathbb{F}}_q)$, pick an ordering of $\overline{\mathbb{F}}_q$ points on D, and pick $\gamma_1, \dots, \gamma_n$ with γ_i a generators of inertia with $\gamma_1\cdots\gamma_n = 1$.

The next step is to pass from orbits of tuples to something more algebraic. Define the quotient of the free group

$$\mathscr{G} := \langle [g] : g \in A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}\rangle / \langle [g_i]\,[g_{i+1}] = [g_{i+1}]\left[g_{i+1}^{-1}g_ig_{i+1}\right]\rangle.$$

Above, $[g]$ is merely a formal symbol associated to the element g. As a semigroup, this above is exactly the orbits of the tuples of all lengths we saw topologically. Orbits of tuples then correspond to elements of $\mathscr{G}$. Now, take

$$[\phi(\gamma_1)]\cdots[\phi\left(\gamma_n\right)] \in \mathscr{G}. \tag{18.1}$$

The following theorem is a group theory argument.

Theorem 18.7. *The above element of* (18.1) *doesn't depend on the ordering or choice of inertia generator. Though it does depend on ζ, the element of $\mu_\infty(\overline{\mathbb{F}}_q)$ we chose above using Exercise 18.6.*

The final input we will need is the following:

Proposition 18.8. *When $n \gg 0$ (relative to the length of tuple or the degree of the ramification divisor) the set of orbits of tuples of length n inject into $\mathscr{G}$.*

The proof uses group theory.

Hence, given an $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ cover $C \to \mathbb{P}^1$ over $\overline{\mathbb{F}}_q$, we obtain an element of $\mathscr{G}$.

Theorem 18.9. *The above constructed element of $\mathscr{G}$ is constant in families.*

The above has two uses. First, one can do this in a family over $\operatorname{Spec}\mathbb{Z}$ the goes from $\operatorname{Spec}\mathbb{C}$ to $\operatorname{Spec}\overline{\mathbb{F}}_q$. So, this can help connect different characteristics. This is also constant in families over $\overline{\mathbb{F}}_q$, such as on a component of $H'_{A\rtimes\mathbb{Z}/2\mathbb{Z}}$.

The key here is specialization maps of π_1 which works as follows. If we have a trait T (the spectrum of a DVR) with geometric generic point η and geometric closed point s, and $X \to T$ is a sufficiently nice family, there is an isomorphism $\pi_1(X_s) \xrightarrow{f} \pi_1(X_{T^{\mathrm{sh}}})$ for T^{sh} the strict henselization (the local ring in the étale topology) which gives a map $\pi_1(X_\eta) \to \pi_1(X_s)$ by composing the map induced by $\eta \to T^{\mathrm{sh}}$ with the inverse of the isomorphism f above. Under this map, the γ_i elements are compatible with the specialization maps.

The upshot is that one can see these $\left|\wedge^2 A\right|$ many components over $\overline{\mathbb{F}}_q$ and work out that Frobenius acts by multiplication by q. Therefore, the Frobenius fixed components correspond to

$$\wedge^2 A[q-1]$$

Therefore, when A is an ℓ group and $\ell \nmid q-1$, there is one Frobenius fixed component over $\overline{\mathbb{F}}_q$. However, there are $\wedge^2 A$ components over $\overline{\mathbb{F}}_q$. This gives the moment $\mathbb{E}\left(\#\operatorname{Surj}\left(\operatorname{Cl}\mathscr{O}_K, A\right)\right) = 1$ in a $q \to \infty$ limit. As $q \to \infty$ this gives a cohen lenstra distribution of $\operatorname{Cl}\mathscr{O}_K$ due to Achter.

Next time, we will discuss more tools from topology and algebraic geometry to say even more.

19. 11/11/20

Let's being by reviewing what we discussed the previous few classes. For large q, $\#X(\mathbb{F}_q)$ is controlled by the number of geometrically irreducible components. In order to understand moments of $\operatorname{Cl}\mathscr{O}_K$, we discussed Hurwitz spaces whose $\mathbb{F}_q$ points give the moments and their components. The upshot was that as $q \to \infty$, and $\ell \nmid q(q-1)$, we see the Cohen-Lenstra moments. We can view $q-1 = \#\mu\left(\mathbb{F}_q(t)\right)$.

Today, the plan is to go beyond just understanding the components and look further at the topology of these spaces. In particular, we will use the Grothendieck-Lefschetz trace formula and not just Lang-Weil.

We'll use X_n to denote our Hurwitz spaces. We had previously been using H, but we want to avoid that because we'll be computing a lot of cohomology. Let X_n be a space over $\mathbb{F}_q$ of dimension n, where n was roughly (up to a

linear function) the number of branch points of our cover over $\overline{\mathbb{F}}_q$, and also roughly $\log_q$ disc and also roughly the genus.

We have

$$\#X_n(\mathbb{F}_q) = \operatorname{tr} F|_{H_c^{2n}} - \operatorname{tr} F|_{H_c^{2n-1}} + \cdots$$

The first term $\operatorname{tr} F|_{H_c^{2n}}$ comes from the components. Next, we consider $\operatorname{tr} F|_{H_c^{2n-1}}$. This has eigenvalues in absolute value at most $q^{n-1/2}$, which uses that X_n is smooth. If X_n were smooth and proper, they would be exactly $q^{n-1/2}$ in absolute value. Smoothness just gives an inequality on their absolute values. If X_n were neither smooth nor proper, we wouldn't be able to say anything about these eigenvalues.

Question 19.1. How many eigenvalues does $\operatorname{tr} F$ have? That is, what is $\dim H_c^{2n-i}(X_n, \mathbb{Q}_\ell) = \dim H^i(X_n, \mathbb{Q}_\ell) =: h_i(n)$. The first equality uses Poincaré duality.

If we want to put the contribution from $\operatorname{tr} F|_{H_c^{2n-1}}$ into the error term using the dimension and bound on the eigenvalues, we need $\frac{n_1(n)q^{n-1/2}}{q^n} = \frac{h^1(n)}{q^{1/2}} \to 0$. Unless $h_1(n) = 0$, we can only have $\frac{h^1(n)}{q^{1/2}} \to 0$ as $q \to \infty$. There are two ways to do this.

(1) We can fix n and let $q \to \infty$, then let $n \to \infty$. In math, this means $\lim_{n\to\infty} \lim_{q\to\infty}$ We have previously discussed this version.
(2) $\lim_{(n,q)\to\infty}$ with n going to infinity slowly enough compared to q. This is formally the same as the first limit above.
(3)

These two ways use no bounds on the nonzero cohomology groups.

The next input is a basic upper bound on $h_1(n)$.

$$\dim H^i(X_n) \leq D^n$$

for D some constant. This uses that there is a topological complex for X_n with at most D^n cells. The consequence of this basic upper bound lets us give an explicit expression for how fact q grows as a function of n. For example, if $q \geq (D+1)^{2n}$ then using the above bound, $\frac{h_1(n)}{q^{1/2}} \to 0$. Before, we saw that as long as n grows slowly enough relative to q, we saw we could take $\lim_{(n,q)\to\infty}$ for n growing slowing enough. Now that we have this bound on cohomology, we get an explicit function for q in terms of n. If we had a better bound, we could obtain less restrictive descriptions of q in terms of n. Eventually, we are interested in the case q is fixed and $n \to \infty$. So, even if we had a linear bound on q in terms of n, one would still need q to grow

with n. We would still need $q^{1/2}$ to out pace the linear function of n. In order to get farther than this, one would need to know a rather different kind of phenomenon to hold: homological stability.

19.1. **Homological stability.**

Remark 19.2. Let's briefly describe the story of homological stability. This is an idea that has been around in topology for a long time. Many times, there is a natural sequence of spaces $X_1, X_2, X_3, \ldots$ which get larger and more complicated as the subscript increases.

For fixed i, $H_i(X_n, \mathbb{Z})$ stabilize as $n \to \infty$.

Example 19.3. Here are some examples of cohomological stability.

(1) Harer stability for M_g where $g = n$ above.
(2) Borel proved similar phenomenon for arithmetic groups (either in terms of group cohomology or the corresponding classifying space) such as showing $H^i(\mathrm{SL}_n(\mathbb{Z}), \mathbb{Q})$ stabilize $H^i(\mathrm{Sp}_{2n}(\mathbb{Z}), \mathbb{Q})$ in n.
(3) McDuff showed stability for configurations spaces where $X_n = \mathrm{Conf}^n M$ for M an open (i.e., not compact) manifold. Here Conf^n is the moduli space of unordered sets of n distinct points.

Here are some more remarks.

Remark 19.4.
(1) There is a huge story of homological stability and there are loads of things that come up. Often, one hopes there are maps $X_n \to X_{n+1}$ that induce isomorphisms on H_i. This sometimes happens, but not always.
(2) There is a question of what coefficients to take for homological stability. Often they stabilize with $\mathbb{Q}$ but not with $\mathbb{Z}$ coefficients.
(3) There is a generalization called representation stability, where one may ask for more refined stability phenomenon. For example, one may order the n points in the configuration spaces above and ask how they vary as S_n representations.

There might be on the order of 10 methods used for proving homological stability, and among them, they have been used to prove hundreds of homological stability results.

Example 19.5. One space we are interested in is $\mathrm{Conf}^n \mathbb{P}^1$ which is essentially the same as $H_{\mathbb{Z}/2\mathbb{Z}}$, the Hurwitz space of hyperelliptic curves.

Recall $H'_{A \rtimes \mathbb{Z}/2\mathbb{Z}, n}$ denotes the Hurwitz space of $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ covers which implicitly depends on n, the number of branch points geometrically. The prime notates restriction on ramification.

Theorem 19.6 (Ellenberg, Venkatesh, Westerland). *$H'_{A\rtimes_{-1}\mathbb{Z}/2\mathbb{Z},n}$ has homological stability with $\mathbb{Q}$ coefficients.*

More precisely, for fixed i, there exists k so that there exist constants a, b depending only on A for $n \geq ai + b$,

$$H_i(X_n, \mathbb{Q}) \simeq H_i(X_{n+k}, \mathbb{Q}).$$

The style of the proof is most similar to that used for showing homological stability of $\mathscr{M}_g$.

Question 19.7. What is the consequence of the above theorem for taking limits and the Cohen-Lenstra heuristics over function fields?

We find $\frac{h_1(n)}{q^{1/2}} \to 0$ holds so long as $q \to \infty$ at any rate. Before, q had to be large compared to n. As we got better bounds we could let q be smaller compared to n. However, now, the upper bound doesn't even depend on n. Note that we will still need to let $q \to \infty$ eventually if we want $h_1(n)$ to be negligible compared to $q^{1/2}$.

Let's now see what the above tells us for higher cohomology groups as well. We'll ignore the issue that

$$H_i(X_n, \mathbb{Q}) \simeq H_i(X_{n+k}, \mathbb{Q}).$$

and take $k = 1$ to conceptually simplify the discussion (which is only done for conceptual purposes; it is easy to work in the value of k if one desires). We find

$$\dim H_i(X_n, \mathbb{Q}) \leq \dim H_i(X_{ai+b}, \mathbb{Q}) \leq D^{ai+b} \leq E^i$$

Therefore, $|\operatorname{tr} F|_{H_c^{2n-i}}| \leq q^{n-i/2}E^i = \left(\frac{E}{\sqrt{q}}\right)^i q^n$. The main term has order q^n. Also, the order of our denominator is q^n. We next need to sum over i. To sum over i, we need $\frac{E}{\sqrt{q}} < 1$ so $q > E^2$. Then we can sum

$$\frac{\#X_n(\mathbb{F}_q)}{q^n} = 1 + c_1 + c_2 + \cdots$$

where the leading 1 is the number of geometrically irreducible components and $|c_i| \leq \left(\frac{E}{\sqrt{q}}\right)^i$. For fixed q, the above sum certainly converges. That is, for fixed $q > E^2$,

$$\limsup_{n\to\infty} \frac{\#X_n(\mathbb{F}_q)}{q^n} \leq \frac{1}{1 - \frac{E}{\sqrt{q}}}$$

We also find

$$\liminf_{n\to\infty} \frac{\#X_n(\mathbb{F}_q)}{q^n} \geq 1 - \frac{\frac{E}{\sqrt{q}}}{1-\frac{E}{\sqrt{q}}}$$

Note, that as $q \to \infty$ the lim sup and lim inf both tend to 1. Therefore, the main consequence of Theorem 19.6 is

Theorem 19.8.

$$\lim_{q\to\infty} \limsup_{n\to\infty} \#H'_{A\rtimes\mathbb{Z}/2\mathbb{Z},n} = \lim_{q\to\infty} \liminf_{n\to\infty} \#H'_{A\rtimes\mathbb{Z}/2\mathbb{Z},n} = 1.$$

In a sense, this is the best $q \to \infty$ result because $q \to \infty$ last. Equivalently, $(q,n) \to \infty$ with q going arbitrarily slowly compared to n.

Remark 19.9. This is much more difficult than taking a $q \to \infty$ limit first. If we used no bound on the cohomology we needed to take $q \to \infty$ first. If we had some exponential bound on homology, we would need to take $q \to \infty$ as a quickly growing function of n. To be able to take $q \to \infty$ slowly, we really need the constant upper bound on the size of homology. This is quite a lot stronger than an exponential bound, or no bound at all.

Remark 19.10. There is a completely inexplicit stabilization phenomenon. That is, there are sequences of surjective maps of finite sets which must eventually become isomorphisms. This is an obstacle to getting explicit values of the constants a and b above, but likely no one has investigated making these constants explicit in too much detail.

Remark 19.11. We expect the above to be true for every fixed q, though that is an open question.

The analog of Cohen-Lenstra over $\mathbb{Q}$ over $\mathbb{F}_q(t)$ would be fixing q and letting $n \to \infty$, and then asking for the number of $\mathbb{F}_q$ points on these Hurwitz spaces in these limits.

From above, for fixed q, if we wanted to compute not just a limsup and liminf, but an actual limit we would need to exactly know $\operatorname{tr} F|_{H_c^{2n-1}}$ and $\operatorname{tr} F|_{H_c^{2n-i}}$, instead of just finding upper and lower bounds. That is:

Question 19.12. (1) Do we know the dimension of H_c^{2n-1}?
(2) Do we know the Frobenius eigenvalues?

The first question is about knowing the stable values. This is still open and seems difficult. Knowing the Frobenius eigenvalues also seems quite difficult.

Remark 19.13. In general, if one is trying to use this picture, how might one try to find the Frobenius eigenvalues. The hope is that one might find dim H^i over $\mathbb{C}$ and topology. Then, one might want to identify the cohomology coming from something algebraic. That is, perhaps they are pulled back from known classes on other spaces. This is especially amenable to analysis when such objects are pulled back from a top dimensional class on some space, so that one knows how Frobenius acts on that.

Example 19.14. In $\mathscr{M}_g$, the stable values are tautological classes, and those can be understood algebraically.

Once one understands algebraic sources of the cohomology, one can hope to understand the Frobenius action on the algebraic objects.

This general strategy has been successful in some examples.

An even better way to know the Frobenius eigenvalues would be if the cohomology group is 0. So, if true, the following conjecture would give a way to compute the stable cohomology.

Conjecture 19.15 (Ellenberg-Venkatesh-Westerland)**.**

$$H^i(H'_{A\rtimes_{-1}\mathbb{Z}/2\mathbb{Z},n},\mathbb{Q}) \to_{n\to\infty} \begin{cases} \mathbb{Q} & \text{if } i=0 \\ \mathbb{Q} & \text{if } i=1 \\ 0 & \text{else} \end{cases}$$

The above conjecture would give the Cohen Lenstra result over $\mathbb{F}_q(t)$ for fixed q sufficiently large compared to A.

20. 11/13/20

The plan for the remaining four lectures is the following. We will discuss higher degree number fields and also what happens when we consider the maximal unramified extension instead of just the maximal abelian unramified extension, corresponding to the class group. In terms of the four meetings, we will discuss

(1) Class groups of Galois extensions
(2) Class groups of non-Galois extensions
(3) Distributions of unramified extensions $\mathrm{Gal}(K^{\mathrm{un}}/K)$
(4) Function field theorems as $q \to \infty$ for all of the above.

We'll discuss many of these questions with reference to the quadratic case that we have already discussed for much of the course. Today, we'll discuss conjectures for distributions of Cl_K for Galois extensions.

The original conjectures are from a paper of Cohen-Martinet. They are often referred to as the Cohen-Lenstra-Martinet conjectures but the three

never wrote a paper together. Rather, there was one paper of Cohen-Lenstra and another paper of Cohen-Martinet. Melanie will present her perspective on these conjectures.

For today, we fix a group Γ and consider Galois Γ extensions K over $\mathbb{Q}$. We also fix the Γ-signature of K, by which we mean the action of Γ on $K \otimes \mathbb{R}$. Equivalently, we fix $\Gamma_\infty \subset \Gamma$, a decomposition group at ∞ defined as the subgroup generated by complex conjugation. In particular, $|\Gamma_\infty| \leq 2$.

Remark 20.1. When we have the above structure, Cl_K is a $\mathbb{Z}[\Gamma]$ module. Even if you only care about the distribution of Cl_K just as an abelian group, the natural way to understand this distribution is to take into account its structure as a Γ module.

Remark 20.2. Note that Cl_K is only a $\mathbb{Z}[\Gamma]$ module if we specify a choice of isomorphism $\Gamma \simeq \mathrm{Gal}(K/\mathbb{Q})$. If we don't specify such a choice, then Cl_K is not naturally a Γ module. Said another way, we should really say that Γ extensions are extensions $K/\mathbb{Q}$ with a specified isomorphism $\Gamma \simeq \mathrm{Gal}(K/\mathbb{Q})$, not just a field for which there exists such an isomorphism. Then, for every field $K/\mathbb{Q}$, we will have $\mathrm{Aut}(\Gamma)$ many such Γ extensions.

The above remark motivates the following definition.

Definition 20.3. We use Γ-*field* to denote an extension $K/\mathbb{Q}$ together with a choice $\Gamma \simeq \mathrm{Gal}(K/\mathbb{Q})$.

In the above, it is convenient to take $K \subset \overline{\mathbb{Q}}$ and fix $\overline{\mathbb{Q}} \subset \mathbb{C}$ so as to obtain complex conjugation and not just a subgroup $\Gamma_\infty \subset \Gamma$ up to conjugacy. That is, the we have rigidified data as above to fix our choices.

On the homework, we saw that in fact the finite order $\mathrm{Gal}(K/\mathbb{Q})$ was a module for the quotient $R' := \mathbb{Z}[\Gamma] / \sum_{\gamma \in \Gamma}$. If we'd like to understand R' modules, we should break our $\mathbb{Z}$ module up as a sum of its sylow p subgroups. Given a map $M \to N$ of finite order $\mathbb{Z}$-modules this induces a map on Sylow p-subgroups $M_p \to N_p$. These different Sylow-p subgroups do not interact. That is, we have

Exercise 20.4. The category of finite order R'-modules is equivalent to

$$\prod_p \text{ the category of finite } p\text{-group } R'\text{-modules}$$

The above lets us reduce to p-group modules, so we may as well consider them as modules for $R := \mathbb{Z}_p[\Gamma] / \sum_{\gamma \in \Gamma} \gamma$.

Question 20.5. How can we describe all R-modules.

The answer is nice when $p \nmid |\Gamma|$. We will throw out such p. This is the nice analog of throwing out 2 for quadratic fields. For the most part, we'll only

consider the part of the class group with $p \nmid |\Gamma|$. In this case, the finite order R modules are basically analogous to what the finite order $\mathbb{Z}_p$ modules are. We will now elaborate on this.

20.1. **The abelian case.** Note that $\mathbb{Q}_p[\Gamma]$ is a semisimple algebra over $\mathbb{Q}_p$.

Definition 20.6. The notion of a maximal order makes sense in the noncommutative setting. An *order* in a $\mathbb{Z}_p$ module is a finitely generated $\mathbb{Z}_p$ module subgroup. A *maximal order* is a maximal such order.

Then $\mathbb{Z}_p[\Gamma]$ is a maximal order relative to $\mathbb{Z}_p$. When Γ is abelian,

$$\mathbb{Q}_p[\Gamma] \simeq E_1 \times \cdots E_r$$

and

$$\mathbb{Z}_p[\Gamma] = \mathcal{O}_{E_1} \times \cdots \times \mathcal{O}_{E_r}$$

for E_r over $\mathbb{Q}_p$ a field extension. When Γ is nonabelian, we have

$$\mathbb{Z}_p[\Gamma] = \prod_i M_{n_i}(\Delta_i) \tag{20.1}$$

where Δ_i denotes a maximal order in a division algebra over $\mathbb{Q}_p$ and $M_n(\Delta)$ denotes $n \times n$ matrices over Δ.

Remark 20.7. In general, for any p, a maximal order in $\mathbb{Q}_p$ is of the form (20.1) which uses $p \nmid |\Gamma|$. In the local setting, maximal orders are unique (though they are not unique in general in the noncommutative setting. Then, $\mathbb{Z}_p[\Gamma]$ is a maximal order in general only when $p \nmid |\Gamma|$. When $p \mid |\Gamma|$ $\mathbb{Z}_p[\Gamma]$ will be a non-maximal order sitting inside the right hand side of (20.1).

Further, when $p \nmid |\Gamma|$ then Δ_i are commutative.

Exercise 20.8. Show that for Γ abelian, the category of $\mathcal{O}_{E_1} \times \mathcal{O}_{E_2} \times \cdots \times \mathcal{O}_{E_r}$-modules is the product over i of the categories of $\mathcal{O}_{E_i}$ modules. *Hint:* Use idempotents in each coordinate.

The above exercise reduces our question to knowing about $\mathcal{O}_{E_i}$ modules of finite order, which is the ring of integers in a local field. Then, $\mathcal{O}_{E_i}$ are Dedekind domains, and so finite modules over such rings are of the form $\prod_j \mathcal{O}_{E_i}/\mathfrak{m}_i^{a_j}$ with $a_1^i \geq a_2^i \cdots$ for $\mathfrak{m}_i$ the maximal ideal of $\mathcal{O}_{E_i}$. Since p does not divide Γ, the components $\mathcal{O}_{E_i}$ correspond to irreducible representations of Γ, and for each such irrep, we get a partition from the above sequence of a_j.

Remark 20.9. Recall we were actually studying $R = \mathbb{Z}_p[\Gamma] / \sum_{\gamma \in \Gamma} \gamma$. Note that $\sum_{\gamma \in \Gamma} \gamma$ is $|\Gamma| \cdot e_1$ for e_1 an idempotent corresponding to the trivial representation. The condition that we quotient by $\sum_{\gamma \in \Gamma} \gamma$ corresponds to the fact

that we have no parts of our module corresponding to the trivial representation, that is, Γ acts nontrivially on each $\mathscr{O}_{E_i}$.

20.2. **The non-abelian case.** We now consider the case Γ is non-abelian.

Theorem 20.10 (Morita)**.** *The category of $M_n(\mathscr{O}_E)$ modules are equivalent to $\mathscr{O}_E$ modules.*

Proof. Given an $\mathscr{O}_E$ module A, we obtain an $M_n(\mathscr{O}_E)$ module A^n with

$$A^n = \begin{pmatrix} A \\ A \\ \vdots \\ A \end{pmatrix}$$

This is naturally an $M_n(\mathscr{O}_E)$ module.

One can then construct an inverse map and show they it is inverse to this one. □

The upshot of the above theorem is that we know all the $\mathbb{Z}_p[\Gamma] / \sum_{\gamma\in\Gamma} \gamma$ finite modules. In terms of data, these modules are given by a partition (in terms of the exponents a_j^i in $\mathscr{O}_{E_i}/\mathfrak{m}_i^{a_j^i}$) for each nontrivial irrep V of Γ over $\mathbb{F}_p$. The nontriviality is coming from Remark 20.9. Here, representations over $\mathbb{F}_p$ are equivalent to representations over $\mathbb{Q}_p$ since $p \nmid |\Gamma|$.

Wedderburn's theorem says that modules for $k[\Gamma]$ for k a field corresponds to Γ reps over K.

A nice fact analogous to the quadratic case is that

$$\sum_{\text{finite } R\text{-modules } A} \frac{1}{\#\operatorname{Aut}_R(A)} < \infty.$$

Here are the steps to construct the Cohen-Martinet Distribution:

(1) Take a $\frac{1}{|\operatorname{Aut}_R|}$ random group. That is, take X with $\operatorname{Prob}(X \simeq A) = \frac{c}{\operatorname{Aut}_R(A)}$. We cannot be done yet because even in the quadratic case, it will not account for real quadratic fields.
(2) Take a certain random quotient of X (described in a somewhat complicated way).

Remark 20.11. Recall in the $\mathbb{Z}/2\mathbb{Z}$ case, the real quadratic distribution is the imaginary quadratic distribution modulo a uniform random element.

We'll now explain another heuristically motivated perspective on how to take the quotient from the second step of Cohen-Martinet's distribution. This will be in forthcoming joint work of Melanie Wood and Yuan Liu.

Consider $I^{S\otimes\mathbb{Z}_p}/\mathscr{O}_S^\times\otimes\mathbb{Z}_p$. Recall in the quadratic case, the top $I^{S\otimes\mathbb{Z}_p}$ has rank $|S|$ and the bottom has rank $|S|$ in the imaginary case and $|S|+1$ in the real quadratic case.

Now, for fixed R modules V and W (finite free $\mathbb{Z}_p$ modules) we have

$$\mathrm{Hom}_R(V,W)\simeq\mathbb{Z}_p^N$$

compact abelian groups with Haar measure, and consider random quotients V/Wviewed as a random R-module given as $V/_{\mathrm{rand}}\phi(W)$ for a Haar random $\phi\in\mathrm{Hom}_R(V,W)$.

Example 20.12. If $R=\mathbb{Z}_p$ then $V\simeq\mathbb{Z}_p^n, W\simeq\mathbb{Z}_p^n$ then $V/_{\mathrm{rand}}W$ is the cokernel of a Haar random matrix in $M_{n\times n}(\mathbb{Z}_p)$.

If $V=\mathbb{Z}_p^n$ and $W=\mathbb{Z}_p^{n+1}$, then $V/_{\mathrm{rand}}W$ is the cokernel of a Haar random $M_{n\times(n+1)}(\mathbb{Z}_p)$.

Question 20.13. How do we choose the set S?

First, S should be Γ closed. Then, Γ acts on I^S and $\mathscr{O}_S^\times$. Also, I^S as a Γ module has structure depending on the splitting type of primes in S.

Example 20.14. If p is a rational prime and $p\mathscr{O}=\mathfrak{p}$ is totally inert, then $\mathfrak{p}$ is fixed by Γ.

If $p\mathscr{O}=\mathfrak{p}_1\cdots\mathfrak{p}_{|\Gamma|}$ splits completely then $I^{\{\mathfrak{p}_1,\dots,\mathfrak{p}_{|\Gamma|}\}}$ gives a regular representation of Γ.

Let

$$I^S\simeq V_{(n_1,n_2,\dots)}$$

be a fixed $\mathbb{Z}_p[\Gamma]$ module, where n_i denotes the number of primes in S of each splitting type. Also,

$$\mathscr{O}_S^\times\simeq(I^S\otimes\mathbb{Z}_p)\times(\mathscr{O}^\times\otimes\mathbb{Z}_p)$$

is an isomorphism as $\mathbb{Z}_p[\Gamma]$ modules. The second pieces $\mathscr{O}^\times\otimes\mathbb{Z}_p$ depends only on Γ_∞ (which is where the signature comes into the story). Here, $\mathscr{O}^\times\otimes\mathbb{Z}_p$ is $\mathrm{Ind}_{\Gamma_\infty}^{\Gamma}\mathbb{Z}_p/\mathbb{Z}_p$.

Remark 20.15. We have

$$0\longrightarrow\mathscr{O}^\times\longrightarrow\mathscr{O}_S^\times\longrightarrow\mathscr{O}_S^\times/\mathscr{O}^\times\longrightarrow 0 \tag{20.2}$$

There is a map $\mathscr{O}_S^\times/\mathscr{O}\to I^S$ given by valuation. This is not in general an isomorphism and only in general has finite index. However, they are both free $\mathbb{Z}_p[\Gamma]$ modules of the same rank, and turn out to be isomorphic as abstract $\mathbb{Z}_p[\Gamma]$ modules. This is a souped-up representation theory version

of the fact that finite index submodules $M \subset N$ of free $\mathbb{Z}_p$ modules are abstractly isomorphic.

Theorem 20.16 (Liu-Wood)**.** *For a fixed R-module Y,*

$$\lim_{\text{all } n_i \to \infty} V_{(n_1,n_2,\ldots)} /_{rand} (V_{(n_1,n_2,\ldots,)} \times Y)$$

exists and is a random R module. The n_i can go to ∞ in any way you want.

Further, when $Y = 1$, you get the $\frac{1}{|\mathrm{Aut}_R|}$ group, i.e., the group from step (1) of the Cohen-Martinet distribution.

Let $Y = \mathrm{Ind}_{\Gamma_\infty}^{\Gamma} \mathbb{Z}_p/\mathbb{Z}_p$. Then the limit above is the Cohen-Martinet conjectured final distribution. This module Y is coming from the Minkowski map $\mathcal{O}^\times \otimes \mathbb{R}/\mathbb{R}$. To see this over $\mathbb{Z}_p$ takes a bit more work, but also holds once you know $p \nmid |\Gamma|$. For this we need the fact that when $p \nmid |\Gamma|$, a finite index submodule of a free module is isomorphic as a Γ module to that free module.

Remark 20.17. We can think of the Cohen-Martinet construction as starting with a random group, and then quotienting by some "missing places." This makes sense as a quotient of Pic^0 in the function field case, but there is no Pic^0 in the number field case. So in the number field case, it could be argued that this is not so motivated. The work of Liu and Wood seems somewhat more motivated because it constructs this random quotient distribution in one fell swoop and connects it to the arithmetic of number fields directly.

Exercise 20.18. Show

$$V_{(n_1,n_2,\ldots)} /_{\mathrm{rand}} (V_{(n_1,n_2,\ldots,)} \times Y) \simeq \left(V_{(n_1,n_2,\ldots)} /_{\mathrm{rand}} (V_{(n_1,n_2,\ldots,)} \right) /_{\mathrm{rand}} \times Y$$

Remark 20.19. As a reference, see the paper by Weitong Wang and Melanie Wood where they show the probability distribution is given by to

$$\frac{c}{|A^{\Gamma_\infty}|\,|\mathrm{Aut}_R(A)|}$$

and the moments are given by

$$\frac{1}{A^{\Gamma_\infty}}$$

and further the moments determine the distribution.

21. 11/18/20

Today, we'll discuss class groups of non-Galois fields. Next time, we'll discuss Galois groups of the maximal unramified extension (the non-abelian case). On our last class, we'll discuss function field proofs as $q \to \infty$ of the above results. This will be within the context we have already setup as counting $\mathbb{F}_q$ points on certain Hurwitz spaces.

21.1. **Relating non-Galois class groups to their Galois closures.** Let $K/\mathbb{Q}$ be a non-Galois extension. Cohen and Martinet did not direct address class groups of non-Galois number fields in their conjectures. However, they gave a reason why they did not need to address the non-Galois case: Let L denote the Galois closure of $K/\mathbb{Q}$, and suppose $\mathrm{Gal}(L/\mathbb{Q}) \simeq \Gamma$. Let $\Gamma' := \mathrm{Gal}(L/K)$. If $p \nmid |\Gamma|$, then we have a map given by pullback of ideal classes,

$$\begin{aligned} i : \mathrm{Cl}_K[p^\infty] &\to \mathrm{Cl}_L[p^\infty] \\ [I] &\mapsto [I\mathscr{O}_L] \end{aligned}$$

Question 21.1. Is the map i above injective?

Indeed, the composition

$$\mathrm{Cl}_K \xrightarrow{i} \mathrm{Cl}_L \xrightarrow{\mathrm{Nm}_{L/K}} \mathrm{Cl}_K$$

sends $[I] \mapsto [I]^{[L:K]}$. Because $p \nmid \Gamma$, the composition of i with the norm map is injective.

Question 21.2. Is i surjective?

In general $i(\mathscr{L}_K) \subset \mathrm{Cl}_L^{\Gamma'}$. So, in general, i will not be surjective. However, we can ask:

Question 21.3. Is $i\left(\mathrm{Cl}_K[p^\infty]\right) = \mathrm{Cl}_L^{\Gamma'}[p^\infty]$?

There are two obstructions to the above equality. One viewpoint on this is the Leray spectral sequence for the composition of first cohomology of $\mathbb{G}_m$ and Γ' invariants. In more elementary terms, we have an exact sequence

$$0 \longrightarrow P_L \longrightarrow I_L \longrightarrow \mathrm{Cl}_L \longrightarrow 0 \tag{21.1}$$

defining the class group, where P_L denotes principal ideals and I_L denotes the free group generated by ideals. We then get an exact sequence on cohomology

$$0 \longrightarrow P_L^{\Gamma'} \longrightarrow I_L^{\Gamma'} \longrightarrow \mathrm{Cl}_L^{\Gamma'} \longrightarrow H^1(\Gamma', P^L). \tag{21.2}$$

In the p-Sylow subgroup (i.e., $\mathrm{Cl}_L \otimes_{\mathbb{Z}} \mathbb{Z}_p$) we obtain a surjection $I_L^{\Gamma'} \otimes \mathbb{Z}_p \to \mathrm{Cl}_L^{\Gamma'}$ because the right most term $H^1(\Gamma', P^L)$ is annihilated by $|\Gamma'|$.

Now, the composition

$$\begin{aligned} I_L^{\Gamma'} \to I_K &\qquad\qquad \to I_L^{\Gamma'} \\ \mathfrak{a} \mapsto \mathfrak{a}^{\Gamma'} &\qquad\qquad \mapsto \mathfrak{a}^{|\Gamma'|}. \end{aligned}$$

is given by raising to the $|\Gamma'|$ power.

Therefore, we find that for $p \nmid |\Gamma'|$,

$$i : \mathrm{Cl}_K [p^\infty] \simeq \mathrm{Cl}_K [p^\infty]^{\Gamma'}.$$

is an isomorphism.

Altogether, Cohen-Martinet gave a distribution for $\mathbb{Z}_p [\Gamma]$ modules. Taking the Γ' fixed parts give a distribution on $\mathbb{Z}_p$ modules. Therefore, the original conjecture of Cohen-Martinet implies some particular conjecture for non-Galois fields obtained by taking the Γ' fixed parts of the distribution on $\mathbb{Z}_p [\Gamma]$ modules.

21.2. **Relating Cohen-Martinet conjectures for different groups.** In §21.1, we didn't need L to be the Galois closure of K, we just needed it to be Galois and contain K. Also, K did not have to be non-Galois. Therefore, we should hope these Cohen-Martinet for different Galois groups are compatible.

Remark 21.4. The key idea defining the Cohen-Martinet distribution was to take class groups distributed proportionally to $\frac{1}{\mathrm{Aut}}$ as a Γ module.

However, in general this $\frac{1}{\mathrm{Aut}}$ distribution doesn't always push forward. More precisely, take a finite $\mathbb{Z}_p$ module distributed proportionally to $\frac{1}{\mathrm{Aut}}$. That is, $\mathrm{Prob}(X \simeq A) = \frac{c}{|\mathrm{Aut}\, A|}$. Then, $X[p] = X/pX$ is not distributed according to $\frac{1}{|\mathrm{Aut}|}$ for $\mathbb{F}_p$ vector spaces.

However, the above non-compatibility phenomenon does not occur when pushing forward between different Galois groups. More precisely, we have:

Theorem 21.5 (Wang and Wood)**.** *The cohen Martinet distributions pushed forward from* 2 *different larger Galois groups agree.*

Retain the assumption $p \nmid |\Gamma|$. Consider the $\mathbb{Z}_p [\Gamma]$ module $A := \mathrm{Cl}_L [p^\infty]$. Note that Γ actually acts on the left. We may wonder whether ${}^{\Gamma'}A$ has any additional structure. That is, is it anything more than a finite abelian group

Example 21.6. If $\Gamma' \subset \Gamma$ were normal, then $\mathbb{Z}_p [\Gamma/\Gamma']$ would act on ${}^{\Gamma'}A$.

When Γ' is not normal, define

$$e_{\Gamma'} := \frac{\sum_{\gamma \in \Gamma'} \gamma}{|\Gamma'|}$$

which is an idempotent element in $\mathbb{Z}_p [\Gamma]$. Because $e_{\Gamma'}$ is idempotent, we obtain a subset $e_{\Gamma'}\mathbb{Z}_p [\Gamma]$ acting on ${}^{\Gamma'}A$. The issue is that $e_{\Gamma'}\mathbb{Z}_p [\Gamma]$ is not a ring because $e_{\Gamma'}$ is not central. However, one can check $H_{\Gamma,\Gamma'} := e_{\Gamma'}\mathbb{Z}_p [\Gamma] e_{\Gamma'}$ is a ring.

Exercise 21.7. Verify $e_{\Gamma'}\mathbb{Z}_p[\Gamma]e_{\Gamma'}$ is a ring, but it is not a subring of $\mathbb{Z}_p[\Gamma]$ because the identity does not map to the identity.

Verify that $e_{\Gamma'}\mathbb{Z}_p[\Gamma]e_{\Gamma'} \simeq \mathbb{Z}_p[\Gamma'\backslash\Gamma/\Gamma']$. the double coset space. This double coset space is often called a Hecke algebra.

Theorem 21.8 (Wang and Wood)**.** *Let A be the $\frac{1}{\mathrm{Aut}_{H_{\Gamma,\Gamma'}}}$. This distribution agrees with the Cohen-Martinet pushed forward distribution on $H_{\Gamma,\Gamma'}$ modules.*

The above discussion points out that class groups of non-Galois fields do have this additional $H_{\Gamma,\Gamma'}$ structure, even though there is no apparent group action on the field.

Example 21.9. Take $\Gamma = A_5$ and $\Gamma' := \langle (123), (12)(45)\rangle$. Then let $L/\mathbb{Q}$ be an A_5 extension, and L/K be a Γ' extension. Then, $K/\mathbb{Q}$ has degree 10 and $K/\mathbb{Q}$ has no nontrivial automorphisms. However, $H_{\Gamma,\Gamma'} \simeq \mathbb{Z}_p[\sigma] / (\sigma^2 - 1)$. Therefore, the class group of K comes with an order 2 automorphisms, which cannot come from an automorphism of $K/\mathbb{Q}$.

21.3. **Other pieces of what is understood for distributions of class groups.** We will now push up to the boundaries of current knowledge. We will discuss some areas where current work is being done and other areas where it would be exciting to see some work be done.

Question 21.10. What about when $p \mid |\Gamma|$.

Let $K/\mathbb{Q}$ be imaginary quadratic. Then genus theory shows $\mathrm{Cl}_K[2] \simeq (\mathbb{Z}/2\mathbb{Z})^{\omega(D_K)-1}$ where ω denotes the function sending an integer to the number of its prime divisors. The issues here are that this does not determine a distribution because the sizes of this group grow too large, too quickly. Additionally, this 2 part is not random, it easily determined from the discriminant.

Gerth suggested that we could instead ask about $2\,\mathrm{Cl} \simeq \mathrm{Cl} \,/\, \mathrm{Cl}[2]$.

Conjecture 21.11 (Gerth)**.** The distribution of $\mathrm{Cl} \,/\, \mathrm{Cl}[2]$ follows the Cohen-Lenstra distribution. That is, the 2-Sylow subgroup of this quotient is distributed proportionally to $\frac{1}{\mathrm{Aut}}$.

Theorem 21.12 (Fouvry-Klüners)**.** *Gerth's conjecture is correct for* 2 *ranks of* $\mathrm{Cl} \,/\, \mathrm{Cl}\,[2]$*, ordered by the discriminant of K.*

The 2-rank of $\mathrm{Cl} \,/\, \mathrm{Cl}[2]$ is called the 4-rank by Fouvry-Klüners. They did this by finding all the moments, using genus theory as an input.

Remark 21.13. One may ask about 4-torsion of class groups by asking about which elements of $\mathrm{Cl}[2]$ are multiples of 2.

In fact, Gerth actually proved a version of Fouvry-Klüners' theorem but with a nonstandard ordering on the fields K where one first orders by the number of prime divisors of Δ_K. That is, Gerth proved this in the limits

$$\lim_{\#\text{ prime divisors of } D_K \to \infty} \lim_{X \to \infty} \bullet.$$

However, in Gerth's proof, it was unclear whether this ordering was misleading because the conjecture was so closely related to the ordering of the conjecture.

Let's say we next want to understand 8-torsion elements. We then can ask which 4-torsion elements are multiples of 2. And the pattern continues for higher powers of 2. Using many other tools, but still getting a first handle on things using genus theory, smith proves Gerth's conjecture for the 2-Sylow subgroup of quadratic fields.

Theorem 21.14 (Smith)**.** *Gerth's conjecture holds for* $(\mathrm{Cl} \,/\, \mathrm{Cl}[2])\,[2^\infty]$ *of quadratic fields.*

Remark 21.15. Smith also proves Goldfeld's conjecture for quadratic twist families of elliptic curves proving that 50% of elliptic curves have rank 0 and 50% have rank 1.

This gives a pretty beautiful and complete story about the $p \mid \Gamma$ case. That is, we have a genus theory part, and the rest of the 2-part of the class groups is provably random, distributed according to $\frac{1}{\mathrm{Aut}}$.

Remark 21.16. One might ask for further things, like the genus theory part and the rest are independent. This is suggested by work of Altug, Shankar, Varma, and Wilson.

For $|\Gamma| > 2$, the $p \mid |\Gamma|$ regime is much murkier. This is the subject of much ongoing research.

Cohen-Martinet construct a $\frac{1}{\mathrm{Aut}}$ random $\mathbb{Z}_p\,[\Gamma]$ module. They do this by using the fact that $\mathbb{Z}_p\,[\Gamma]$ is a maximal order in $\mathbb{Q}_p\,[\Gamma]$. When $p \mid |\Gamma|$, the ring $\mathbb{Z}_p\,[\Gamma]$ fails to be maximal in $\mathbb{Q}_p\,[\Gamma]$. However, there are some cases where some things can be recovered.

Example 21.17. Note that irreducible central idempotent are in bijection with irreps of Γ. So central idempotents correspond to subsets of the irreps of Γ. However, if

(1) $e \in \mathbb{Q}_p\,[\Gamma]$ is a central idempotent which in fact lies in $\mathbb{Z}_p\,[\Gamma]$, i.e., has no p's in its denominator,
(2) $e\mathbb{Z}_p\,[\Gamma]$ is a maximal order in $\mathbb{Q}_p\,[\Gamma]$,

then Cohen-Martinet call the pair (p, e) *good*.

When a pair (p, e) is good, for L a Γ field, $e \operatorname{Cl}_L[p^\infty] \in \operatorname{Cl}_L[p^\infty]$ is a module for the ring $e\mathbb{Z}_p[\Gamma]$.

For (p, e) good, Cohen-Martinet conjecture that $e \operatorname{Cl}_L[p^\infty]$ is distributed similarly to their usual distribution described last time, except the first step is replaced by a random group distributed proportionally to $\frac{1}{\operatorname{Aut}_{e\mathbb{Z}_p[\Gamma]}}$.

Remark 21.18. Let $e_{\Gamma/\Gamma'}$ corresponds to the induced representation in the trivial representation for Γ' up to Γ.

In Melanie's work with Weitong, for $(p, e_{\Gamma/\Gamma'})$ good in the Cohen-Martinet sense, then

$$\operatorname{Cl}_K[p^\infty] \simeq \left(e_{\Gamma/\Gamma'} \operatorname{Cl}_L[p^\infty]\right)^{\Gamma'}.$$

So, sometimes, when $p \mid |\Gamma|$, one can still prove $\operatorname{Cl}_K[p^\infty]$ is some particular function of $\operatorname{Cl}_K[p^\infty]$.

Example 21.19. Take $\Gamma = S_3, \Gamma' \simeq (23) \subset S_3$ and $p = 2$. This corresponds to the 2-part of the class group of non-Galois cubic fields. In this case, the 2-part of the class group sits inside the 2 part of $\left(e_{\Gamma/\Gamma'} \operatorname{Cl}_L[p^\infty]\right)^{\Gamma'}$, so we might guess this is distributed according to Cohen-Martinet. However, Bhargava proved the first moment is proven to be in accordance with the Cohen-Martinet conjectures.

Remark 21.20 (Roots of unity)**.** In the function field case, we saw the heuristics seem to change when there are roots of unity in the base field. That is, the average of torsion in quadratic fields in the function field case in the large q limit is predicted to be $\wedge^2 A[q-1]$, which is an ℓ group. Achter, Malle, and Garton saw roots of unity have some impact on the distribution. There are revised conjectures for when roots of unity lie in the base field due to Malle, Garton, and Lipnowski-Sawin-Tsimerman.

22. 11/20/20

Last time we discussed the case that the Galois group of $K/\mathbb{Q}$ may fail to be abelian. Today we will discuss a different non-abelian generalization. Namely, that where we try to understand the distribution of a non-abelian version of the class group.

Observe that $\operatorname{Cl}(K) = \operatorname{Gal}(K^{\text{un,ab}}/K)$, the maximal unramified abelian extension. Therefore, $\operatorname{Cl}(K)$ is the abelianization of $\operatorname{Gal}(K^{\text{un}}/K)$, for K^{un} the maximal unramified abelian extension. Recall that being unramified is really more of a property of $\mathcal{O}_K$ instead of K. In fact, $\operatorname{Gal}(K^{\text{un}}/K) = \pi_1(\operatorname{Spec} \mathcal{O}_K)$. We can think of the class group sort of like a first cohomology group H^1 of $\mathcal{O}_K$, (since the first cohomology group is the abelianization of the fundamental

group) though this is not precise. Recall also $\pi_1(\operatorname{Spec} K) = \operatorname{Gal}(K^s/K)$, for k^s the separable closure.

Question 22.1. For K in some family of number fields, what is the distribution of $\operatorname{Gal}(K^{\mathrm{un}}/K)$?

An answer to this question would refine and imply the distribution on class groups.

Here is some motivation for studying the above question.

(1) One of the goals of number theory is to understand $\operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$. We really want to know how this group interacts with its inertia subgroups and Frobenius elements. That is, we also want to understand the important arithmetic pieces of this group. One can view arithmetic statistics as trying to understand statistical aspects of this question. For example, trying to count degree 3 extensions is related to counting index 3 subgroups of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

(2) This can help us understand Cl_K by taking the abelianization. For example, if we consider the Cohen-Lenstra $\frac{1}{\operatorname{Aut}}$ distribution on finite abelian p groups, we can push it forward by taking p-torsion to obtain a distribution on $\mathbb{F}_p$ vector spaces. This is not proportional to the $\frac{1}{\operatorname{Aut}}$ distribution on $\mathbb{F}_q$ vector spaces. Since the class group is naturally the abelianization of a group $\operatorname{Gal}(K^{\mathrm{un}}/K)$ with extra structure, it is conceivable we might want to understand this bigger group.

Example 22.2. There is an example in the paper of Melanie Wood with Yuan Liu and David Zureick-Brown which shows certain class groups cannot occur. The way they show this is by using that these groups do not appear as quotients of the abelianization of $\operatorname{Gal}(K^{\mathrm{un}}/K)$. The example occurs when K is a cyclic cubic extension of $\mathbb{Q}$ and they example $\operatorname{Cl}_K[2^\infty]$.

(3) It can help us understand $\operatorname{Gal}(K^{\mathrm{un,pro\text{-}p}}/K)$, the p-class tower group. This is an analog of the p-sylow subgroup of the class group. This is called the p-class tower group because it can be obtained as a tower of p-Hilbert class fields. In other words, we take the p-part of the Hilbert class field, then take the p-part of the Hilbert class field, and continue indefinitely.

Remark 22.3. Taking the Hilbert class tower (instead of the p-Hilbert class tower) gives the maximal unramified pro-solvable extension and has Galois group $\operatorname{Gal}(K^{\mathrm{un,pro\text{-}solvable}}/K)$. It turns out that this is not particularly well studied. Unlike $\operatorname{Cl}_K = \prod_p \operatorname{Cl}_K[p^\infty]$, $\operatorname{Gal}(K^{\mathrm{un}}/K)$ is not built up in this way. However, $\operatorname{Gal}(K^{\mathrm{un,pro\text{-}p}}/K)$ is the most studied piece of $\operatorname{Gal}(K^{\mathrm{un}}/K)$.

Golud-Shafarevich have a theorem about finite p-groups and their generators and relations. As a corollary they obtain the following.

Corollary 22.4. *Let p be an odd prime. If K is an imaginary quadratic field and $\#\mathrm{Cl}_K[p] \geq p^4$ then $\mathrm{Gal}(K^{\mathrm{un},pro\text{-}p}/K)$ is infinite.*

Proof. Galois cohomology tells something about the number of generators and relations of $\mathrm{Gal}(K^{\mathrm{un},\text{pro-p}}/K)$. By the above mentioned theorem of Golud-Shafarevich, there are no finite such groups whose abelianization has p-rank at least 4. □

Question 22.5. How do we understand the distribution on $\mathrm{Gal}(K^{\mathrm{un}}/K)$.

For real quadratic fields, the conjectured distribution of $\mathrm{Cl}_K^{\mathrm{odd}}$ was discrete. For imaginary quadratic fields, this conjectured distribution of $\mathrm{Cl}_K^{\mathrm{odd}}$ was a product of distributions on p-groups. For $\mathrm{Gal}(K^{\mathrm{un}}/K)$, the limiting distribution will not be discrete.

Example 22.6. The p-adic measure on $\mathbb{Z}_p$ is not discrete. However, we work with this measure on finite quotients by using the fact that it has compatible discrete measures on $\mathbb{Z}/p^k\mathbb{Z}$.

The answer to the above question needs to be a distribution on profinite groups. Now, we can't just point to a group and say the probability. We next describe the sort of shape the answer will have.

Remark 22.7. Suppose the class group is trivial. Then in turns out the maximal unramified pro-p group is also trivial. Also, all the p-class tower groups are trivial. This holds by the Burnside basis theorem (the number of generators of a p-group is the number of generators of its abelianization).

Remark 22.8. Observe that $\mathrm{Gal}(K^{\mathrm{un}}/K)$ is sometimes infinite, by Corollary 22.4. Since the family of infinite profinite groups is uncountable, there can't really be a discrete distribution on this infinite set of groups because uncountable sets don't have interesting discrete measures. Of course, ultimately there has to be a countable set of such possibilities that are realized because there are only countably many number fields. It could be that there is a countable list of groups in which the class group always lies in, but we don't know how to identify such a countable set.

Remark 22.9. There are only countably many number fields, so one might wonder how it is possible for a countable sequence can have a non-discrete distribution.

This is illustrated by the following example: If one has a countable sequence of points on an interval, they can tend to the distribution of Lebesgue measure on the interval.

The moral is that whenever a countable set is landing in an uncountable set tending toward a limiting distribution, one should expect the limiting distribution to be non-discrete.

To discuss these distributions, one needs to put a σ-algebra on profinite groups. To deal with set theoretic issues, one may need to sprinkle words like "small" throughout. We will elide these issues. The idea will be to understand this will be similar to that in Example 22.6 by understanding it on finite quotients.

Definition 22.10. Let C be a set of finite groups. A *variety* (in the context of group theory) $\overline{C}$ is a set of finite groups closed under taking subgroups, quotients, and finite direct products.

Example 22.11. Let $C = \{1\}$. Then $\overline{C} = \{1\}$.

Example 22.12. Let $C = \{\mathbb{Z}/2\mathbb{Z}\}$. Then

$$\overline{C} = \left\{\mathbb{Z}/2\mathbb{Z}, 1, \mathbb{Z}/2\mathbb{Z}^2, \ldots, (\mathbb{Z}/2\mathbb{Z})^k, \ldots\right\}.$$

Definition 22.13. For C a finite set of finite groups, and $\overline{C}$ the associated variety, and G a topological group, we define

$$G^{\overline{C}} := \lim_{G/N \in \overline{C}//\text{continuous quotients}} G/N$$

The above construction something we have previously implicitly done a lot of.

Example 22.14.
(1) Consider $\overline{C}$ to be the set of abelian groups. Then, $G^{\overline{C}}$ is the pro-abelianization, the maximal abelian quotient.
(2) Take $\overline{C}$ to be the set of p-groups. Then $G^{\overline{C}}$ is the pro-p completion.
(3) We have $G^{\overline{\{\mathbb{Z}/2\mathbb{Z}\}}} = G^{\text{ab}}/2G^{\text{ab}}$.

Later today, we will define the Borel σ-algebra using the following topology.

Definition 22.15. Here is a topology on the set of profinite groups. Let C be a finite set of finite groups We let $\overline{C}$ denote the variety associated to C. For every C a finite set of finite groups and H a finite group, we define a basis for our topology by the open sets

$$U_{H,\overline{C}} = \left\{G : G^{\overline{C}} \simeq H\right\}.$$

To define our σ-algebra, we will want to understand what sort of structure this quotient has, so we can then take the above quotients randomly, so long as they have that additional structure.

Remark 22.16. If we were doing the above construction in all pro-finite groups, we shouldn't require H is finite. But, we will later be working in the subcategory where $G^{\overline{C}}$ is a finite group.

One can think of C or $\overline{C}$ as a way to zoom in on our finite groups, and the opens are levels of precision to look at our finite groups. Even though one is not working with a discrete measure, this gives a way to study things discretely.

Exercise 22.17. Show that, for C finite, $\mathrm{Gal}\,(K^{\mathrm{un}}/K)$ have finite $G^{\overline{C}}$ is finite. *Hint:* Try to understand the number of number fields with a specified discriminant.

For each C, we can now ask about the distribution on $\mathrm{Gal}\,(K^{\mathrm{un}}/K)^{\overline{C}}$. Because this will be finite by the above exercise, we now want a distribution on finite groups. In fact, the resulting distribution turns out to be conjecturally discrete (as conjectured in work of Liu, Wood, and Zureick-Brown).

We might now hope we could take the $\frac{1}{\mathrm{Aut}}$ distribution on $\mathrm{Gal}\,(K^{\mathrm{un}}/K)^{\overline{C}}$. However, this cannot be correct, as demonstrated in the following example.

Example 22.18. Take $C = \{\mathbb{Z}/p\mathbb{Z}\}$. Then, $\mathrm{Gal}\,(K^{\mathrm{un}}/K)^{\overline{C}} = \mathrm{Cl}_K/p\,\mathrm{Cl}_K \simeq \mathrm{Cl}_K[p]$.

Since the p-torsion is not distributed according to $\frac{1}{\mathrm{Aut}}$, this cannot be the distribution over general $\overline{C}$. We also described the Cohen-Lenstra distribution as cokernels of matrices. This approach turns out to be more promising.

Question 22.19. What should the analog of cokernel of matrices be?

If we have $M \in M_{n\times n}(\mathbb{Z})$, we can view

$$\mathrm{coker}\, M = \mathbb{Z}^n/(\ n\text{-relations given by the columns of M }).$$

In the non-abelian world, we will describe these distributions in terms of generators and relations. We can view the above as a free abelian group by random relations determined by M. We can now generalize this to non-abelian groups.

Let F_n denote the free group on n-generators. We let $\widehat{F}_n$ denote its profinite completion. We want to construct the quotient of F_n by n random relations. What distribution we get as $n \to \infty$ depends on how we choose our matrix (i.e., is it an arbitrary matrix, or a symmetric matrix, or a matrix preserving a symplectic form, etc.?)

Remark 22.20. In a paper by Melanie Wood and Yuan Liu, the authors studied

$$\widehat{F}_n/(\ n \text{ independent relations from Haar measure }).$$

However, the above group cannot actually be the answer to determining the distribution of $\mathrm{Gal}(K^{\mathrm{un}}/K)$ because there are additional structures constraining $\mathrm{Gal}(K^{\mathrm{un}}/K)$ that we have to take into account to obtain the desired distribution.

22.1. **Liu, Wood, and Zureick-Brown.** The rest of the discussion will be about understanding the distribution of $\mathrm{Gal}(K^{\mathrm{un}}/K)$ following work of Liu, Wood, and Zureick-Brown.

Let $K/\mathbb{Q}$ be a Galois extension with Galois group Γ. Let $K^{\mathrm{un},\prime}$ denote the maximal unramified extension of order prime to $2\,|\Gamma|$. The reason we include 2 is to account for roots of unity in $\mathbb{Q}$. Let $G_K := \mathrm{Gal}\,(K^{\mathrm{un},\prime}/K)$. Here are some things we know about G_K.

Fact 22.21. We have the following three facts about G_K.

(1) The group G_K has a Γ action, generalizing the fact that Cl_K is a $\mathbb{Z}[\Gamma]$ module. We have an exact sequence

(22.1)
$$1 \longrightarrow G_K \longrightarrow \mathrm{Gal}\,(K^{\mathrm{un},\prime}/\mathbb{Q}) \longrightarrow \Gamma := \mathrm{Gal}\,(K/\mathbb{Q}) \longrightarrow 1.$$

We get an action of Γ on G_K using Schur-Zassenhaus, see Remark 22.27.

(2) We next have a restriction generalizing the constraint $\left(\sum_{\gamma\in\Gamma}\gamma\right)\mathrm{Cl}_K = 0$.

Theorem 22.22. *The group G_K is generated by elements of the form $x\gamma(x)^{-1}$ (using the Γ action of the previous point) for $\gamma \in \Gamma_g x \in G_K$.*

In the abelianization, let's check this makes sense.

Exercise 22.23. In the abelian case, a group is generated by elements of the form $x - \gamma(x)$ if and only if the group is annihilated by $\sum_{\gamma\in\Gamma}\gamma$.

(3) There is one further constraint relating to embedding problems. If one has a non-split central extension of Γ-groups

(22.2)
$$1 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 1$$

with $\mathbb{Z}/p\mathbb{Z}$ the trivial Γ-module and a map

(22.3)
$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \searrow & & \\ 1 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \widetilde{H} & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

there exists a lift

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \downarrow & \searrow & \\ 1 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \widetilde{H} & \longrightarrow & H & \longrightarrow & 1 \end{array} \tag{22.4}$$

This follows from (but is not trivial from) the Hasse-Brauer-Noether theorem.

Remark 22.24. It is important we take $\mathbb{Z}/p\mathbb{Z}$ to be the trivial Γ-module, or else the above construction would prohibit certain possibilities for class groups. There does not exist a non-split abelian central extension of a non-trivial Γ-module by a trivial Γ-module. However, in for non-abelian groups, there do exist such extensions.

Corollary 22.25. *If H has a non-split central extension, then $G_K \not\cong H$.*

Remark 22.26. For the third fact of Fact 22.21, the Galois group can have non-split central extensions of size dividing the roots of unity.

Remark 22.27. In general, when we have an exact sequence, the quotient only defines an outer action on the subgroup. An outer action of H on G is not an action, but rather a map from H to $\mathrm{Out}(G)$, the outer automorphisms of G. By definition, the inner automorphisms are automorphisms arising from conjugation, and the outer automorphisms are the quotient of all automorphisms by inner automorphisms.

But now, Schur Zassenhaus tells us that when N, G, H are groups with $\gcd(|N|, |H|) = 1$, there is a section to the exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1 \tag{22.5}$$

which is unique up to conjugacy by elements of N. This section gives us an action, as opposed to only an outer action.

We now want to say what the random group model is subject to the three constraints of Fact 22.21.

We now define the model for G_K. To give some motivation, we now state some facts. Let $\widehat{F_{n|\Gamma|}}$ denote the profinite free group on the $n|\Gamma|$ elements (the profinite completion of $F_{n|\Gamma|}$) γx_i for $\gamma \in G, 1 \leq i \leq n$, coming with the natural Γ action. Consider $\mathscr{F} \subset F_{n|\Gamma|}$ the subgroup defined as

$$\mathscr{F} := \langle y\gamma(y)^{-1} : y \in F_{n|\Gamma|, \gamma \in G} \rangle.$$

Fact 22.28. $\mathscr{F}$ is in fact generated by elements of the form $z\gamma(z)^{-1}$ for $z \in \mathscr{F}, \gamma \in \Gamma$.

Fact 22.29. The third property of Fact 22.21 holds if and only if G_K can be presented in the form

$$G_K \simeq \mathscr{F} / \langle r\gamma(r)^{-1} \rangle_{r \in R, \gamma \in G}$$

Here is the model.

Definition 22.30. We take G_K distributed as

$$\mathscr{F} / \langle r\gamma(r)^{-1} \rangle_{r \in R, \gamma \in G}$$

for r independent Haar random elements in $\mathscr{F}$ and let $n \to \infty$.

Remark 22.31. When we let $n \to \infty$, we want convergence in the weak topology for the topology with basis $U_{H,\overline{C}}$, given above.

23. 12/2/20

Today is the last class. Melanie will try to leave some time for questions at the end of class. She particularly invites questions along the lines of "where can I learn more about this topic."

Today we'll review and then describe some aspects of the proofs of more general conjectures about distributions of unramified extensions.

Fix Γ a finite group and Γ_∞ a subgroup of Γ having order 1 or 2.

Question 23.1. Let Q either be $\mathbb{Q}$ or $\mathbb{F}_q(t)$. Let K varies among Γ fields over Q, i.e., K/Q is Galois with an isomorphism $\mathrm{Gal}(K/Q) \simeq \Gamma$ and a decomposition group over ∞ given by Γ_∞ under the above isomorphism. What is the distribution of $\mathrm{Gal}(K^{\mathrm{un},\prime}/K)$ for varying such K?

Here, the $\prime$ in $K^{\mathrm{un},\prime}$ indicates that the extension is prime to $|\Gamma| \left|\mu_Q\right|$, for μ_Q the roots of unity in Q.

Last class, we described a random group in terms of generators and random relations that was a conjectural answer. How do we detect this distribution? We can use the moments. Recall that the moments are

$$\mathbb{E}\left(\#\mathrm{Surj}\left(\mathrm{Gal}\left(K^{\mathrm{un},\prime}/K\right), H\right)\right)$$

the average number of unramified H extensions of K. The moment problem was also studied in the non-abelian case. See, for example, recent work of Will Sawin. Which moments do we consider? Recall that Γ acts on $\mathrm{Gal}\left(K^{\mathrm{un},\prime}/K\right)$ It is natural to then ask for groups M with a Γ action and look at the Equivariant moments

$$\mathbb{E}\left(\#\mathrm{Surj}_\Gamma\left(\bullet, M\right)\right).$$

Definition 23.2. We call a group with a Γ action is a Γ-group.

23.1. **Γ-equivariant moments.** Equivariant moments should determine the distribution on Γ groups. However, the previous moments should give a distribution on all groups.

Remark 23.3. Clearly, the non-equivariant moments cannot determine the distribution on Γ groups.

Remark 23.4. The equivariant moments can determine the distribution of Γ-groups, subject to certain conditions on growth of these moments. These can determine the distribution on all groups.

Remark 23.5. We should expect that the non-equivariant moments are a function of the equivariant moments. Indeed, this is the case. Let G be a Γ-group and H be a group. Then,

$$\mathrm{Hom}\left(G, H\right) \simeq \mathrm{Hom}_\Gamma(G, \mathrm{Ind}_{\mathrm{id}}^\Gamma H).$$

Here, $\mathrm{Ind}_{\mathrm{id}}^\Gamma H$ denotes the group whose underlying set is H^Γ with Γ permuting the copies of H. The above isomorphism is the "usual" adjunction isomorphism between restriction and induction.

The surjections $\mathrm{Surj}\left(G, H\right) \subset \mathrm{Hom}(G, H)$ defines a subset, which corresponds to $\mathrm{Hom}_\Gamma^*(G, \mathrm{Ind}_{\mathrm{id}}^\Gamma H)$ where the $*$ superscript denotes homomorphisms that surject onto the first factor of H[1] appearing in $H^{\oplus\Gamma} \simeq \mathrm{Ind}_{\mathrm{id}}^\Gamma H$, where this isomorphism is viewed as an isomorphism of sets.

Then,

$$\left|\mathrm{Surj}\left(G, H\right)\right| = \sum_{\substack{S \subset \mathrm{Ind}_{\mathrm{id}}^\Gamma H \\ \Gamma-\text{submodule surjecting onto the first factor of } H}} \left|\mathrm{Surj}_\Gamma\left(G, S\right)\right|.$$

The right hand side is a sum of equivariant moments.

The easiest way to understand the plain moments may often be to do the above translation and compute the Γ moments as above.

We now are trying to understand

$$\mathrm{Surj}_\Gamma\left(\mathrm{Gal}\left(K^{\mathrm{un},\prime}/K\right), M\right).$$

[1]Equally well, we could take any factor; to see if the map on the left hand side is a surjection, it is equivalent to check if the map to any coordinate is a surjection.

We have

$$\begin{array}{c} L \\ \Big\downarrow M, \text{ unramified} \\ K \\ \Big\downarrow \Gamma \\ Q \end{array} \tag{23.1}$$

a tower of extensions, where Γ equivariance of L/K is equivalent to L/Q being Galois. When we were thinking about the degree 2 case for $\Gamma = \mathbb{Z}/2\mathbb{Z}$, we didn't see this because extensions L/K were automatically Γ equivariant and automatically Galois.

Lemma 23.6. *In the above setting, we have* $\mathrm{Gal}(L/Q) \simeq M \rtimes \Gamma$.

Proof. The Galois groups $\mathrm{Gal}(L/Q)$ sits in an exact sequence

$$0 \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/Q) \longrightarrow \mathrm{Gal}(K/Q) \longrightarrow 0 \tag{23.2}$$

Because $(|\Gamma|, |M|) = 1$ the above sequence splits, so $\mathrm{Gal}(L/Q) \simeq M \rtimes \Gamma$. □

We will assume throughout that q is relatively prime to $|\Gamma|$ and $|M|$. Over $Q = \mathbb{F}_q(t)$, we therefore want to count the ratio of

$$\frac{M \rtimes \Gamma \text{ extensions, where the } M \text{ part } L/K \text{ is unramified}}{\Gamma \text{ extensions}}$$

There are Hurwitz spaces $H'_{M\rtimes\Gamma}$ and H_Γ, where the prime H' indicates an inertia condition so that the M part is unramified, and the above ratio is given by

$$\frac{\#H'_{M\rtimes\Gamma}(\mathbb{F}_q)}{\#H_\Gamma(\mathbb{F}_q)}.$$

So, using Lang Weil, the question reduces to: what are the components of these Hurwitz spaces?

Let $C \to \mathbb{P}^1_{\mathbb{F}_q}$ be a Galois G extension. If r is a nontrivial conjugacy class of cyclic subgroups of G for $G = M \rtimes \Gamma$ or Γ so that the inertia type of $C/\mathbb{P}^1$ is r. Define

$$e_r := \sum_{\substack{x \in \mathbb{P}^1_{\mathbb{F}_q} \\ x \text{ has inertia type } r}} \deg x.$$

Remark 23.7. For $G = \mathbb{Z}/2\mathbb{Z}$ or $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ when inertia does not intersect A, there is only one inertia type not intersecting A (since all such elements have order 2 and are conjugate). In our more general Γ extension setup, there are many ways to be ramified.

The datum $(e_r)_r$ is a component invariant.

One can imagine there is a lattice of components of Hurwitz spaces where to each lattice point $(e_{r_1}, \dots, e_{r_k})$ for different ramification types r_i and at that lattice point we put the number of components of the relevant Hurwitz space.

There are now two questions for how to count these.

(1) First, we want to decide how to order points in this lattice. One can project these components to one dimension to obtain a single invariant to count by.

    Example 23.8. The genus of the extension is given by a linear combination of the e_r, as follows from Riemann-Hurwitz. The coefficients involve the order of the cyclic subgroup and the order of Γ.

    Instead of the genus, we can also take a more arithmetic invariant, the product of the ramified places. In other words, we will count by the degree of the reduced branch divisor on $\mathbb{P}^1$.

(2) Second, we want to understand which $(e_r)_r$ have any components at all.

    Example 23.9. If $C \to \mathbb{P}^1$ is a hyperelliptic curve, the degree of the branch divisor is always even.

(3) Third, for the $(e_r)_r$ satisfying the congruence conditions, how many Frobenius fixed components are there?

Remark 23.10. In Melanie's world, the condition that the degree of the branch locus is even is analogous to the fact that discriminants are 0 or 1 mod 4.

Lemma 23.11. *If $C \to \mathbb{P}^1$ is a hyperelliptic curve, the degree of the branch divisor is always even.*

The following proof is not the most straightforward one, but will generalize to relate to $\mathbb{Q}$ extensions well.

Proof. Using Class Field theory quadratic extensions of $\mathbb{F}_q(t)$ correspond to maps

$$J_{\mathbb{F}_q(t)} \xrightarrow{\Phi} \mathbb{Z}/2\mathbb{Z}$$

where ramification is given by $\Phi|_{\mathscr{O}_v^\times} =: \phi_v$ with $\phi_v : \mathscr{O}_v^\times \to \mathbb{Z}/2\mathbb{Z}$. Then, $\phi_v = 1$ if v is unramified in odd characteristic. There is only one nonzero map

$$\phi_v : \mathscr{O}_v^\times \to \kappa(v)^\times \to \mathbb{Z}/2\mathbb{Z}$$

where $\kappa(v)$ is the residue field at v and is a cyclic group of order $q^{\deg v} - 1$.

Let ε be a generator of ${\mathbb{F}_q}^\times$. Then, on the one hand, $\Phi(\varepsilon) = 0$ by definition of $J_{\mathbb{F}_q(t)} = \prod K_v^\times / K^\times$, with 0 the identity element in $\mathbb{Z}/2\mathbb{Z}$. On the other hand, $\Phi(\varepsilon)$ is also equal to the number of ramified v so that ε is not a square in the residue field $\kappa(v)$, modulo 2.

Exercise 23.12. Show that ε is not a square in $\kappa(v)$ if and only if the degree of v is odd.

In conclusion, the number of ramified v, so that $\deg v$ is odd, is even. Hence, the total branch locus degree is even. □

Exercise 23.13. Generalize the above proof to show that all discriminants of number fields over $\mathbb{Q}$ to be 0 or 1 modulo 4. Class field theory is not just about quadratic extensions.

In general, this consideration gives all obstructions to which $(e_r)_r$ are possible.

We are now following the paper of Yuan Liu, Melanie Wood, and David Zureick-Brown.

Suppose we have maps

(23.3)
$$\begin{array}{ccc} C & \longrightarrow & C^{\mathrm{ab}} \\ & \searrow \quad \swarrow & \\ & \mathbb{P}^1 & \end{array}$$

where $C \to \mathbb{P}^1$ is a Γ extension and $C^{\mathrm{ab}} \to \mathbb{P}^1$ is a Γ^{ab} extension. Then, we get a map $J_{\mathbb{F}_q(t)} \to \Gamma^{\mathrm{ab}}$. The fact that $\Phi({\mathbb{F}_q}^\times) = 0$ gives multiple congruence conditions on certain linear combinations of the e_r.

Theorem 23.14 (Liu, Wood, Zureick-Brown)**.** *There are no Hurwitz components when the above conditions fail. When the conditions are satisfied and e_r are sufficiently large, there exist Hurwitz components with these e_r.*

Example 23.15. If the group Γ has a large order and requires many generators, one cannot expect to have any components with very few branch points, because they cannot possibly generate the group. But once one passes silly obstructions like this, there are always components with specified invariants, subject to the above restrictions coming from class field theory.

Finally, we want to address, for the $(e_r)_r$ satisfying the congruence conditions, how many Frobenius fixed components are there? Unfortunately, the number of Frobenius fixed components is an awkward messy number. However, the ratio turns out to be nice. That is, for $(e_r)_r$ as above satisfying the congruence conditions and all e_r sufficiently large, the ratio of numbers of Frobenius fixed components is

$$\frac{\#\text{ Frobenius fixed components of } H'^{,(e_r)_r}_{M\rtimes\Gamma(\mathbb{F}_q)}}{\#\text{ Frobenius fixed components of } H_\Gamma(\mathbb{F}_q)} = \left|H_2(M,\mathbb{Z})^\Gamma\left[\left|\mu_{\mathbb{F}_q(t)}\right|\right]\right|$$

where $H_2(M,\mathbb{Z})$ denotes the Schur multiplier and $\left|\mu_{\mathbb{F}_q(t)}\right| = q-1$. The above is 1 when $(|M|,(q-1)|\Gamma|)$.

This gives the main term, and then one needs to bound the number of e_r when the invariants are not sufficiently large. The final result is that as $q\to\infty$, one obtains the conjectural moments for $\mathrm{Gal}(K^{\mathrm{un},\prime}/K)$.

23.2. **Questions.**

Question 23.16. What is the cutting edge in the number field case?

In certain families, one can find the average size of 2-torsion, the $\mathbb{Z}/2\mathbb{Z}$ moments. See work by Shankar, Ho, and Varma. They compute a single moment. Alex Smith finds the entire distribution of $\mathrm{Cl}_K[2^\infty]$ for quadratic fields.

REFERENCES

[CL84] H. Cohen and H. Lenstra. Heuristics on class groups of number fields. *Number Theory Noordwijkerhout 1983*, pages 33–62, 1984.