Arithmetic Statistics 2025

Abstract

These are the lecture notes of the instructional conference "Arithmetic Statistics" held June 17-20, 2025 at the Ohio State University (organized by Jennifer Park, Dave Anderson, Angelica Cueto, and Stefan Patrikis). The conference featured two mini-courses of four lectures each given by Alexander Smith ("BSD implies Goldfeld") and Jiuya Wang ("Malle's Conjecture and Cohen-Lenstra Heuristics"), and supplemented by background lectures given by PhD students and postdoc participants. For $n = 1 \dots 8$, talk (i.e., section in this document) $2n - 1$ is the background lecture for talk $2n$, which may also rely on some earlier talks.

The conference and subsequent mathematical retreat in which the students worked on the notes was funded by an NSF Research Training Grant, DMS-2231565, and by Ohio State's Mathematics Research Institute.

For more information about the conference and retreat, see https://people.math.osu.edu/cueto.5/RTG/rtg25/RTGConference25.html. For lecture videos from the conference, see https://www.youtube.com/@OSU_RTG_AGNT.

Contents

1 Tauberian Theorems. Speaker: Elia Gorokhovsky. Notes by Luke Wiljanen.

1.1 Introduction

This talk was based on the notes [PTBZ25] by Pierce, Turnage–Butterbaugh, and Zaman.

1.1.1 Number Theory

On the number theoretic side we have arithmetic sequences $\{a_n\}_{n\in\mathbb{N}}$ where $a_n \geq 0$. For example, we could have the sequence

$$a_n = \#\{K/\mathbb{Q} \mid \mathrm{Gal}(K/\mathbb{Q}) \cong G, \mathrm{Disc}_{K/\mathbb{Q}} = n\}.$$

1.1.2 Complex Analysis

From the sequence $\{a_n\}_{n\in\mathbb{N}}$, we can form the Dirichlet series $A(s) = \sum_{n=1}^{\infty} a_n n^{-s}$. Tauberian theorems gives us a way to transform analytic information about the Dirichlet series into arithmetic information about the sequence.

Example 1. The Riemann zeta function $\zeta(s) = A(s) = \sum_{n=1}^{\infty} n^{-s}$ arises as the Dirichlet series for the sequence given by $a_n = 1$ for all n. The Riemann zeta function has some nice properties:

- It has a meromorphic continuation to $\mathbb{C}$ with only one singularity, a pole of order 1 at $s = 1$ with residue 1.
- It has an Euler product $\zeta(s) = \prod_p (1 + p^{-s} + p^{-2s} + \cdots) = \prod_p (1 - p^{-s})^{-1}$ reflecting the Fundamental Theorem of Arithmetic that every positive integer can be written uniquely as a product of prime powers.

Example 2. We can take a_n to be the indicator function of the square-free positive integers, i.e., $a_n = 1$ if n is squarefree and $a_n = 0$ otherwise. Then,

$$A(s) = \prod_p (1 + p^{-s}) = \prod_p \frac{1 - p^{-2s}}{1 - p^{-s}} = \frac{\zeta(s)}{\zeta(2s)}.$$

Thus, we can deduce properties about the squarefree integers by understanding the zeta function.

1.2 Tauberian Theorems

Theorem 3 (Ikehara-Wiener, Delange)**.** *Assume that $A(s)$ has a meromorphic continuation to $\{Re(s) \geq \alpha\}$ for some $\alpha > 0$ and that $A(s)$ has only one pole at $s = \alpha$ of order m. Then,*

$$\sum_{n \leq X} a_n = cX^{\alpha}(\log X)^{m-1} + o(X^{\alpha}(\log X)^{m-1})$$

where c is defined by

$$c = \frac{g(\alpha)}{\alpha(m-1)!}$$

if

$$A(s) = \frac{g(s)}{(s-\alpha)^m} + h(s)$$

for holomorphic functions g and h with $g(\alpha) \neq 0$.

Remark 4. The assumption that $A(s)$ has only one pole is crucial as we will see later.

Example 5. For the Riemann zeta function $A(s) = \zeta(s) = \sum_{n=1}^{\infty} n^{-s}$, we have $\alpha = 1$, $m = 1$, and $c = 1$. If we were to apply the theorem to this case, we would get the celebrated result that $\sum_{n \leq X} 1 = X + o(X)$ which is very useful.

Example 6. For the indicator of the squarefree integers, we had $A(s) = \zeta(s)/\zeta(2s)$. In this case, we have a pole at $s = 1$ of order 1 with residue $1/\zeta(2) = 6/\pi^2$. Under mild assumptions, for example if we assume the Riemann hypothesis, then

$$\sum_{\substack{n \leq X \\ n \text{ squarefree}}} 1 \sim \frac{6}{\pi^2} X.$$

Of course, this is known without any assumptions; for example, see the book by Hua [Hua82, Theorem 6.1] where this asymptotic estimate is proved with an error bound by elementary means.

Example 7. We will now see why the only one pole assumption is necessary. Consider the Dirichlet series

$$A(s) = \zeta(s) + \frac{1}{2}\zeta(s+i) + \frac{1}{2}\zeta(s-i) = \sum_{n=1}^{\infty} \frac{1 + \cos(\log(n))}{n^s}$$

for the sequence $a_n = 1 + \cos(\log(n))$. Then, $\sum_{n \leq X} a_n$ looks like $X + \sum_{n \leq X} \cos(\log(n))$. If we approximate the sum by an integral, we have that

$$\sum_{n \leq X} \cos(\log(n)) \approx \int_0^X \cos(\log t) dt = \frac{X}{\sqrt{2}} \cos\left(\log(X) - \frac{\pi}{4}\right).$$

If we assume this estimate is not too bad, then no estimate of the form in the theorem can hold.

Theorem 8. *Assume that*

- *$A(s)$ has a meromorphic continuation to $\{Re(s) \geq \alpha - \delta\}$ where $0 < \delta < \alpha$,*
- *$A(s)$ has only one pole located at $s = \alpha$ and which is of order m,*
- *and the growth condition that on $Re(s) = \alpha - \delta$ we have the estimate*

$$|A(s)| \leq C(1 + |\Im(s)|)^{\kappa} (\log(3 + |\Im(s)|)^{m-1}$$

for some real number $\kappa \geq 0$.

Then,

$$\sum_{n \leq X} a_n = \text{Res}_{s=\alpha} \left(A(s) \frac{X^s}{s} \right) + \begin{cases} \mathcal{O}(X^{\alpha - \frac{\delta}{\kappa+1}} (\log X)^{m-1} & \text{if } \kappa > 0 \\ \mathcal{O}(X^{\alpha - \delta} (\log X)^m & \text{if } \kappa = 0. \end{cases}$$

Remark 9. We now look more closely at the residue term. Assume $A(s) = \frac{g(s)}{(s-\alpha)^m} + h(s)$ for holomorphic g and h, as before. Then,

$$\text{Res}_{s=\alpha} \left(A(s) \cdot \frac{X^s}{s} \right) = \frac{1}{(m-1)!} \lim_{s \to \alpha} \left(\frac{d^{m-1}}{ds^{m-1}} (g(s) + (s-\alpha)^m h(s)) \cdot X^s / s \right) = cX^{\alpha} (\log X)^{m-1} + \cdots .$$

1.3 Indications of the Proof

We break the proof into 4 steps:

- smoothing,
- Mellin inversion and Perron's formula,
- set up a contour integral,
- and bounding terms in the contour integral.

1.3.1 Smoothing

Instead of working with $\sum_{n\leq X} a_n = \sum_{n=1}^{\infty} a_n \mathbf{1}_{\{n\leq X\}}(n)$, we replace the indicator function $\mathbf{1}_{\{n\leq X\}}(n)$ with a smooth approximation $\varphi(n)$. So, we consider a sum $\sum_{n=1}^{\infty} a_n\varphi(n)$. The hard part is choosing a suitable smooth approximation φ; everything else is fairly standard.

1.3.2 Mellin Inversion and Perron's Formula

We have that

$$\sum_{n\leq X} a_n\varphi(n) = \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} A(s)\hat{\varphi}(s)ds$$

where $\hat{\varphi}(s) = \int_0^{\infty} \varphi(u)u^{s-1}du$ is the Mellin transform of φ.

1.3.3 Set Up a Contour Integral

We integrate along a rectangular contour from $\sigma - iT$ to $\sigma + iT$ to $\beta + iT$ to $\beta - iT$ where $\alpha - \delta \leq \beta < \alpha < \sigma$. Then,

$$\begin{aligned}\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT} A(s)\hat{\varphi}(s)ds - \frac{1}{2\pi i}\int_{\beta-iT}^{\beta+iT} A(s)\hat{\varphi}(s)ds \\ = \frac{1}{2\pi i}\int_{\beta+iT}^{\sigma+iT} A(s)\hat{\varphi}(s)ds - \frac{1}{2\pi i}\int_{\beta-iT}^{\sigma-iT} A(s)\hat{\varphi}(s)ds + \mathrm{Res}_{s=\alpha}\left(A(s)\hat{\varphi}(s)\right).\end{aligned}$$

1.3.4 Bounding Terms in the Contour Integral

One can use the Phragmen–Lindelöf convexity principle to get a growth condition on the region

$$\alpha - \delta \leq Re(s) \leq \sigma.$$

One can then show that the horizontal integrals

$$\frac{1}{2\pi i}\int_{\beta+iT}^{\sigma+iT} A(s)\hat{\varphi}(s)ds$$

and

$$\frac{1}{2\pi i}\int_{\beta-iT}^{\sigma-iT} A(s)\hat{\varphi}(s)ds$$

will not contribute as $T \to \infty$, and that the integral

$$\frac{1}{2\pi i}\int_{\beta-iT}^{\beta+iT} A(s)\hat{\varphi}(s)ds$$

will affect the error term.

1.4 Squarefree Example

Consider the sequence

$$a_n = \begin{cases} 0 & n \text{ is not squarefree} \\ 2^{\omega(n)} & n \text{ is squarefree} \end{cases}$$

where $\omega(n)$ is the number of prime divisors of n. We have the Dirichlet series $A(s) = \prod_p (1 + 2p^{-s})$. Since $\log A(s) \approx \sum_p 2p^{-s}$, the Dirichlet series $A(s)$ converges absolutely if $Re(s) > 1$.

We would like to talk about a meromorphic continuation of $A(s)$, so we relate $A(s)$ to the main Dirichlet series that we know something about, namely the Riemann zeta function $\zeta(s)$. We have that

$$(1+2p^{-s})(1-p^{-s})^2 = 1-3p^{-2s}+2p^{-3s}.$$

Thus,

$$A(s) = \zeta(s)^2 \prod_p (1-3p^{-2s}+2p^{-3s}).$$

Let $H(s) = \prod_p (1-3p^{-2s}+2p^{-3s})$. Since $\log H(s) \approx \sum_p (-3p^{-2s}+2p^{-3s})$, we find that $H(s)$ converges absolutely for $Re(s) > 1/2$.

Then, $A(s)$ has a pole at $\alpha = 1$ of order $m = 2$. Standard convexity bounds give a growth condition:

$$|A(s)| \lesssim C(1+|\mathrm{Im}(s)|)^{\delta+\epsilon}$$

on $\mathrm{Re}(s) = \alpha - \delta$ for any $\varepsilon > 0$.

The main term is

$$\mathrm{Res}_{s=\alpha}\left(A(s)\frac{X^s}{s}\right) = \lim_{s\to 1}\frac{d}{ds}\left((s-1)^2\zeta(s)^2 H(s)\right) = H(1)Xlog(X) + (H'(1)-H(1))X$$

with error term $O(X^{\alpha-\frac{\delta}{k+1}}\log X) = O(X^{2/3+\varepsilon})$. Then, the theorem says

$$\sum_{\substack{n\le X \\ \text{squarefree}}} 2^{\omega(n)} = H(1)X\log(X) + (H'(1)-H(1))X + O(X^{2/3+\varepsilon}).$$

2 Malle's conjecture, lecture 1. Speaker: Jiuya Wang. Notes by Jake Huryn.

2.1 Setup of the problem

In this talk, all number fields live inside $\overline{\mathbb{Q}} \subseteq \mathbb{C}$. For a number field K, we write $G_K \coloneqq \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for its absolute Galois group.

Question 1. How many number fields are there?

Obviously, there is a countable infinity of number fields; we can get a more enlightening and meaningful answer if we count fields K that are "bounded in size" in some way, e.g. with absolute discriminant $\mathrm{Disc}(K) \leq X$. We will ask a more precise question in which we also specify that the Galois group be a fixed transitive permutation subgroup G of S_m, where we view G as being defined up to conjugacy inside S_m. By this we mean the following:

Definition 10. Let G be as above, and let K be a number field. Let $\widetilde{K}$ be the Galois closure of K in $\overline{\mathbb{Q}}$, i.e. the smallest subfield of $\overline{\mathbb{Q}}$ which contains K and is Galois over $\mathbb{Q}$. For example, we may pick a presentation $K = \mathbb{Q}(\alpha)$, and let $f(t) \in \mathbb{Q}[t]$ be the minimal polynomial of α; then $\widetilde{K}$ is the field obtained by adjoining all m roots of $f(t)$ to $\mathbb{Q}$. We say that K *has Galois group* G if $[K : \mathbb{Q}] = m$ and the following equivalent statements hold.

- The action of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ on the roots of $f(t)$ identifies $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ with (a conjugate of) G after picking a bijection between the set of roots and $\{1, \ldots, n\}$.
- The action of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ on the coset space $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})/\mathrm{Gal}(\widetilde{K}/K)$ identifies $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ with (a conjugate of) G after picking an appropriate bijection.
- The action of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ on the set of embeddings $K \hookrightarrow \overline{\mathbb{Q}}$ identifies $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ with (a conjugate of) G after picking an appropriate bijection.

Definition 11. Let G be as above. For $X \in \mathbb{R}$, let $E(G, X)$ denote the set of number fields of absolute discriminant $\leq X$ which have Galois group G in the sense of Definition 10.

Remark 12. Let G be as above.

1. The specific embedding $G \hookrightarrow S_m$ carries information additional to G and m. For example, S_4 can be given the structure of a transitive permutation subgroup of S_6 in two distinct (i.e. non-conjugate) ways.
2. If $L/\mathbb{Q}$ is finite Galois with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$, then $L/\mathbb{Q}$ has a unique subextension $K/\mathbb{Q}$ which has Galois group G in the sense of Definition 10, namely, the fixed field of $G \cap \{\sigma \in S_m : \sigma(1) = 1\}$ Therefore, $\bigcup_{X \in \mathbb{R}} E(G, X)$ is in bijection with $\mathrm{Surj}_{\mathrm{cts}}(G_{\mathbb{Q}}, G)/\sim$, the set of continuous surjections $G_{\mathbb{Q}} \twoheadrightarrow G$ modulo the action of $\mathrm{Aut}(G)$; the fixed permutation representation of G simply controls the images of the individual sets $E(G, X)$ inside $\mathrm{Surj}_{\mathrm{cts}}(G_{\mathbb{Q}}, G)/\sim$. Explicitly, the bijection puts in correspondence a continuous surjection $\rho \colon G_{\mathbb{Q}} \twoheadrightarrow G$ with the field $K_\rho \coloneqq \overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)}$.

2.2 Counting quadratic extensions

Recall that the quadratic extensions of $\mathbb{Q}$ are parameterized by the squarefree integers $\neq 1$; such an integer d corresponds to the field $\mathbb{Q}(\sqrt{d})$, which has discriminant $D = d$ if $d \equiv 1 \pmod 4$, or $D = 4d$ if $d \equiv 2, 3 \pmod 4$. This allows us to estimate $\#E(C_2, X)$; here are two approaches.

1. (Analytic). We consider two counting problems separately. For $j = 0, 1$, let $N_j(X)$ be the number of discriminants D such that $|D| \leq X$ and $D \equiv j \pmod 2$, so that $\#E(C_2, X) = N_0(X) + N_1(X)$.

Notice that $N_1(X)+1$ equals the number of odd squarefree positive integers n such that $n \le X$. By inclusion–exclusion,

$$N_1(X)+1 = \sum_{\substack{k \le X \\ k \text{ odd squarefree}}} 1 = \sum_{\substack{n \le \sqrt{X} \\ n \text{ odd squarefree}}} (-1)^{\omega(n)} \sum_{\substack{k = n^2 m \le X \\ k \text{ odd}}} 1$$

The interior sum in the final expression equals $X/(2n^2)+\epsilon_n$ for some $\epsilon_n \in [0,1)$, so

$$N_1(X) = O(\sqrt{X}) + \sum_{\substack{n \le \sqrt{X} \\ k \text{ odd squarefree}}} (-1)^{\omega(n)} \cdot \frac{X}{2n^2} = O(\sqrt{X}) + X \cdot \prod_{p \neq 2} \left(1 - \frac{1}{p^2}\right).$$

So $N_1(X) = cX + O(\sqrt{X})$ for $c = \frac{1}{2}\prod_{p \neq 2}(1-p^{-2})$. We leave it as an exercise to estimate $N_0(X)$.

2. (Algebraic). We are going to transform the problem into a Dirichlet series and apply a Tauberian theorem. Let a_D be the number of extensions of $\mathbb{Q}$ of degree ≤ 2 with absolute discriminant *equal to* D. Then

$$a_D = \begin{cases} 1, & 2 \nmid D,\ D \text{ squarefree} \\ 1, & 4 \mid D,\ D/4 \text{ squarefree},\ D/4 \equiv 1,3 \pmod 4 \\ 2, & 4 \mid D,\ D/4 \text{ squarefree},\ D/4 \equiv 2 \pmod 4 \\ 0, & \text{otherwise.} \end{cases}$$

We obtain an Euler product for the corresponding Dirichlet series:

$$\sum_{D \ge 1} \frac{a_D}{D^s} = (1 + 4^{-s} + 2 \cdot 8^{-s}) \cdot \prod_{p \neq 2} (1 + p^{-s}).$$

Comparing this to Riemann's zeta function and applying the Ikehara–Wiener Tauberian theorem, we find that $\#E(C_2, X) \sim cX$ with $c = 1/\zeta(2)$.

The "algebraic approach" is very useful for counting extensions for which one has significant structural information about the family of extensions in question (such as quadratic extensions as above, or abelian extensions more generally, as we'll see in the next section). The "analytic approach" is more useful in other cases, such as counting extensions with Galois group S_n.

2.3 Counting abelian extensions

Now let A be an arbitrary abelian group. We are going to use the "algebraic approach" to guess the size of $\#E(A, X)$.[1]

As in §2.2, there is just one faithful transitive permutation representation of A, namely the regular representation. In other words, we aim to count finite Galois extensions $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong A$ as abstract groups, which we will view as continuous surjections $G_{\mathbb{Q}} \twoheadrightarrow A$ up to the action of $\mathrm{Aut}(A)$.

The key tool will be the Kronecker–Weber theorem, which says that the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ equals $\mathbb{Q}(\mu_\infty)$, the maximal cyclotomic extension of $\mathbb{Q}$. In particular, $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \cong \prod_p \mathbb{Z}_p^\times$, so a continuous homomorphism $\rho\colon G_{\mathbb{Q}} \to A$ is the same as a collection of continuous homomorphisms $\rho_p\colon \mathbb{Z}_p^\times \to A$ for each p such that ρ_p is trivial for all but finitely many p. [2]

Given such a ρ, we need to understand $\mathrm{Disc}(K_\rho)$. Factor it into powers of primes: $\mathrm{Disc}(K_\rho) = \prod_p \mathrm{Disc}_p(K_\rho)$. Then $\mathrm{Disc}_p(K_\rho) = \prod_{v \mid p} \mathrm{Disc}(K_{\rho,v})$, where v ranges over the places of K_ρ lying above p and $K_{\rho,v}$ is the completion at v. When $p \nmid \#\mathrm{Img}(\rho_p)$, the extension $K_{\rho,v}/\mathbb{Q}_p$ is tamely ramified, so

$$\mathrm{Disc}_p(K_\rho) = \prod_{v \mid p} p^{(e_v - 1) f_v} = p^{[K_\rho:\mathbb{Q}] - [K_\rho:\mathbb{Q}]/e_p}$$

[1] See [Wri89] for a proof that the guess is correct.

[2] Continuity and the definition of the product topology forces ρ to factor through $\mathbb{Z}_{p_1}^\times \times \cdots \times \mathbb{Z}_{p_k}^\times$ for some distinct primes $p_1, \ldots, p_k$.

where e_v and f_v are, respectively, the ramification and inertial degrees of $K_{\rho,v}/\mathbb{Q}_p$, and e_p is the ramification degree of p in $K_\rho/\mathbb{Q}$. Note that if $p \neq 2$, then $e_p = \mathrm{ord}(\rho_p(\xi))$, where ξ is a topological generator of $\mathbb{Z}_p^\times$, since $\mathbb{Z}_p^\times$ is the inertia group of $\mathbb{Q}(\mu_\infty)$ at p. Since we have fixed A, the "wildly ramified" case $p \mid \#\mathrm{Img}(\rho_p)$ only rarely occurs, so we will ignore it below, along with the prime 2.

Instead of counting surjections, it will be easier to count *all* homomorphisms, and then sieve out the non-surjections using Möbius inversion. Let $N \coloneqq \#A$. Given any continuous $\rho\colon G_\mathbb{Q} \to A$, define $\mathrm{Disc}(\rho) \coloneqq \mathrm{Disc}(K_\rho)^{N/[K_\rho:\mathbb{Q}]}$, the points being that $\mathrm{Disc}(\rho) = \mathrm{Disc}(K_\rho)$ if ρ is surjective, and $\mathrm{Disc}_p(\rho)$ depends only on n and ρ_p for tamely ramified p. Then

$$\#\mathrm{Surj}_{\mathrm{cts}}(G_\mathbb{Q}, A; X) = \sum_{B \leq A} \#\mathrm{Hom}_{\mathrm{cts}}(G_\mathbb{Q}, A; B; X) \cdot \mu(A, B), \tag{2.1}$$

where μ denotes the Möbius function of the lattice of subgroups of A, and $\mathrm{Hom}_{\mathrm{cts}}(G_\mathbb{Q}, A; B; X)$ is the set of continuous homomorphisms $\rho\colon G_\mathbb{Q} \to A$ with $\mathrm{Img}(\rho) \subseteq B$ and $\mathrm{Disc}(\rho) \leq X$ (similarly with $\mathrm{Surj}_{\mathrm{cts}}(G_\mathbb{Q}, A; X)$).

Let a_D denote the number of continuous homomorphisms $\rho\colon G_\mathbb{Q} \to A$ such that $\mathrm{Disc}(\rho) = D$. Because $\mathrm{Disc}_p(\rho)$ only depends on ρ_p and n, we have an Euler product if we ignore the wild ramification:

$$\sum_{D \geq 1} \frac{a_D}{D^s} \approx \prod_{p \nmid 2N} (\text{polynomial in } p^{-s} \text{ with nonnegative coefficients}).$$

For the $p \nmid 2N$, we only pick up ρ_p which factor through $\mathbb{Z}_p^\times \twoheadrightarrow \mathbb{F}_p^\times$, and we can use our formula for the discrimant of a tamely ramified extension:

$$\sum_{D \geq 1} \frac{a_D}{D^s} \approx \prod_{p \nmid 2N} \sum_{\substack{y \in A \\ \mathrm{ord}(y) \mid p-1}} \frac{1}{p^{\mathrm{ind}(y) \cdot s}},$$

where $\mathrm{ind}(y) \coloneqq N - N/\mathrm{ord}(y)$.

Now let a and r be, respectively, the minimal values of $\mathrm{ind}(y)$ and $\mathrm{ord}(y)$ as y ranges over $A \smallsetminus \{1\}$. That is, r is the smallest prime factor of N, and $a = N - N/r$. Then the factors in the product above are polynomials in p^{-s} of the form $1 + \delta(p)\phi(r)b \cdot p^{-as} + O(p^{-(a+1)s})$, where

- $\delta(p) = 1$ if $p \equiv 1 \pmod r$, otherwise $\delta(p) = 0$;
- b is the number of $y \in A/\!\sim$ satisfying $\mathrm{ind}(y) = a$, where $A/\!\sim$ is the quotient of A by the action of $\widehat{\mathbb{Z}}^\times$ via $n \cdot z \coloneqq z^n$ (which preserves $\mathrm{ind}(z)$; equivalently, the action of $G_\mathbb{Q}$ on A via the cyclotomic character).

Thus, by comparing to Dirichlet L-functions, $\sum_{D \geq 1} a_D \cdot D^{-s}$ defines a meromorphic function on $\{s \in \mathbb{C} \mid \mathrm{re}(s) > 1/(a+1)\}$ with its only pole in this region at $s = 1/a$, which is of order b.[3] So, according to Ikehara–Wiener Tauberian theorem, we should have

$$\#\mathrm{Hom}_{\mathrm{cts}}(G_\mathbb{Q}, A; A; X) \sim c_0 X^{1/a} (\log X)^{b-1} \tag{2.2}$$

[3] Here is an explanation, following [Alb24, Example 6.2]. We are interested in a Dirichlet series $f(s)$ of the form

$$f(s) = \prod_{p \equiv 1 \,(\mathrm{mod}\, r)} (1 + \phi(r)b \cdot p^{-as} + p^{-(a+1)s} \cdot g_p(p^{-s})) \cdot \prod_p (1 + p^{-(a+1)s} \cdot h_p(p^{-s})) =: A(s) \cdot B(s),$$

where g_p and h_p are polynomials with uniformly bounded coefficients and degrees. First consider $B(s)$. Fix $x > 1$, and set $B_x(s) \coloneqq \prod_{p \geq x} (1 + p^{-(a+1)s} \cdot h_p(p^{-s}))$. Find C such that $|h_p(t)| \leq C$ for all p and $t \in [0, 1]$. Then

$$|\log B_x(s)| \leq \sum_{p \geq x} \sum_{k \geq 1} \frac{(p^{-(a+1)\sigma} \cdot |h_p(p^{-s})|)^k}{k} \leq \sum_{p \geq x} \sum_{k \geq 1} C^k \cdot (p^k)^{-(a+1)\sigma} \leq \sum_{p \geq x} \sum_{k \geq 1} C^{\log_x(p^k)} \cdot (p^k)^{-(a+1)\sigma}$$

where $\sigma \coloneqq \mathrm{re}(s)$. Now view this double sum as a sum over prime powers p^k; we get something bigger by including all positive integers:

$$|\log B_x(s)| \leq \sum_{n \geq 1} C^{\log_x(n)} \cdot n^{-(a+1)\sigma} = \sum_{n \geq 1} n^{\log_x(C) - (a+1)\sigma}$$

for some $c_0 > 0$. In certain cases, (2.1) and (2.2) together (plus the analogous estimates for $\#\mathrm{Hom}_{\mathrm{cts}}(G_{\mathbb{Q}}, A; B; X)$ for $B \leq A$) imply that $\#E(A, X) \sim cX^{1/a}(\log X)^{b-1}$ for some $c > 0$,[4] which turns out to be correct in general.

2.4 Counting general extensions: Expectations

Fix $G \subseteq S_N$. As we saw in the case of abelian extensions, the most important part of the discriminant comes from tame ramification.

For each p, fix an embedding $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$. If $\rho\colon G_{\mathbb{Q}} \to G$ is such that $K_\rho/\mathbb{Q}$ is tamely ramified at p (e.g. if $p \nmid \#G$), then $\rho|_{G_{\mathbb{Q}_p}}$ factors through the maximal tamely ramified quotient $G_{\mathbb{Q}_p}^{\mathrm{tr}}$ of $G_{\mathbb{Q}_p}$, which is isomorphic to $\langle x_p, y_p \mid x_p y_p x_p^{-1} = y_p^p \rangle$ (here x_p stands for a Frobenius element). For such p, we still have

$$\mathrm{Disc}_p(\rho_p) = p^{[K_\rho:\mathbb{Q}]-[K_\rho:\mathbb{Q}]/e_p},$$

where $e_p = \mathrm{ord}(\rho_p(y_p))$. For $y \in G$, let us again write $\mathrm{ind}(y) \coloneqq N - N/\mathrm{ord}(y)$; note that $N/\mathrm{ord}(y)$ equals the number of orbits for the action of y on S_N.

Now for a finite set S of primes, let G_S be the Galois group of the maximal unramified-outside-S extension of $\mathbb{Q}$. We will imagine that G_S behaves like the free product $\bigstar_{p\in S} I_p$, where I_p denotes the inertia group of $G_{\mathbb{Q}_p}$ (a precise statement along these lines is "Riemann's existence theorem for number fields"). According to this heuristic, a map $\rho\colon G_{\mathbb{Q}} \to G$ is determined by the elements $\rho_p(y_p)$ (plus possibly more complicated behavior at the finitely many primes dividing $\#G$, which we'll ignore). Moreover, if $\rho_p(y_p)$ is chosen, we blindly guess that with a probability of $1/\#G$ a given $x \in G$ determines a homomorphism $G_{\mathbb{Q}_p}^{\mathrm{tr}} \to G$ by setting $\rho_p(x_p) \coloneqq x$. So, we are led to examine the Dirichlet series

$$\begin{aligned}\prod_{p\nmid \#G} \sum_{\substack{x,y\in G\\ xyx^{-1}=y^p}} \frac{1}{\#G \cdot p^{\mathrm{ind}(y)\cdot s}} &= \prod_{p\nmid \#G} \sum_{\substack{y\in G\\ y\sim y^p}} \frac{1}{p^{\mathrm{ind}(y)s}} \cdot \frac{\#\{x \in G \mid xyx^{-1} = y^p\}}{\#G} \\ &= \prod_{p\nmid \#G} \sum_{\substack{y\in G\\ y\sim y^p}} \frac{1}{p^{\mathrm{ind}(y)\cdot s}} \cdot \frac{1}{\#C_G(y)} \\ &= \prod_{p\nmid \#G} \sum_{\substack{\mathcal{C}\subseteq G\\ \mathcal{C}=\mathcal{C}^p}} \frac{1}{p^{\mathrm{ind}(\mathcal{C})\cdot s}},\end{aligned}$$

Thus $B_x(s)$ is holomorphic and nonvanishing when $\mathrm{re}(s) > (\log_x(C)+1)/(a+1)$. So $B(s)$ is holomorphic when $\mathrm{re}(s) > 1/(a+1)$. Also, $B(s)$ is nonvanishing at $s = 1/a$, since the coefficients of h_p are positive. Now we turn to $A(s)$. We may write

$$A(s) = \prod_{p\nmid r} \left(1 + \sum_{\chi \bmod r} \chi(p) b \cdot p^{-as} + O(p^{-(a+1)s})\right),$$

where χ is ranging over all Dirichlet characters mod r. Now we multiply by a "strategic Euler factor" for each term in the sum, factor out the denominator, and expand the numerator:

$$A(s) = \prod_{p\nmid r} \frac{(1 + \sum_\chi \chi(p) b p^{-as} + p^{-(a+1)s} g_p(s)) \cdot \prod_\chi (1 - \chi(p)p^{-as})^b}{\prod_\chi (1 - \chi(p)p^{-as})^b} = \prod_\chi L(as, \chi)^b \cdot \prod_{p\nmid r} (1 + O(p^{-(a+1)s})).$$

As in the argument for $B(s)$, the second product is holomorphic if $\mathrm{re}(s) > 1/(a+1)$, and is nonvanishing at $s = 1/a$ because the coefficients of g_p are nonnegative and $1 - \chi(p)p^{-1} \neq 0$. Moreover, it is well known that if $\chi \neq 1$, then $L(s, \chi)$ is an entire function nonvanishing at $s = 1$, and $L(s, 1)$ is holomorphic on $\mathbb{C} \smallsetminus \{1\}$ and has a simple pole at $s = 1$. It follows from the above that $f(s)$ is holomorphic when $\mathrm{re}(s) > 1/(a+1)$ aside from a pole of order b at $s = 1/a$.

[4] For example, if $A = C_\ell^k$ with ℓ prime, then (2.1) and (2.2) together imply that $\#E(A, X) \sim c' X^{1/\phi(\ell^k)} (\log X)^{\ell^k - 2}$. If A does not have this form, it appears that (2.2) is not sharp enough to say anything about $\#E(A, X)$ other than the upper bound $\#E(A, X) = O(X^{1/a}(\log X)^{b-1})$; one needs to know about the constant c.

where $\mathcal{C}$ is ranging over all conjugacy classes of G. An analysis of this series very similar to the one carried out for abelian extensions[5] leads us to make the following conjecture:

Conjecture (Malle's conjecture)**.** *We have $\#E(G,X) = cX^{1/a}(\log X)^{b-1}$ for some $c > 0$, where a is the minimal value of* $\mathrm{ind}(\mathcal{C})$ *over all nontrivial conjugacy classes $\mathcal{C}$ of G and $b = \#(\mathcal{C}_{\min}/\sim)$, where $\mathcal{C}_{\min}$ is the set of conjugacy classes whose index is a and $\sim$ is the action of $\widehat{\mathbb{Z}}^\times$ (equivalently, of $G_{\mathbb{Q}}$ via the cyclotomic character).*

The reader is warned that this conjecture is *false*, as we will see in the future lectures. But the known counterexamples are due to roots of unity, and we expect that Malle's conjecture holds if one considers only number fields K satisfying $K \cap \mathbb{Q}(\mu_\infty) = \mathbb{Q}$.

[5]Here is a brief sketch. Let a be the minimal value of $\mathrm{ind}(\mathcal{C})$ as $\mathcal{C}$ ranges over all nontrivial conjugacy classes of G, and set $r \coloneqq \mathrm{ord}(\mathcal{C})$ for any such $\mathcal{C}$. Again, r is the smallest prime factor of $\#G$, and $a = N - N/r$. For any integer u, let $\mathcal{C}_{\min,u}$ denote the set of $\mathcal{C}$ such that $\mathrm{ind}(\mathcal{C}) = a$ and $\mathcal{C} = \mathcal{C}^u$, and set $b'_u \coloneqq \#\mathcal{C}_{\min,u}$. Note that if $u \equiv u' \pmod r$, then $\mathcal{C}_{\min,u} = \mathcal{C}_{\min,u'}$. Thus our Dirichlet series of interest takes the form

$$\prod_p (1 + b'_p p^{-as} + O(p^{-(a+1)s})) = \prod_{d \bmod r} \left(\prod_{p \equiv d \,(\mathrm{mod}\, r)} (1 + b'_d p^{-as} + O(p^{-(a+1)s})) \right).$$

Fixing d, the inner product in the final expression equals

$$\prod_{p \equiv d \,(\mathrm{mod}\, r)} \left(1 + \sum_{\chi \bmod r} \frac{b'_d}{\chi(d)\phi(r)} \cdot \chi(p) p^{-as} + O(p^{-(a+1)s}) \right).$$

Using the "strategic Euler factor" method outlined in footnote 3, this equals

$$\prod_{\chi \bmod r} L(as, \chi)^{b'_d/(\chi(d)\phi(r))}$$

up to factor which is holomorphic for $\mathrm{re}(s) > 1/(a+1)$ and nonvanishing at $s = 1/a$. (Writing this out rigorously would require carefully dealing with these non-integer exponents.) So our Dirichlet series of interest is holomorphic for $\mathrm{re}(s) > 1/(a+1)$ aside from a pole at $s = 1/a$ of order $\sum_{d \bmod r} b'_d/\phi(r)$. This number equals the integer b in the statement of Malle's conjecture.

3 The Birch and Swinnerton-Dyer Conjecture. Speaker: Tristan Phillips. Notes by Yen-Kang (Ted) Fu.

The essence of Diophantine Equations are integral ($\mathbb{Z}$) or rational ($\mathbb{Q}$) solutions to polynomial equations.

Example 13 (Diophantus, 250 CE)**.** Divide a given number into two numbers such that their product is a cube minus its side.

This question can be formulated as:
Given $a \in \mathbb{Z}$, does there exist $x, y \in \mathbb{Q}$ such that

$$y(a-y) = x^3 - x?$$

Diophantus found a solution when $a = 6$: $(x, y) = (17/9, 26/27)$.

Example 14 (1800 BCE)**.** Which right triangles have integral side lengths?

This can be formulated as:

$$x^2 + y^2 = z^2 \quad x, y, z \in \mathbb{Z}.$$

Divide by z (when $z \neq 0$), we get

$$x^2 + y^2 = 1 \quad x, y \in \mathbb{Q}.$$

Example 15. What integers are the area of a right triangle with rational side lengths? Integers that have this property are called congruent numbers.

7 is a congruent number since it's the area of the right triangle of side lengths

$$\left(\frac{24}{5}, \frac{35}{12}, \frac{337}{60}\right).$$

Fermat proved that 1 is not a congruent number using descent. This implies that every perfect square (e.g. $45^2 = 2025$) is not congruent by rescaling.

The question about congruent numbers can be formulated as:
For $n \in \mathbb{Z}$, does there exist $x, y, z \in \mathbb{Q}$ such that

$$x^2 + y^2 = z^2 \quad \text{and} \quad \frac{xy}{2} = n?$$

Example 16 (Fermat, 1637)**.** For $n \geq 3$, there's no trivial integral solution to

$$x^n + y^n = z^n.$$

When studying rational solutions to polynomials, we can first classify the polynomials by the number of variables.

In 1 variable, regardless of the degree, we can use

Theorem 17 (Rational Root Theorem)**.** *Let*

$$f(x) = c_n x^n + \cdots + c_0, \quad c_0 c_n \neq 0,$$

then any rational solution a/b (with $(a, b) = 1$) must satisfy

$$a \mid c_0 \quad \textit{and} \quad b \mid c_n.$$

In 2 variables, we can further classify the polynomial by its degree.

3.1 Degree 1

Let

$$f(x) = ay + bx + c \in \mathbb{Q}[x, y], \quad a, b \neq 0.$$

The rational solutions are

$$(x, y) = \left(s, -\frac{bs + c}{a}\right), \quad s \in \mathbb{Q}.$$

3.2 Degree 2

Example 18. Let

$$f(x, y) = x^2 + y^2 - 3.$$

Then $f(x, y) = 0$ has no rational solution.

Example 19. Let

$$f(x, y) = x^2 + y^2 - 1.$$

Then $f(x, y) = 0$ has infinitely many rational solution.

More precisely, it's clear that $(x, y) = (-1, 0)$ is a rational solution. Suppose (a, b) is another rational solution, then the slope s of the line through $(-1, 0)$ and (a, b) must be rational. In fact, the converse is also true:

Theorem 20. *There is a bijection*

$$\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\} \longleftrightarrow \left\{\textit{rational solution to } x^2 + y^2 = 1\right\}$$
$$s \mapsto \left(\frac{1 - s^2}{1 + s^2}, \frac{2s}{1 + s^2}\right).$$

Corollary 21. *Any right triangle with integral side lengths must be similar to a triangle with side lengths*

$$\left(m^2 - n^2, 2mn, m^2 + n^2\right)$$

for some $m, n \in \mathbb{N}$.

Theorem 22. *If* $f(x, y) \in \mathbb{Q}[x, y]$ *is of degree* 2*, then*

$$\#\left\{(x, y) \in \mathbb{Q} : f(x, y) = 0\right\} \in \{0, \infty\}.$$

Remark 23. This theorem is not entirely correct. For example, $x^2 + y^2 = 0$ has exactly 1 solution. However, it's true in the projective space.

Theorem 24. *If* $F(X, Y, Z) \in \mathbb{Q}[X, Y, Z]$ *is homogeneous of degree* 2*, then there are either* 0 *or infinitely many rational solutions.*

Theorem 25 (Hasse-Minkowski)**.** *Let* $f(x, y) \in \mathbb{Q}[x, y]$ *be of degree* 2*. Then* $f(x, y) = 0$ *has a solution in* $\mathbb{Q}$ *if and only if it has a solution in* $\mathbb{R}$ *and* $\mathbb{Q}_p$ *for all* p*.*

3.3 Degree 3, Elliptic Curves

Example 26 (Selmer)**.** If $f(x,y) = 3x^3 + 4y^3 + 5$, then $f(x,y) = 0$ has no rational solutions.

In particular, the Hasse principle fails in this example since it does have solution at all places.

Example 27. If $f(x,y) = x^3 - y^2 - y$, then $f(x,y) = 0$ has exactly 2 rational solutions.

Example 28. Recall Diophantus' question in Example 13. Let

$$f(x,y) = x^3 - x - y(6-y).$$

It's clear that $(-1,0)$ is a rational solution. We can use the "chord-and-tangent" method to find other rational solutions.

For example, the tangent line at $(-1,0)$ intersect the curve at a third point, $(\frac{17}{9}, \frac{26}{27})$. Since the curve is symmetric with respect to $y = 3$, $(\frac{17}{9}, 6 - \frac{26}{27})$ is another rational point on the curve. The chord through $(-1,0)$ and $(\frac{17}{9}, 6 - \frac{26}{27})$ intersect the curve at a third point, $(\frac{-644}{169}, \frac{-11220}{2197})$.

With little work, one can show that $f(x,y) = 0$ has infinitely many solutions.

The curve in this example is in fact an elliptic curve. Before we formally define it, we need some more terminology.

Definition 29. A polynomial $f(x,y) \in \mathbb{Q}[x,y]$ defines a (affine) plane curve

$$C = f(x,y) = 0.$$

Definition 30. A curve is smooth if there are no (x_0, y_0) such that

$$0 = f(x_0,y_0) = \frac{\partial f}{\partial x}(x_0,y_0) = \frac{\partial f}{\partial y}(x_0,y_0).$$

Definition 31. We can homogenize a polynomial $f(x,y) \in \mathbb{Q}[x,y]$ and get a projective curve.

Example 32. Let $f(x,y) = x^2 + y^2 - 1$. It's homogenization $F(X,Y,Z) = X^2 + Y^2 - Z^2$ defines a projective curve in $\mathbb{P}^2$.

Definition 33. An elliptic curve E over $\mathbb{Q}$ is a smooth projective genus 1 algebraic curve with a specified $\mathbb{Q}$-point $\mathcal{O} \in E(\mathbb{Q})$.

Any elliptic curve over $\mathbb{Q}$ can be written in the Weierstraß form,

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Q},$$

and $\Delta(E) = -16(4A^3 - 27B^2) \neq 0$.

Example 34. Recall Diophantus' question in Example 13.

$$y(6-y) = x^3 - x \implies y(6-y) - 9 = x^3 - x - 9.$$

With the change of variable of

$$\begin{aligned} x &\mapsto -x \\ y &\mapsto y + 3, \end{aligned}$$

we get

$$y^2 = x^3 - x + 9.$$

In fact, the set of rational solution $E(\mathbb{Q})$ forms a (abelian) group under the group law.

Theorem 35 (Mordell). *$E(\mathbb{Q})$ is finitely generated. Thus*

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{r(E)},$$

with $r(E)$ called the rank of E.

Remark 36. Mazur showed that $E(\mathbb{Q})_{\text{tors}}$ must be isomorphic to one of 15 known abelian groups.

Theorem 37. *An integer n is congruent if and only if*

$$E_n : y^2 = x^3 - n^2 x$$

has $r(E_n) > 0$.

3.4 Reduction to Primes and BSD

For a generic elliptic curve E, we have

$$\#E(\mathbb{F}_p) \approx p$$

by the Quadratic reciprocity. On the other hand, the heuristic of "higher rank implies more solution" tends to be preserved by reduction.

Conjecture (Birch, Swinnerton-Dyer). *Let E be an elliptic curve, then*

$$\prod_{p \leq X} \frac{\#E(\mathbb{F}_p)}{p} \asymp \log(X)^{r(E)}.$$

Remark 38. This is the the original formulation of the conjecture. There are more modern formulations in terms of L-functions.

Definition 39. Let $p \nmid \Delta(E)$, we define

$$a_p = p + 1 - \#E(\mathbb{F}_p).$$

This is the trace of Frobenius.

Definition 40. Let E be an elliptic curve, the local L-function of E at place p is defined as follows. Let $s \in \mathbb{C}$,

$$L_p(E, s) = \begin{cases} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}, & \text{if } p \nmid 2\Delta(E) \\ \text{something else} & \text{otherwise.} \end{cases}$$

The (global) L-function is then defined as

$$L(E, s) = \prod_p L_p(E, s).$$

Theorem 41. *When $\text{Re}(s) > \frac{3}{2}$, $L(E, s)$ converges absolutely.*

Moreover, the Modularity Theorem implies

Theorem 42 (Wiles, Breuil-Conrad-Diamond-Taylor). *$L(E, s)$ has holomorphic continuation to all $\mathbb{C}$.*

Conjecture (BSD). *The Taylor expansion of $L(E, s)$ at $s = 1$ is*

$$L(E, s) = c(s - 1)^{r(E)} + \text{higher order terms},$$

where c is an explicit nonzero constant that's related to the Tate-Shafarevich group of E.

Definition 43. The analytic rank of E is defined as

$$r_{\text{an}}(E) = \text{ord}_{s=1} L(E, s).$$

Conjecture (BSD reformulated). *Let E be an elliptic curve, then*

$$r_{\text{an}}(E) = r(E).$$

4 Goldfeld's Conjecture, Selmer groups, and the Cassels–Tate Pairing, lecture 1. Speaker: Alexander Smith. Notes by Luke Wiljanen.

4.1 Quadratic Twists

Choose an elliptic curve

$$E : y^2 = x^3 + ax + b,$$

$a, b \in \mathbb{Q}$. Given $d \in \mathbb{Q}^\times$, let

$$E^d : dy^2 = x^3 + ax + b$$

be the twist. We have an isomorphism $\beta_d : E^d \xrightarrow{\sim} E$ given by $(x, y) \mapsto (x, \sqrt{d}y)$.

Given $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = G_\mathbb{Q}$. We have

$$\sigma(\beta_d(x, y)) = \sigma(x, \sqrt{d}y) = (\sigma x, \sigma(\sqrt{d})\sigma(y))$$

and

$$\beta_d(\sigma(x, y)) = (\sigma x, \sqrt{d}\sigma(y)).$$

So,

$$\sigma(\beta_d(x, y)) = \frac{\sigma(\sqrt{d})}{\sqrt{d}}\beta_d(\sigma(x, y)).$$

Let $\chi_d : G_\mathbb{Q} \to \{\pm 1\}$ be defined by $\chi_d(\sigma) = \frac{\sigma(\sqrt{d})}{\sqrt{d}}$. Then,

$$\sigma(\beta_d(z)) = \chi_d(\sigma)\beta_d(\sigma(z))$$

and

$$E^d[2] \cong E[2].$$

Conjecture ([Gol79]). *Given any E, the analytic rank in the twist family satisfies*

$$r_{\mathrm{an}}(E^d) = \begin{cases} 0 & \text{for } 50\% \text{ of } d \\ 1 & \text{for } 50\% \text{ of } d \\ \geq 2 & \text{for } 0\% \text{ of } d. \end{cases}$$

The above conjecture is sometimes known as the minimalist's conjecture because it is conjecturing that rank is as small as possible 100% of the time. This is qualified by a functional equation (maybe up to some fudge factor) $L(s, E^d) = \omega(E^d)L(2 - s, E^d)$ where $\omega(E^d) \in \{\pm 1\}$ is the global root number. When the global root number is +1, the order of vanishing is even, and when the global root number is -1, the order of vanishing is odd. Each of these cases happen 50% of the time. So, the conjecture is saying the rank is as small as possible given the global root number.

Theorem 44 ([Smi25]). *The BSD Conjecture implies Goldfeld's Conjecture.*

4.2 Selmer Groups

We have the exact sequence

$$0 \to E[n] \to E \xrightarrow{n} E \to 0$$

for $n \geq 2$. From this, we get the exact sequence on cohomology

$$H^0(G_\mathbb{Q}, E) \xrightarrow{n} H^0(G_\mathbb{Q}, E) \to H^1(G_\mathbb{Q}, E[n]) \to H^1(G_\mathbb{Q}, E[n]) \to H^1(G_\mathbb{Q}, E)$$

We also have the commutative diagrams coming from restriction

$$\begin{array}{ccccc} E(\mathbb{Q}) & \xrightarrow{n} & E(\mathbb{Q}) & \longrightarrow & H^1(G_{\mathbb{Q}}, E[n]) \\ \downarrow & & \downarrow & & \downarrow \\ E(\mathbb{Q}_v) & \xrightarrow{n} & E(\mathbb{Q}_v) & \longrightarrow & H^1(G_{\mathbb{Q}_v}, E[n]) \end{array}$$

Moreover, we have an injection

$$E(\mathbb{Q})/nE(\mathbb{Q}) \hookrightarrow \mathrm{Sel}^n(E) = \ker\left(H^1(G_{\mathbb{Q}}, E[n]) \to \prod_v \frac{H^1(G_{\mathbb{Q}_v}, E[n])}{\mathrm{Image}(E(\mathbb{Q}_v))}\right).$$

We define

$$r_n(E) = \max\{r \mid (\mathbb{Z}/n\mathbb{Z})^r \hookrightarrow \mathrm{Sel}^n(E)/\mathrm{Image}(E_{tors}(\mathbb{Q}))\}.$$

We have the following facts:

1. $r_n(E) \geq \mathrm{rank}(E)$
2. $r_2(E) \geq r_4(E) \geq r_8(E) \geq \cdots \geq r_{2^\infty}(E) \geq \mathrm{rank}(E)$
3. (Conjecture) $r_{2^\infty}(E) = \mathrm{rank}(E)$
4. $r_{an}(E) \equiv r_2(E) \equiv r_4(E) \equiv \cdots \pmod 2$.

Theorem 45 ([Smi25])**.** *We have*

$$r_{2^\infty}(E^d) = \begin{cases} 0 & \text{for } 50\% \text{ of } d \\ 1 & \text{for } 50\% \text{ of } d \\ \geq 2 & \text{for } 0\% \text{ of } d. \end{cases}$$

Corollary 46. *The BSD Conjecture implies Goldfeld's conjecture.*

Sketch. Suppose BSD holds. Then, $r_{an}(E^d) = \mathrm{rank}(E^d) \leq r_{2^\infty}(E^d)$ and $r_{an}(E^d) \equiv r_{2^\infty}(E^d) \pmod 2$. So, if $r_{2^\infty}(E^d) \leq 1$, we find $r_{2^\infty}(E^d) = r_{an}(E^d)$. □

The following remark was in response to a question of the audience.

Remark 47 (p-Converse Theorems). There are p-Converse Theorems of the following shape: Suppose we have an elliptic curve E and a prime p satisfying some condition and that $r_{p^\infty}(E) \leq 1$. Then, $\mathrm{rank}(E) = r_{p^\infty}(E) = r_{an}(E)$. One such result is due to Skinner-Urban [SU14]. See Remark 1.5 in Smith's paper [Smi25].

4.3 Cassels–Tate Pairing

Theorem 48 ([Cas62a])**.** *Given $n \geq 2$ and an elliptic curve E, there is a pairing*

$$\mathrm{Sel}^n(E)/\mathrm{Image}(E_{tors}) \times \mathrm{Sel}^n(E)/\mathrm{Image}(E_{tors}) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

that is alternating and whose kernel is $n\mathrm{Sel}^{n^2}(E)/\mathrm{Image}(E_{tors})$.

Corollary 49. *We have*

$$r_2(E) \equiv r_4(E) \equiv r_8(E) \equiv \cdots \pmod 2.$$

Definition 50. Given $k \geq 1$, define

$$\mathrm{CTP}_{k,E} : 2^{k-1}\mathrm{Sel}^{2^k}(E)/\mathrm{Image}(E_{tors}) \times 2^{k-1}\mathrm{Sel}^{2^k}(E)/\mathrm{Image}(E_{tors}) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$$

by $\mathrm{CTP}_{k,E}(2^{k-1}\phi, 2^{k-1}\psi) = \langle \phi, 2^{k-1}\psi\rangle = \langle 2^{k-1}\phi, \psi\rangle$.

The pairing $\mathrm{CTP}_{k,E}$ is an alternating pairing on $\mathbb{F}_2^{r_{2^k}}(E)$ with kernel

$$2^k\mathrm{Sel}^{2^{k+1}}(E)/\mathrm{Image}(E_{tors})$$

of dimension $r_{2^{k+1}}(E)$.

Expectation: As d varies, CTP_{k,E^d} behaves like a random alternating pairing on $\mathbb{F}_2^{r_{2^k}(E^d)}$.

Theorem 51 ([Smi22b])**.** *Let $P^{\mathrm{Alt}}(j \mid n)$ be the probability that a uniformly selected $n \times n$ alternating matrix over $\mathbb{F}_2$ has kernel of dimension j. Then, if $E(\mathbb{Q})[2] = 0$, we have*

$$\mathbb{P}(r_2(E^d) = r_2, r_4(E^d) = r_4, r_8(E^d) = r_8, \ldots) = \lim_{k\to\infty} \frac{1}{2} P^{\mathrm{Alt}}(r_2 \mid 2k) p^{\mathrm{Alt}}(r_4 \mid r_2) P^{Alt}(r_8 \mid r_4) \cdots$$

for $r_2 \geq r_4 \geq r_8 \geq \cdots$.

Remark 52. This theorem also holds if $E(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$ and E has no cyclic rational 4-isogeny. It holds in no other cases.

Remark 53. This is the distribution of 2^∞-Selmer groups constructed by BKLPR [BKL+15] and Delaunay [Del01].

4.4 Why 2?

Recall that the group cohomology group

$$\begin{aligned} H^1(G_{\mathbb{Q}}, E[n]) &= \frac{\text{1-cocycles in } E[n]}{\text{1-coboundaries in } E[n]} \\ &= \frac{\{\phi : G_{\mathbb{Q}} \to E[n] \text{ continuous } \mid \phi(\sigma\tau) = \sigma\phi(\tau) + \phi(\sigma) \text{ for all } \sigma, \tau \in G_{\mathbb{Q}}\}}{\{(\sigma \mapsto (\sigma - 1)x) \mid x \in E[n]\}}. \end{aligned}$$

Since

$$E^d[2] \cong E[2],$$

we have that $H^1(G_{\mathbb{Q}}, E[2]) \cong H^1(G_{\mathbb{Q}}, E^d[2])$. Hence, the Selmer group

$$\mathrm{Sel}^2(E^d) = \ker\left(H^1(G_{\mathbb{Q}}, E[2]) \to \prod_v \frac{H^1(G_v, E[2])}{\mathcal{L}_v(E^d[2])}\right)$$

only has dependence in d coming from the local conditions.

In the $n = 4$ case, we do not always have $E^d[4] \cong E[4]$. However, $E^{d_1 d_2}[4]$ is a subquotient of

$$E[4] \oplus E^{d_1}[4] \oplus E^{d_2}[4].$$

Example 54. Consider

$$E_d : y^2 = x^3 - d^2.$$

We have the twist by $\sqrt{-3}$, given by

$$E'_d : y^2 = x^3 + 27d^2.$$

Then, we have an isomorphism

$$E_d[\sqrt{-3}] \cong E[\sqrt{-3}],$$

but

$$E_d[3] \ncong E[3].$$

The $\sqrt{-3}$-Selmer group is an analogue of the 2-Selmer group in the quadratic twist family. The 3-Selmer group is an analogue of the 4-Selmer group in the quadratic twist family.

Theorem 55 ([KS24]). *We have*

$$r_{3^\infty}(E_d) = \begin{cases} 0 & \text{for } \geq 31\% \text{ of } d \\ 1 & \text{for } \geq 47\% \text{ of } d \\ \geq 2 & \text{for } \leq 22\% \text{ of } d. \end{cases}$$

5 Nilpotent groups and The Frattini subgroup. Speaker: Simo Liu. Notes by Santak Panda.

The goal of this pre-talk is to describe some characterizing properties of finite nilpotent groups; to do so we will use Frattini's argument, and then study the Frattini subgroup of a group.

5.1 Nilpotent groups

Definition 56. A group G is called nilpotent if it has a central series, that is, a normal[6] series $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ such that G_{i+1}/G_i is contained in the center of G/G_i for all i. The length of a shortest central series of G is the nilpotent class of G.

Theorem 57. *Let G be a finite group. The following statements are equivalent:*

1. *G is nilpotent.*
2. *for all proper $H < G$, $H \lneq N(H)$.*
3. *all non-trivial quotient groups have non-trivial center.*
4. *every subgroup has an ascending subnormal[7] series to G, that is, every subgroup is subnormal.*
5. *G is the direct product of its Sylow p-subgroups.*
6. *every maximal[8] subgroup of G is normal.*

Proof of (1) $\leftrightarrow$ (3), (1) $\rightarrow$ (2), (1) $\rightarrow$ (6): As G is finite, we see that repeated (but finitely many) applications of (3) starting with the quotient $G/\{1\}$ gives us a central series, thus (3) implies (1). Conversely if G is nilpotent then we have a central series $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$, multiplying this series with H for a proper normal subgroup H, we see with little work that (3) holds. Since this technique is quite useful we state it as a separate lemma.

Lemma 58. *Suppose G is nilpotent and $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ is a central series. Let H be any proper subgroup of G. Then we obtain a series*[9]

$$H = HG_1 \triangleleft HG_2 \triangleleft \cdots \triangleleft HG_n = G.$$

If i is the smallest such that $H \lneq HG_i$, then $H \triangleleft HG_i$, and in particular $H \lneq N_G(H)$. If H is furthermore normal then all HG_j are normal in G and $HG_{j+1}/HG_j \leq Z(G/HG_j)$ for all $j = 1, \cdots, n-1$. With i as before, we have that $H \triangleleft HG_i$, $HG_i/H \leq Z(G/H)$ and $Z(G/H)$ is non-trivial.

Thus (1) $\rightarrow$ (3). This lemma also shows that (1) $\rightarrow$ (2). We now show that (1) $\rightarrow$ (6). Let M be a maximal proper subgroup of G. Then let i be as in the lemma, we have that $H \lneq HG_i$ and $H \triangleleft HG_i$. Since M is maximal $HG_i = G$ and we win as $H \triangleleft HG_i = G$. □

Example 59. All abelian groups are nilpotent. From the class equation formula we know that any non-trivial p-group has non-trivial center. Thus any p-group satisfies (3) and is therefore nilpotent.

A full proof of the fact that $(1), (2), (4), (5), (6)$ are all equivalent can be found in §5.2 of [Rob96]. For our purposes, we are particularly interested in the equivalence of (1) and (5), so we prove this next. For our proof, the following argument is an important step.

[6] $G_0 \leq G_1 \leq \cdots \leq G_n \leq \cdots$ is called a normal series if each G_i is normal in G.
[7] we shall call $G_0 \leq G_1 \leq \cdots \leq G_n \leq \cdots$ a subnormal series if each G_i is normal in G_{i+1}.
[8] by this we mean a proper subgroup of G that is not strictly contained in any other proper subgroup of G.
[9] below the set products HG_i are literally the subgroup generated by H and G_i because $G_i \triangleleft G$.

Proposition 60 (Frattini's argument)**.** *Let G be a finite group and let $H \triangleleft G$. Let P be a Sylow p-subgroup in H, then*

$$N_G(P) \cdot H = G.$$

Proof. This is a straightforward application of Sylow's conjugate theorem. Let $g \in G$. Since H is normal $gPg^{-1} < H$, it is also a Sylow p-subgroup of H as P is. Thus there exists an $h \in H$ such that $gPg^{-1} = hPh^{-1}$, whence $gh^{-1} \in N_G(P)$ and we win. □

Corollary 61. *Let G be a finite group and P be a Sylow p-subgroup of G, then $N_G(N_G(P)) = N_G(P)$.*

Proof. Let $G' := N_G(N_G(P))$ and $H = N_G(P)$. Then $H \triangleleft G'$ and P is a Sylow p-subgroup in H. So using Frattini's argument we find that

$$N_{G'}(P) \cdot N_G(P) = N_G(N_G(P)).$$

It is easily checked that $N_{G'}(P) = N_G(P)$ as $G' = N_G(P)$. Thus we find that $N_G(P) \cdot N_G(P) = N_G(N_G(P))$ and our claim is proved. □

Proof of (1) $\leftrightarrow$ (5): First let's assume that G is a direct product of it's Sylow subgroups, we show that G is nilpotent. It's easily seen that if G_1, G_2 are nilpotent then so is $G_1 \times G_2$. Thus we may assume that G is a p-group. Then from our proof of (1) $\leftrightarrow$ (3) we find that G is nilpotent.

Now suppose that G is nilpotent. We shall write n_p for the number of Sylow p-subgroups of G for a prime $p \mid \#(G)$. The following lemma is standard and easy to prove.

Lemma 62. *A finite group G is a direct product of it's Sylow subgroups if and only if $n_p = 1$ for all primes $p \mid \#(G)$, that is, all Sylow subgroups are normal.*

Let P be a Sylow p-subgroup of G. We shall prove that P is normal in G. Suppose $P \not\lhd G$, then $N_G(P) \lneq G$. Recall that we have proven (1) $\rightarrow$ (2). Since we are assuming G is nilpotent, from (2) we see that $N_G(P) \lneq N_G(N_G(P))$, contradicting what we proved in the corollary above. Thus all Sylow subgroups of G are normal and G is a direct product of it's Sylow subgroups. □

5.2 The Frattini subgroup

Definition 63. The Frattini subgroup $\Phi(G)$ of a groups G is defined as $\Phi(G) := \bigcap_{\substack{M \text{ maximal} \\ \text{proper in } G}} M$.

If M is a maximal subgroup of G then so is gMg^{-1} for any $g \in G$. Thus we see that $g\Phi(G)g^{-1} = \Phi(G)$ for all $g \in G$ and so the Frattinin subgroup $\Phi(G) \triangleleft G$.

Proposition 64. *For any finite group G, the Frattini subgroup $\Phi(G)$ is nilpotent.*

Proof. We will show that $\Phi(G)$ is a direct product of it's Sylow subgroups and therefore nilpotent. Let $P \leq \Phi(G)$ be a Sylow p-subgroup. To prove our claim we need to show that $N_{\Phi(G)}(P) = \Phi(G)$. We'll prove something stronger, we will show that $N_G(P) = G$. Since $\Phi(G)$ is normal, by Frattini's argument we have

$$N_G(P) \cdot \Phi(G) = G.$$

If $N_G(P)$ were a proper subgroup, then $N_G(P) \leq M$ for some maximal subgroup M, but then since $\Phi(G) \leq M$, we would have that $N_G(P) \cdot \Phi(G) \leq M \lneq G$. Thus $N_G(P) = G$ and so $n_p = 1$ for all prime $p \mid \#(\Phi(G))$, proving that $\Phi(G)$ is nilpotent. □

Lemma 65. *If G is nilpotent and finite then $[G, G] \leq \Phi(G)$.*

Proof. Let M be a maximal subgroup of G, then from (1) $\rightarrow$ (6), we know that $M \triangleleft G$. From (1) $\rightarrow$ (3) we infer that G/M has non-trivial center. Since M is maximal, this means that $Z(G/M) = G/M$ and so G/M is abelian and therefore $[G, G] \subset M$. The claim follows because M was arbitrary. □

Now suppose G is a finite p-group. Let M be a maximal proper subgroup, then by Sylow's theorem, $G/M \cong C_p$[10]. So for all $g \in G$, $g^p \in M$. Let

$$G^p = \langle g^p : g \in G \rangle,$$

so we see that $G^p \leq M$. Since M was arbitrary, this shows that $G^p \leq \Phi(G)$. From the last lemma we also have $[G, G] \leq \Phi(G)$, hence $G^p[G, G] \leq \Phi(G)$. To prove the converse, we shall need the following simple but useful definition.

Definition 66. A abelian group G is said to be an elementary abelian p-group if every non-identity element of G has order p.

Remark 67. If G is a finite elementary abelian group, then from the structure theorem of finite abelian groups we see that $G = (C_p)^n$ for some n. In general, an elementary abelian group is a direct product of C_p (see problem 8 in exercises 1.4 of [Rob96]).

Proposition 68. *Suppose G is a finite p-group, then $G^p[G, G] = \Phi(G)$.*

Proof. To finish the proof, we have to show that $\Phi(G) \leq G^p[G, G]$. We note that $G^p[G, G] \triangleleft G$ and $G/G^p[G, G]$ is an elementary abelian p-group. Since $G^p[G, G] \leq \Phi(G)$, $G/\Phi(G)$ is also p-elementary abelian. We now need the following lemma.

Lemma 69. *If $H \triangleleft G$ such that G/H is a finite elementary abelian p-group then $\Phi(G) \leq H$.*

Proof. Following the last remark made above, we can write

$$G/H = \prod_{i=1}^{n} C_p = \prod_{i=1}^{n} \langle x_i \rangle,$$

for some $n \geq 1$ and generators x_i's of the n copies of C_p. We set

$$H_i := \langle H, x_j : x_j \neq x_i \rangle.$$

then each H_i is normal in G and is maximal proper (because $G/H_i \cong C_p$) in G. By construction $\bigcap_i H_i = H$. So by the definition of $\Phi(G)$, we find that $\Phi(G) \leq \bigcap_i H_i = H$. □

This lemma therefore shows that $\Phi(G) \leq G^p[G, G]$, and we win. □

5.3 Two useful results

We end with a Galois theoretic consequence of Sylow's theorem and re-state a particular result in theorem (57) about nilpotent groups.

Lemma 70. *If $G \hookrightarrow S_n$ is a p-group and E/F is a field extension with $\mathrm{Gal}(E/F) = G$, then we have a tower of extension*

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E$$
$$\mathrm{Gal}(F_i/F_{i-1}) = C_p$$

where $\#(G) = p^m$.

Proof. This follows from one of Sylow's theorem and Galois theory. We can find a sequence $\{1\} = H_0 \leq H_1 \leq \cdots \leq H_m = G$, such that $\#(H_i) = p^i$ for each $i = 0, 1, \cdots, m$. Consequently, $H_i \triangleleft H_{i+1}$ for each $i = 0, 1, \cdots, m-1$. Setting $F_i := E^{H_{m-i}}$, we see that $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E$, and from Galois theory we find that F_i is normal over F_{i-1} and $\mathrm{Gal}(F_i/F_{i-1}) = H_{m-i+1}/H_{m-i} = C_p$ for each $i = 1, \cdots, m$. □

Lemma 71. *If $G \hookrightarrow S_n$ is a nilpotent group, then G can be decomposed as $\prod_{p|\#(G)} \mathrm{Syl}_p(G)$ as a permutation group.*

[10] by this we mean the cyclic group of order p.

6 Genus theory and nilpotent extensions, lecture 2. Speaker: Jiuya Wang. Notes by Jake Huryn.

We continue with the notation of §2.

6.1 Malle's conjecture for nilpotent extensions

Here are two conjectures which give upper bounds for counting number fields.

Conjecture (Weak Malle's conjecture)**.** *For any finite permutation group G, we have $\#E(G,X) = O_\epsilon(X^{1/a+\epsilon})$ for all $\epsilon > 0$.*

Conjecture (Discriminant multiplicity conjecture)**.** *For any finite permutation group G, we have $a_D = O_\epsilon(D^\epsilon)$ for all $\epsilon > 0$.*

According to [KW22, Theorem 1.3], these two conjectures are equivalent.

Proposition 72. *The discriminant multiplicity conjecture holds for nilpotent extensions.*

Proof. We verify it for p-extensions and then defer to Lemma 71. Fix a p-group G, and let D be a positive integer. Let S be the set of primes dividing D, and let $G_S(p)$ be the maximal pro-p quotient of G_S.[11] Since $G_S(p)^{\mathrm{ab}} \cong \prod_{v\in S} \mathbb{Z}_v^\times(p)$, the group $G_S(p)^{\mathrm{ab}}$ has rank $\leq \#S$, so $G_S(p)$ has rank[12] $\leq \#S$ by the Frattini argument. So, the number of continuous homomorphisms $G_S(p) \to G$ is $\leq (\#G)^{\#S} = O_\epsilon(D^\epsilon)$ for any $\epsilon > 0$. Since each G-extension of $\mathbb{Q}$ with discriminant D is determined by a continuous surjection $G_S(p) \twoheadrightarrow G$, we are done. □

Now we discuss lower bounds. The approach is essentially the same as solving the inverse Galois problem for nilpotent groups: Given a p-group G, we pick a central series $1 = G_0 \subseteq \cdots \subseteq G_n = G$ and try to successively solve the central embedding problems

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}} & & \\ & & & & & \overset{\widetilde{\phi}}{\swarrow} & \downarrow{\scriptstyle \phi} & & \\ 1 & \longrightarrow & G_i/G_{i-1} & \longrightarrow & G/G_{i-1} & \longrightarrow & G/G_i & \longrightarrow & 1. \end{array}$$

As long as a solution $\widetilde{\phi}$ exists, we immediately get many solutions, namely

$$\widetilde{\phi} + H^1(G_{\mathbb{Q}}, G_i/G_{i-1}) = \widetilde{\phi} + \mathrm{Hom}(G_{\mathbb{Q}}, G_i/G_{i-1})$$

—twists of $\widetilde{\phi}$ by G_i/G_{i-1}-extensions over $\mathbb{Q}$, which are abelian. The twisting process can guarantee that we find solutions with small discriminant.

Here are some results on this problem.

Theorem 73. *Let G be a finite nilpotent permutation group.*

1. *Assume the chosen permutation representation of G is the regular representation (i.e. we are counting Galois G-extensions). Then we have*

$$X^{1/a}(\log X)^{b''-1} \ll \#E(G,X) \ll X^{1/a}(\log X)^{b'-1}$$

for some $b'' \leq b \leq b'$.

[11] Recall that G_S denotes the Galois group of maximal unramified-outside-S extension of $\mathbb{Q}$.
[12] By "rank", we mean the minimal number of generators in any presentation of $G_S(p)$.

2. *For an arbitrary permutation representation, we have*

$$X^{1/a'} \ll \#E(G,X) \ll X^{1/a}(\log X)^{b'-1}$$

for some $b' \geq b$ and $a' \geq a$.

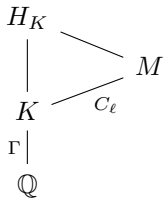
3. *Assume that the elements of G of minimal index generate a (nontrivial) abelian normal subgroup of G. Then Malle's conjecture holds for G.*

In summary, we have very good bounds for counting extensions of $\mathbb{Q}$ with nilpotent Galois group. This is to be contrasted with the case of more general groups, in which even the discriminant multiplicity conjecture is unknown in all cases. For example, with $G = S_3$, the best known bound is $a_D = O(D^{0.31\ldots})$.

6.2 Connection between Malle's conjecture and class group problems

Estimating the size of class groups is one of the motivations for counting number fields. First, we describe how to translate a problem about class groups into a problem about field extensions.

Fix a finite extension $K/\mathbb{Q}$. By class-field theory, the set $\mathrm{Cl}_K^\vee[\ell]$ is in bijection with the set of unramified C_ℓ-extensions M/K. Letting H_K be the Hilbert class field of K, we have the following picture:



(6.1)

Since $K \subseteq M$ and $\mathrm{Gal}(M/K) \cong C_\ell$, we get an embedding[13] $\epsilon\colon \mathrm{Gal}(M/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(M/K) \wr \Gamma$ corresponding to the injection

$$\{M \hookrightarrow \overline{\mathbb{Q}}\} \hookrightarrow \{\iota\colon M \hookrightarrow \overline{\mathbb{Q}} \mid \iota|_K = \iota_0\} \times \{K \hookrightarrow \overline{\mathbb{Q}}\}$$

where ι_0 is a fixed embedding $K \hookrightarrow \overline{\mathbb{Q}}$. It has the following properties:

1. $\mathrm{Gal}(M/\mathbb{Q})$ surjects onto Γ.
2. For any $a_1 \in \mathrm{Gal}(M/K)$, there exist $a_2, \ldots, a_n \in \mathrm{Gal}(M/K)$ such that $(a_1, \ldots, a_n) \rtimes e \in \epsilon(\mathrm{Gal}(M/\mathbb{Q}))$ (the notation coming from writing $\mathrm{Gal}(M/K) \wr \Gamma = \mathrm{Gal}(M/K)^{\#\Gamma} \rtimes \Gamma$).
3. Since M/K is unramified, we have $I_p(M/\mathbb{Q}) \cap \mathrm{Gal}(M/K) = \{e\}$ for any prime p, where I_p denotes the inertia group at p.

Example 74. Take $\Gamma = C_2$. Then $\mathrm{Gal}(M/\mathbb{Q})$ embeds into $C_\ell \wr C_2 = C_\ell^2 \rtimes C_2$. Suppose $(a,b) \rtimes \gamma \in I_p(M/\mathbb{Q})$. Then $((a,b) \rtimes \gamma)^2 \in C_\ell^2$, so by (3), $((a,b) \rtimes \gamma)^2 = (ab, ab) \rtimes e$ is trivial, i.e. $ab = e$ in C_ℓ. We deduce that $I_p(M/\mathbb{Q}) \subseteq C_\ell \rtimes C_2 = D_\ell$, where C_ℓ is embedded antidiagonally in C_ℓ^2. Since the groups $I_p(M/\mathbb{Q})$ as p vary generate all of $\mathrm{Gal}(M/\mathbb{Q})$, we deduce from (1) and (2) that $\mathrm{Gal}(M/\mathbb{Q}) = D_\ell$ (the dihedral group of size 2ℓ).

We call extensions satisfying (1)–(3) "admissible" and the possible Galois groups the "defining Galois groups" for this class-group problem. This transforms the class-group problem into a certain field-counting problem. Specifically, we have

$$\begin{aligned}\#\mathrm{Cl}_K[\ell] &\leq \#\{M/\mathbb{Q} \text{ only ramified at } \mathrm{Ram}(K/\mathbb{Q})\} \\ &\leq \sum_{G \text{ admissible}} \#\{M/\mathbb{Q} \text{ only ramified at } \mathrm{Ram}(K/\mathbb{Q}), \mathrm{Gal}(M/\mathbb{Q}) \cong G\};\end{aligned}$$

under the discriminant multiplicity conjecture, which we proved above for nilpotent groups, this quantity is $O_\epsilon(\mathrm{Disc}(K)^\epsilon)$ for any $\epsilon > 0$. This leads to:

[13] For abstract groups A and B, we write $A \wr B$ for the semidirect product $(\prod_{b \in B} A) \rtimes B$ in which B acts on $\prod_{b \in B} A$ by permuting the indices via left-multiplication, i.e. $b_0 \cdot (a_b)_{b \in B} \coloneqq (a_{b_0 b})_{b \in B}$.

Conjecture (ℓ-torsion conjecture)**.** *We have* $\#\mathrm{Cl}_K[\ell] = O_\epsilon(\mathrm{Disc}(K)^\epsilon)$ *for any* $\epsilon > 0$.

6.3 Better bounds

We continue in the setting of (6.1), but specialize to the case $\Gamma = C_2$.

Example 75. Take $\ell = 2$. The admissible Galois group is C_2^2, which is abelian. Thus we have essentially complete control via class-field theory, as follows. For simplicity,[14] assume 2 is not ramified in K. Since $M/\mathbb{Q}$ must be unramified away from $\mathrm{Ram}(K/\mathbb{Q})$, our embedding problem looks like

$$\begin{array}{ccccccccc} & & & & & & \prod_{p\in\mathrm{Ram}(K/\mathbb{Q})}\mathbb{Z}_p^\times & & \\ & & & & & \overset{\phi_1}{\swarrow} & \downarrow{\scriptstyle \phi_0} & & \\ 1 & \longrightarrow & C_2 & \longrightarrow & C_2^2 & \longrightarrow & C_2 & \longrightarrow & 1. \end{array}$$

Since there are two possible lifts of $\mathbb{Z}_p^\times \to C_2$ to a map $\mathbb{Z}_p^\times \to C_2^2$, we get that there are $2^{\#\mathrm{Ram}(K/\mathbb{Q})}$ lifts ϕ_1 of ϕ_0. Dividing by $2 = \#\mathrm{Aut}(C_2^2)$, we get that $\#\mathrm{Cl}_K^+[2] = 2^{\#\mathrm{Ram}(K/\mathbb{Q})-1}$. This is Gauß's "genus theory". Informally, $\mathrm{Cl}_K^+[2]^\vee$ (along with $\mathrm{Cl}_K[2]^\vee$—see (1) of the remark below) is "deterministic".

Remark 76.

1. To study $\mathrm{Cl}_K[2]$ instead of $\mathrm{Cl}_K^+[2]$ (which could differ only for real quadratic K), use class-field theory to keep track of where complex conjugation goes (i.e. ramification at infinity).
2. For $K/\mathbb{Q}$ quadratic or more generally abelian, one often defines its "genus field" to be the maximal unramified K^{g}/K such that $K^{\mathrm{g}}/\mathbb{Q}$ remains abelian. According to Fröhlich, we should extend this definition to $K/\mathbb{Q}$ not necessarily abelian by defining K^{g}/K to be the maximal unramified extension which is the composite of K with abelian extensions of $\mathbb{Q}$. In these settings, we are able to study pieces of the class group via class-field theory as in Example 75.

Example 77. Take $\ell = 4$. The admissible Galois group is D_4, and the embedding problem is

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}} & & \\ & & & & & \overset{\phi_2}{\swarrow} & \downarrow{\scriptstyle \phi_1} & & \\ 1 & \longrightarrow & C_2 & \longrightarrow & D_4 & \longrightarrow & C_2^2 & \longrightarrow & 1. \end{array}$$

The bottom row defines a class $\epsilon \in H^2(C_2^2, C_2) = H^2(\mathrm{Gal}(M/\mathbb{Q}), C_2)$ by the correspondence between group extensions and H^2. There is an exact sequence

$$H^1(G_M, C_2) \to H^2(\mathrm{Gal}(M/\mathbb{Q}), C_2) \xrightarrow{\inf} H^2(G_{\mathbb{Q}}, C_2),$$

(a piece of the five-term inflation–restriction sequence), and the embedding problem is solvable if and only if $\inf(\epsilon) = 0$. Since $Ш^2(G_{\mathbb{Q}}, C_2) = 0$, if suffices to determine when $\inf(\epsilon) = 0$ locally.

Now M lives inside $\mathbb{Q}(\sqrt{p_1^*}, \dots, \sqrt{p_n^*})$, where $p_1, \dots, p_n$ are the primes that ramify in $K/\mathbb{Q}$, and $p_i^* \in \{p_i, -p_i\}$. So the number of ϕ_1 which admit a lift ϕ_2 is controlled by the matrix of Legendre symbols

$$\left(\frac{p_i}{p_j}\right).$$

Studying the distribution of these matrices allows one to get the correct estimates for $\#\mathrm{Cl}_K[4]$. Informally, $\mathrm{Cl}_K[4]$ behaves with "bounded randomness".

Example 78. Take $\ell = 3$. Then the admissible Galois group is S_3, and we want to count S_3-extensions with $I_p \cap A_3 = \{e\}$. As we saw above, we do not have good estimates for counting S_3-extensions (see e.g. work of Davenport–Heilbronn for what little we do know). Informally, $\mathrm{Cl}_K[3]$ behaves with "unbounded randomness".

[14] because $\mathbb{Z}_p^\times$ is procyclic if p is odd, but $\mathbb{Z}_2^\times$ is not (but is nonetheless simple to describe)

7 Local Poitou–Tate Duality. Speaker: Niven Achenjang. Notes by Santak Panda.

The goal of this pre-talk is to describe the local duality map and the global Poitou-Tate duality map. First we recall a few things. Suppose $F = \mathbb{F}_q$ (is the finite field with q elements) and E/F is a finite extension of degree n in $\overline{\mathbb{F}_q}$. Then E is the splitting field of $X^{q^n} - X = 0$ inside $\overline{\mathbb{F}_q}$ and $\mathrm{Gal}(E/F) \cong \mathbb{Z}/n\mathbb{Z}$. Thus we see that $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$.

Now let K be a finite extension of $\mathbb{Q}_p$, and let $F = \mathbb{F}_q$ be its residue field, K^{un} be the maximal[15] unramified extension of K in a fixed algebraic closure $\overline{K}$. We recall that there is a correspondence between the subfields of K^{un} containing K and subfields of $\overline{\mathbb{F}_q}$ containing $\mathbb{F}_q$.

Theorem 79 (Proposition 7.50 in [Mil20a])**.** *Let L be an algebraic extension of K, and let l be the residue field[16] of L. The map $K' \mapsto k'$ sending an unramified extension K' of K contained in L to its residue field k' is a one-to-one correspondence between the sets*

$$\{K' \subset L,\ \textit{finite and unramified over } K\} \leftrightarrow \{k' \subset l,\ \textit{finite over } k\}.$$

Moreover there is a natural Galois theoretic correspondence between these. Consequently, if K_L^{un} is the maximal unramified extension of K contained in L, then $\mathrm{Gal}(K_L^{\mathrm{un}}/K) \cong \mathrm{Gal}(l/k)$.

It is easily proved that the residue field of $\overline{K}$ is $\overline{\mathbb{F}_q}$. So as a consequence of theorem (79), the Galois group $\mathrm{Gal}(K^{\mathrm{un}}/K)$ is seen to be isomorphic to $\widehat{\mathbb{Z}} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. In our setting we further infer that for each $m \geq 1$, there exists a unique unramified field extension K_m of K of degree m, and $\mathrm{Gal}(K_m/K) \cong \mathbb{Z}/m\mathbb{Z}$.

Below we shall be working with $\mathrm{Gal}(\overline{K}/K) =: G_K$-modules M, we can get (as we shall see below) from M a $\mathrm{Gal}(K^{\mathrm{un}}/K) = \mathrm{Gal}(\overline{F}/F) =: G_F$-module by considering the submodule of M fixed by the inertia group. Thus we often come across $\widehat{\mathbb{Z}}$-modules, now we do some cohomology computations.

7.1 Duality in the finite field setting

Proposition 80. *Let M be a discrete torsion[17] G_F-module. Then $H^1(G_F, M) \cong M/(\mathrm{Frob}-1)M =: M_{\mathrm{Frob}}$. The module M_{Frob} is called the Frobenius coinvariants of M.*

Proof. Let $Z^1(G_F, M)$ be the group of 1-cocyles. A 1-cocycle is a map $\varphi : G_F \to M$ satisfying the crossed homomorphism condition: $\varphi(gh) = \varphi(g) + g\varphi(h)$, for all $g, h \in G$. The main claim is that the natural map,

$$\Theta : Z^1(G_F, M) \to M,\ \varphi \mapsto \varphi(\mathrm{Frob})$$

is an isomorphism. Since Frob is a topological generator of $\widehat{\mathbb{Z}}$, any continuous map $\varphi : G_F \to M$ is determined by $\varphi(\mathrm{Frob})$, so the map described above is injective. Proving that this map is surjective utilizes the assumption that M is torsion. Let $m \in M$, then there exists $n \neq 0$ such that $n \cdot m = 0$. The group G_F acts continuously on the discrete abelian group M, in particular, the following map is continuous:

$$\Phi_m : G_F \to M,\ g \mapsto g \cdot m.$$

As M is discrete the subgroup $H := \{g \in G : g \cdot m = m\}$ stabilizing m is an open subgroup of G_F. Since $G_F = \widehat{\mathbb{Z}}$ is profinite (and thus in particular compact), we see that $\ell := [G_F : H]$ is finite. In what follows we shall use $\mathrm{Frob} \in G_F$ interchangeably with the element

$$(1 + i\mathbb{Z})_{i \in \mathbb{N}} \in \widehat{\mathbb{Z}}.$$

[15] This makes sense because a compositum of two unramified extensions over K is unramified over K. To see this we note that a compositum of two unramified finite extensions over K is unramified over K and that an extension L is unramified over K if and only if all its finite sub-extensions F are unramified over K; this last statement is easy to prove as all $\mathcal{O}_F$ are discrete valuation rings and so we can show that if the maximal ideal $\mathfrak{p}$ of K ramifies in L then it also ramifies in some finite sub-extension F.

[16] For an algebraic extension L of a local field K there exists a unique absolute value on L extending that on K. We use this absolute value to define the ring of integers in L and its residue field.

[17] By this we mean a torsion abelian group.

Let $m_0 := 0, m_1 := m$ and $m_{-1} := -\mathrm{Frob}^{-1}(m)$ and define for $i > 0$

$$m_i := m_1 + \mathrm{Frob}(m_1) + \cdots + \mathrm{Frob}^{i-1}(m_1),$$
$$m_{-i} := m_{-1} + \mathrm{Frob}^{-1}(m_{-1}) + \cdots + \mathrm{Frob}^{-i+1}(m_{-1}).$$

It is easily verified from these definitions that the following crossed homomorphism condition holds:

$$m_{i+j} = m_i + \mathrm{Frob}^i(m_j) \qquad \text{for all } i, j \in \mathbb{Z}.$$

We also have that $n \cdot m = 0$ and $\mathrm{Frob}^\ell(m) = m$, from these it is easily checked that $m_{\ell n} = 0$ and then from the crossed homomorphisms above we infer that

$$m_i = m_j \qquad \text{whenever } i \equiv j \pmod{\ell n}.$$

Let $\psi : \mathbb{Z}/\ell n\mathbb{Z} \to M$ be the map taking $i \mapsto m_i$, then ψ is continuous when $\mathbb{Z}/\ell n\mathbb{Z}$ is given discrete topology. Let $U = \left(\prod_{j\in\mathbb{N}} V_j\right) \cap \widehat{\mathbb{Z}}$, where $V_j = \mathbb{Z}/j\mathbb{Z}$ if $j \neq \ell n$ and $V_{\ell n} = (0) \subset \mathbb{Z}/\ell n\mathbb{Z}$. Then $\widehat{\mathbb{Z}}/U \cong \mathbb{Z}/\ell n\mathbb{Z}$ as topological abelian groups (beacuse the quotient topology on $\widehat{\mathbb{Z}}/U$ is discrete). The projection map $\pi : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}/U$ is continuous. Thus the composition $\varphi : \widehat{\mathbb{Z}} \to M$ of π and ψ

$$\widehat{\mathbb{Z}} \xrightarrow{\pi} \widehat{\mathbb{Z}}/U \xrightarrow{\psi} M, \qquad \widehat{\mathbb{Z}} \xrightarrow{\varphi} M$$

is continuous. By construction $\varphi(\mathrm{Frob}^i) = m_i$ for all $i \in \mathbb{Z}$ and in particular $\varphi(\mathrm{Frob}) = m$. Also from construction $\varphi(gh) = \varphi(g) + g \cdot \varphi(h)$ for all $g, h \in \langle \mathrm{Frob} \rangle \subset \widehat{\mathbb{Z}}$. Since $\overline{\langle \mathrm{Frob} \rangle} = \widehat{\mathbb{Z}}$ and φ is continuous, it follows that φ is a crossed homomorphism. This proves that Θ is an isomorphism. As Θ takes the co-boundaries $\subset$ co-cycles to $(\mathrm{Frob} - 1)M$,

$$H^1(G_F, M) \overset{\text{def}}{=} \frac{Z^1(G_F)}{\text{co-boundaries}} \overset{\Theta}{\cong} \frac{M}{(\mathrm{Frob} - 1)M},$$

and we win! □

Proposition 81. *Let M be as above, then $H^n(G_F, M) = 0$ for all $n \geq 2$. Consequently, together with the result above, we get an exact sequence*

$$0 \to H^0(G_F, M) \to M \xrightarrow{\mathrm{Frob}-1} M \to H^1(G_F, M) \to 0.$$

Proof. To prove this we will use a dimension shifting argument. Consider $\mathrm{Ind}_1^{G_F}(M) = \mathrm{Map}_{\mathrm{cts}}(G, M)$. By Shapiro's lemma (cf. proposition II.1.11 in [Mil20b]) one knows that $\mathrm{Ind}_1^G(M)$ is an acyclic G_F-module, that is,

$$H^n(G_F, \mathrm{Ind}_1^{G_F}(M)) = 0 \quad \text{for all } n \geq 1.$$

From the construction of $\mathrm{Ind}_1^{G_F}$, one get an isomorphism

$$\mathrm{Hom}_{G_F}(M, \mathrm{Ind}_1^{G_F}(M)) \cong \mathrm{Hom}_{\mathrm{cts}}(M, M),$$

the G_F-module homomorphism $M \to \mathrm{Ind}_1^{G_F}(M)$ corresponding to the identity map is the map $\varphi : M \to \mathrm{Ind}_1^{G_F}(M)$ sending $m \mapsto (g \mapsto g \cdot m)$. As $\varphi(m)(e) = m$, φ is an injection. We define M' to be the G_F-module that makes the following sequence exact:

$$0 \to M \xrightarrow{\varphi} \mathrm{Ind}_1^{G_F}(M) \to M' \to 0.$$

From the resulting long exact sequence of cohomology and that $\mathrm{Ind}_1^{G_F}(M)$ is acyclic, we find that

$$H^n(G_F, M') \cong H^{n+1}(G_F, M) \quad \text{for all } n \geq 1. \tag{7.1}$$

In particular $H^2(G_F, M) \cong H^1(G_F, M')$. It is easily checked that $\mathrm{Ind}_1^{G_F}(M)$ is a torsion abelian group as M is torsion and G_F is profinite (so that any continuous map G_F to a discrete set has finite image), and so M' is also a torsion G_F-module. So from our calculations above, $H^1(G_F, M') = M'/(\mathrm{Frob} - 1)M'$. Since $M' = \mathrm{Ind}_1^{G_F}(M)/M$, we have a surjection

$$H^1(G_F, \mathrm{Ind}_1^{G_F}(M)) = \mathrm{Ind}_1^{G_F}(M)/(\mathrm{Frob} - 1)\mathrm{Ind}_1^{G_F}(M) \twoheadrightarrow M'/(\mathrm{Frob} - 1)M' = H^1(G_F, M')$$

where we used the proposition above again for writing the first equality. From the acyclicity of $\mathrm{Ind}_1^{G_F}(M)$, we deduce that $H^1(G_F, M') = 0$. Thus $H^2(G_F, M) = 0$. Since M was an arbitrary torsion G_F-module, we find that (on replacing M by M') $H^2(G_F, M') = 0$ and then (7.1) implies that $H^3(G_F, M) = 0$. Repeating this argument we see that $H^n(G_F, M) = 0$ for all $n \geq 2$. □

Theorem 82. *Let M be as above, and define $M^\vee := \mathrm{Hom}_{\mathbf{Ab}}(M, \mathbb{Q}/\mathbb{Z})$[18]. Then for all n, we have a perfect pairing,*

$$H^n(G_F, M) \times H^{1-n}(G_F, M^\vee) \to H^1(G_F, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}.$$

Proof. The natural map $M \otimes_{\mathbb{Z}} M^\vee \to \mathbb{Q}/\mathbb{Z}$ defined by sending $m \otimes f \mapsto f(m)$ is a morphism of G_F-modules (where $\mathbb{Q}/\mathbb{Z}$ is viewed as a trivial G_F-module). So via cup product, we get a map $H^n(G_F, M) \times H^{1-n}(G_F, M^\vee) \xrightarrow{\cup} H^1(G_F, M \otimes_{\mathbb{Z}} M^\vee) \to H^1(G_F, \mathbb{Q}/\mathbb{Z})$, where the last map arises from the natural map above and the fact that $H^1(G_F, -)$ is a covariant functor. Now as $\mathbb{Q}/\mathbb{Z}$ is a trivial G_F-module, $H^1(G_F, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}_{\mathrm{cts}}(G_F, \mathbb{Q}/\mathbb{Z})$. Since $G_F = \widehat{\mathbb{Z}}$ is topologically generated by a single element (for example the Frobenius), we see that $\mathrm{Hom}_{\mathrm{cts}}(G_F, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$. Note that it is easier to prove $H^1(G_F, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$ using proposition (80).

We have explicit descriptions for the groups $H^n(G_F, M)$ and $H^{1-n}(G, M^\vee)$ for all n from propositions (80) and (81), and also an explicit description for the cup product (see remark after theorem (87) below), so the claim of the theorem may be checked by a brute-force calculation. □

Recall that for a G_F-module M, we have defined $M_{\mathrm{Frob}} := M/(\mathrm{Frob} - 1)M$. The last theorem says that $(M^{\mathrm{Frob}})^\vee = (M^\vee)_{\mathrm{Frob}}$ and $(M_{\mathrm{Frob}})^\vee = (M^\vee)^{\mathrm{Frob}}$.

7.2 Duality in the local setting

Now fix a prime p, and let $K/\mathbb{Q}_p$ be a finite extension. The inertia group $I_{\overline{K}/K}$ is the closed subgroup of G_K such that $K^{\mathrm{un}} = (\overline{K})^{I_{\overline{K}/K}}$, we have an exact sequence

$$1 \to I_{\overline{K}/K} \to \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(K^{\mathrm{un}}/K) \to 1.$$

We have an analogous exact sequence with $\overline{K}$ replaced by K^{ab}, in that case we further know that $I_{K^{\mathrm{ab}}/K}$ is equal to the image of the units $U_K \subset \mathcal{O}_K$ under the reciprocity map of local class field theory. In what follows we shall write I_K to denote the inertia group $I_{\overline{K}/K}$. Note that I_K is a subgroup of G_K, so that any G_K-module M is also an I_K-module.

Definition 83 (Unramified cohomology)**.** For a G_K-module M, we define the n^{th} unramified cohomology $H^n_{\mathrm{un}}(G_K, M)$ to be the submodule of $H^n(G_K, M)$ such that the sequence

$$0 \to H^n_{\mathrm{un}}(G_K, M) \to H^n(G_K, M) \xrightarrow{\mathrm{res}} H^n(I_K, M)$$

is exact, where res is the restriction map.

Remark 84. One can identify $H^1_{\mathrm{un}}(K, M)$ with $H^1(G_K/I_K, M^{I_K}) = H^1(G_F, M^{I_K})$ (cf. proposition II.1.34 on the inflation-restriction exact sequence in [Mil20b]). If M is torsion free, then from our work above we find that

$$H^1_{\mathrm{un}}(G_K, M) = H^1(G_F, M^{I_K}) = (M^{I_K})_{\mathrm{Frob}}.$$

[18] we view $M^\vee$ as a G_F-module as follows: for $g \in G_F$ and $f \in M^\vee$, we define $(g \cdot f)(m) := f(g^{-1} \cdot m)$ for all $m \in M$, that is, we view $\mathbb{Q}/\mathbb{Z}$ as a trivial G_F-module and use the usual G-module structure one puts on $\mathrm{Hom}_{\mathbf{Ab}}(M, N)$ for G-modules M, N.

Definition 85. A G_K-module M is *unramified* if $M = M^{I_K}$. We then have from the note above that

$$H^1_{\text{un}}(G_K, M) \cong H^1(G_F, M).$$

If M is furthermore a torsion module, then by Proposition 80 we have that $H^1_{\text{un}}(G_K, M) \cong M_{\text{Frob}}$.

Example 86. Let E/K be an elliptic curve with good reduction and fix a prime $\ell \neq p$. Then $E[\ell]$ is an unramified,[19] torsion[20] G_K-module and so $H^1_{\text{un}}(G_K, E[\ell]) = E[\ell]_{\text{Frob}}$.

From local class field theory we have a canonical (once we choose arithmetic or geometric Frobenius) isomorphism between the Brauer group $\text{Br}(K) := H^2(G_K, \overline{K}^\times)$ and $\mathbb{Q}/\mathbb{Z}$, we shall denote this map by inv_K and call it the *invariant* map. The isomorphism

$$\text{inv}_K \colon \text{Br}(K) \to \mathbb{Q}/\mathbb{Z}$$

furthermore satisfies some nice compatibility properties as we change the base field K.

Theorem 87 (Tate Duality)**.** *Let M be a finite G_K-module and let $M^\vee := \text{Hom}_{\mathbf{Ab}}(M, \mu_\infty)$ (this is a G_K-module with the action being $(g\cdot\varphi)(m) = g\varphi(g^{-1}m)$). The natural evaluation map $M \times M^\vee$ is G_K-equivariant and so cup product induces the duality map*

$$\langle \cdot, \cdot \rangle_K : H^n(G_K, M) \times H^{2-n}(G_K, M^\vee) \xrightarrow{\cup} H^2(G_K, M \otimes M^\vee) \to H^2(G_K, \mu_\infty) \to H^2(G_K, \overline{K}^\times) \cong \mathbb{Q}/\mathbb{Z}.$$

This pairing is furthermore perfect.

Implicit in the statement above is that $H^n(G_K, M)$ and $H^n(G_K, M^\vee)$ both vanish when $k \geq 3$.

Remark 88. We can make the duality map above more explicit when $n = 1$, as in that case we have a simple description for the cup product. Let M, N be G-modules (for any group G) and let $\varphi : G \to M$, $\psi : G \to N$ be two elements of $H^1(G, M)$ and $H^1(G, N)$ respectively. Then under the cup product

$$\cup : H^1(G, M) \times H^1(G, N) \to H^2(G, M \otimes_{\mathbb{Z}} N),$$

(φ, ψ) is mapped to the 2-cocycle[21] $\varphi \cup \psi$ that sends $(g, h) \mapsto \varphi(g) \otimes g \cdot \psi(h) \in M \otimes N$, for all $g, h \in G$.

Remark 89. Suppose M is a finite, unramified G_K-module and $p \nmid \#M$. Then $M^\vee$ is also unramified and we have the following commutative diagram:

$$\begin{array}{ccc} H^1(G_F, M) \times H^1(G_F, M^\vee) & \longrightarrow & H^2(G_F, M \otimes_{\mathbb{Z}} M^\vee) = 0 \\ \downarrow \cong & & \downarrow \\ H^1_{\text{un}}(G_K, M) \times H^1_{\text{un}}(G_K, M^\vee) & \xrightarrow{\langle \cdot, \cdot \rangle_K} & H^2(G_K, \overline{K}^\times). \end{array}$$

That $H^2(G_F, M \otimes_{\mathbb{Z}} M^\vee) = 0$ follows from Proposition 81. Thus the two unramified cohomologies are orthogonal to each other. In fact these are orthogonal complements in $H^1(G_K, M)$.

Example 90. We continue the earlier elliptic curve example. Recall that there is the Weil pairing

$$E[\ell] \times E[\ell] \to \overline{K}^\times.$$

As this pairing is perfect, we get an isomorphism $E[\ell]^\vee \cong E[\ell]$. Thus $H^1_{\text{un}}(G_K, E[\ell])$ is a maximal isotropic subspace of $H^1(G_K, E[\ell])$. As a consequence of this maximal isotropicity, we find from linear algebra that

$$\dim(H^1(G_K, E[\ell])) = 2\dim(H^1_{\text{un}}(G_K, E[\ell])) = 2\dim E[\ell]_{\text{Frob}} = 2\dim E[\ell]^{\text{Frob}} = 2\dim E[\ell](K).$$

[19] that is I_K fixes $E[\ell]$ and so if $P \in E[\ell]$, then $P \in E[\ell](L)$ for some finite unramified extension L of K.
[20] as everything is killed by definition by ℓ.
[21] an inhomogeneous 2-cocyle is a function $x : G \times G \to M$ such that $x(\sigma\tau, \rho) + x(\sigma, \tau) = x(\sigma, \tau\rho) + \sigma x(\tau, \rho)$.

7.3 Duality in the global setting

From global class field theory, we have for every number field K the following exact sequence:

$$0 \to \mathrm{Br}(K) \to \oplus_v \mathrm{Br}(K_v) \xrightarrow{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0.$$

Let M be a finite G_K-module, $M^\vee := \mathrm{Hom}_{\mathbf{Ab}}(M, \overline{K}^\times)$. For every place v, local duality gives $H^n(G_{K_v}, M) \cong H^{2-n}(G_{K_v}, M^\vee)^*$, where $^* := \mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$. There is an analogous global duality statement (cf. theorem (8.4.4) in [NSW08]). We define the following groups (roughly, these are products of the local cohomology groups):

$$\begin{aligned} P^0(K, M) &= \prod_{v<\infty} H^0(K_v, M) \times \prod_{v|\infty} \hat{H}^0(K_v, M), \\ P^1(K, M) &= \prod_v H^1(K_v, M), \\ P^2(K, M) &= \bigoplus_v H^2(K_v, M) \end{aligned}$$

(here v runs through all places of K, $\prod$ denotes the restricted product with respect to the unramified cohomology subgroups, and $\hat{H}^0(K_v, M)$ is the modified cohomology group; we refer to pages 22, 473 and 474 of [NSW08] for the details). Combining the local and global duality statements leads to the main result of arithmetic Galois cohomology:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0(K,M) & \longrightarrow & P^0(K,M) & \longrightarrow & H^2(K,M^\vee)^* \\ & \dashrightarrow & H^1(K,M) & \longrightarrow & P^1(K,M) & \longrightarrow & H^1(K,M^\vee)^* \\ & \dashrightarrow & H^2(K,M) & \longrightarrow & P^2(K,M) & \longrightarrow & H^0(K,M^\vee)^* \longrightarrow 0, \end{array}$$

a 9-term exact sequence connecting the local and global cohomology groups (cf. theorem (8.6.10) in [NSW08][22]). This may be viewed as a refinement of the (Brauer) exact sequence above.

[22] note that [NSW08] use $\prime$ for what we denote by $\vee$, and $\vee$ for what we denote by $*$.

8 Tamagawa ratios and the distribution of isogeny Selmer groups, lecture 2. Speaker: Alexander Smith. Notes by William C. Newman.

8.1 Greenberg–Wiles Formula

Definition 91. Let F be a global field. A module with local conditions, $(M, (\mathcal{L}_\nu)_\nu)$, is a finite G_F-module, M, with $\operatorname{char} F \nmid \#M$, and a subgroup $\mathcal{L}_\nu \subset H^1(G_\nu, M)$ for each place ν of F, with $\mathcal{L}_\nu = H^1_{\mathrm{ur}}(G_\nu, M)$ for all but finitely many ν.

The Selmer group of a module with local conditions $(M, (\mathcal{L}_\nu)_\nu)$ is

$$\mathrm{Sel}(M, (\mathcal{L}_\nu)_\nu) \coloneqq \ker\left(H^1(G_F, M) \to \prod_\nu \frac{H^1(G_\nu, M)}{\mathcal{L}_v}\right).$$

Because all but finitely many local conditions are equal to $H^1_{ur}(G_\nu, M)$, Selmer groups are finite.

We can define the dual of a module with local conditions, $(M, (\mathcal{L}_\nu)_\nu)$ to be

$$(M^\vee, \mathcal{L}_\nu^\perp)$$

where

$$M^\vee \coloneqq \mathrm{Hom}(M, (F^{sep})^\times),$$

(which is the Tate twist of the Pontryagin dual) and $\mathcal{L}_\nu^\perp$ is the orthogonal complement with respect to the Tate duality map

$$H^1(G_\nu, M) \times H^1(G_\nu, M) \to \mathrm{Br}(F_\nu).$$

As noted in the last talk, $H^1_{\mathrm{ur}}(G_\nu, M)^\perp = H^1_{\mathrm{ur}}(G_\nu, M^\vee)$, so the dual does indeed satisfy all but finitely many local conditions are equal to the unramified cohomology. The Tamagawa ratio is defined to be

$$\mathcal{T}(M) \coloneqq \frac{\#\mathrm{Sel}(M, (\mathcal{L}_\nu)_\nu)}{\#\mathrm{Sel}(M^\vee, (\mathcal{L}_\nu^\perp)_\nu)}.$$

The Greenberg–Wiles formula gives a way to compute the Tamagawa ratio.

Theorem 92 (Greenberg–Wiles Formula)**.**

$$\mathcal{T}(M) = \frac{\#H^0(G_F, M)}{\#H^0(G_F, M^\vee)} \cdot \prod_\nu \left(\frac{\#\mathcal{L}_\nu}{\#\mathcal{L}_\nu^\perp}\right)^{1/2}.$$

8.2 2-Isogeny Selmer group's average size

We think about the following example for the rest of the talk. Let $E/\mathbb{Q}$ be an elliptic curve and $\varphi : E \to E_0$ a degree 2 isogeny. We can decorate the $G_\mathbb{Q}$-module $E[\varphi] := \ker(\varphi)$ with the local conditions

$$\mathcal{L}_\nu(E[\varphi]) = \ker(H^1(G_\nu, E[\varphi]) \to H^1(G_\nu, E)),$$

and then we recover $\mathrm{Sel}^\varphi E = \mathrm{Sel} E[\varphi]$. Let $\varphi_0 : E_0 \to E$ be the dual isogeny. One can see that

$$E[\varphi]^\vee = (E_0[\varphi_0], (\mathcal{L}_\nu(E_0[\varphi_0]))_\nu) = E_0[\varphi_0^\vee].$$

The Greenberg–Wiles formula gives that

$$\frac{\#\mathrm{Sel}^\varphi E}{\#\mathrm{Sel}^{\varphi_0} E} = \prod_\nu \left(\frac{\#\mathrm{coker}(E(\mathbb{Q}_\nu) \to E_0(\mathbb{Q}_\nu))}{\#\mathrm{coker}(E_0(\mathbb{Q}_\nu) \to E(\mathbb{Q}_\nu))}\right)^{1/2}.$$

It is important that the right hand side of this can (and often does) explode. We will want to control this.

The morphsim φ induces $\varphi : E^d \to E_0^d$ for $d \in \mathbb{Z}$. Fix $0 \neq e \in E[\varphi]$. Note

$$\mathrm{Sel}^\varphi E^d \subset H^1(G_\mathbb{Q}, E^d[\varphi]) = \mathrm{Hom}(G_\mathbb{Q}, K_2) \cong \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

We want to think about how these Selmer groups vary with d inside of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

There are three ways that the local conditions can behave:

- ν is good for E (good reduction, not 2 or ∞) and $\nu \nmid d$, and in this case, $\mathcal{L}_\nu = H^1_{ur}(G_{\mathbb{Q}_\nu}, E[\varphi])$.
- ν is bad for E. These are annoying but not important, since there are only finitely many and they do not vary with d, so we have some finite calculation.
- ν is good for E but $\nu | d$. These we must account for carefully.

We have

$$\mathcal{L}_\nu(E^d[\varphi]) = \ker(H^1(G_\nu, E^d[\varphi]) \to H^1(G_\nu, E^d)),$$

and since $\nu \neq 2$, we can restrict to $E^d[2^\infty]$ in that final group (this more-or-less is a thought that comes from Bloch–Kato). We can also flip this around with the exact sequence

$$0 \to E^d[\varphi] \to E^d[2^\infty] \to E_0^d[2^\infty] \to 0,$$

giving the long exact sequence in cohomology and the equality

$$\mathcal{L}_\nu(E^d[\varphi]) = \mathrm{im}(H^0(G_\nu, E_0^d[2^\infty]) \xrightarrow{\delta_d} H^1(G_\nu, E^d[\varphi])).$$

Note that $E_0^d[2^\infty]^{I_\nu} = E_0^d[2]^{I_\nu} = E_0^d[2]$ since $E_0^d[2] \cong E_0[2]$ as Galois modules. Then we also reduce to

$$\mathcal{L}_\nu(E^d[\varphi]) = \mathrm{im}(H^0(G_\nu, E_0[2]) \xrightarrow{\delta_d} H^1(G_\nu, E[\varphi])),$$

where note that we no longer have d in most places. The relevant connecting map is coming from

$$E[\varphi] \to E^d[2\varphi] \to E_0[2],$$

but we can also consider

$$E[\varphi] \to E[2\varphi] \to E_0[2],$$

which is clearly a close relative. If $\langle e' \rangle := E_0[\varphi_0]$, then $\delta_d(e') = \delta_1(e')$. Choosing some $e_2' \in E_0[2] \setminus E_0[\varphi_0]$, if G_ν fixes e_2', then $\delta_d(e_2') = \delta_1(e_2') + \chi_d \cdot e_1$.

Casing on the size of $H^0(G_p, E[2])$ and $H^0(G_p, E_0[2])$, we can calculate $\mathcal{L}_p$:

1. If $\#H^0(G_\nu, E_0[2]) = 4, \#H^0(G_\nu, E[2]) = 2$, then $\mathcal{L}_\nu = 0$ by considering squares mod p.
2. If $\#H^0(G_\nu, E_0[2]) = 2, \#H^0(G_\nu, E[2]) = 2$, then $\mathcal{L}_\nu = H^1_{ur}$.
3. If $\#H^0(G_\nu, E_0[2]) = 4, \#H^0(G_\nu, E[2]) = 4$, , then $\mathcal{L}_\nu \subset \mathbb{Q}_\nu^\times/(\mathbb{Q}_\nu^\times)^2$ is generated by $\delta_d(e_2')$.
4. $\#H^0(G_\nu, E_0[2]) = 2, \#H^0(G_\nu, E[2]) = 4$, then $\mathcal{L}_\nu = \mathbb{Q}_\nu^\times/(\mathbb{Q}_\nu^\times)^2$.

Thus, if you want your Selmer group to be big, one would want a lot of primes satisfying (4); analogously for small Selmer, one wants primes satisfying (1). This allows one to enforce arbitrarily large or small Selmer ranks, if one is careful.

Assume from now on that $E[2](\mathbb{Q}) = E_0[2](\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^2$ — this enforces only having the third type of prime p considered above, and we will consider the mean size of Selmer groups. Let $\mathcal{V}$ equal the set of bad primes, i.e. the set of primes of bad reduction together with 2 and ∞, and let

$$A \coloneqq \prod_{p \in \mathcal{V}, p \neq \infty} p.$$

Choose disjoint, finite sets of primes $X_1, \dots, X_k \subset \mathbb{P}$ without primes dividing A. We identify a tuple $d = (p_1, \dots, p_k) \in X_1 \times \cdots \times X_k$ with the natural number $p_1 \cdots p_k$.

Our goal is to estimate

$$\sum_{d \in X_1 \times \cdots \times X_k} \#\mathrm{Sel}^\varphi E^d.$$

We make the following assumptions, which we refer to later by number

1. For $p_i, p_i' \in X_i$ and $a|A$, we have
$$\left(\frac{a}{p_i}\right) = \left(\frac{a}{p_i'}\right)$$
2. For $i \neq j$ and any function $c : X_i \to [-1, 1]$, the quantity
$$\sum_{p_j \in X_j} \left| \sum_{p_i \in X_i} c(p_i) \cdot \left(\frac{p_i}{p_j}\right) \right|$$
is small.
3. For any divisor $1 \neq a|A$, there exists $i \leq k$ so that
$$\left(\frac{a}{p_i}\right) = -1$$
for all $p_i \in X_i$.

Assumption (2) is natural, and is true for large sieve assumptions on X, like those in [Jut75].

Define

$$V \coloneqq \{a \in \mathbb{Z} : a|A\} \times \mathcal{P}(\{1, \dots, k\}),$$

which we consider as a vector space over $\mathbb{F}_2$ by

$$(a, S) + (a', S') = \left(\frac{\mathrm{lcm}(a, a')}{\gcd(a, a')}, S \setminus S' \cup S' \setminus S\right).$$

For $d = (p_1, \dots, p_k) \in \prod X_i$, which we identify with the natural number $p_1 \cdot \cdots \cdot p_k$, we define

$$\mathcal{B}_d : V \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

$$(a, T) \mapsto a \cdot \prod_{i \in T} p_i.$$

This is evidently an isomorphism onto

$$\{b \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \mid \mathrm{ord}_p(b) \text{ odd} \implies p \in \mathcal{V} \text{ or } p|d\}$$

Claim 93. *Any element in* $\mathrm{Sel}^\varphi E^d$ *is represented in* $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ *by something in the image of* $\mathcal{B}_d$.

This is true because a Selmer element can only be ramified at bad primes of E and primes dividing d.

Let $V_0 \subset V$ be the subspace with $\mathcal{O}_{Ld}(V_0)$ satisfies the local conditions at all bad ν.

Claim 94.

1. *V_0 is independent of $d \in X_1 \times \cdots \times X_k$*
2. *We have an explicit formula for V_0.*

The first is a consequence of assumption (1). We will explain the second claim in the next lecture.

9 Idèle Class Groups for Number Fields and Artin Reciprocity. Speaker: Peikai Qi. Notes by Yen-Kang (Ted) Fu.

9.1 Local Reciprocity Map

Theorem 95. *Let K be a local field, then there exists a (injective) homomorphism*

$$\theta_K : K^\times \hookrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

where K^{ab} is the maximal abelian extension of K, satisfying

1. *Let L/K be a finite abelian extension, then θ_K induces an isomorphism*

$$\begin{aligned} \theta_K : K^\times/\mathrm{Nm}_{L/K}(L^\times) &\to \mathrm{Gal}(L/K) \\ a &\mapsto \theta_K(a)|_L\,, \end{aligned}$$

2. *The group of units are mapped to the inertia group, i.e.*

$$\theta_K(\mathcal{O}_K^\times)\big|_L = I(L/K),$$

3. *If L/K is unramified and π is an uniformizer, then*

$$\theta_K(\pi)|_L = \mathrm{Frob}_{L/K}.$$

The θ_K in this theorem is called the local reciprocity map, and its properties give rise to the following correspondence.

Theorem 96. *We have the following bijections*

$$\left\{ \begin{array}{c} \textit{finite index open} \\ \textit{subgroups of } K^\times \end{array} \right\} \xleftrightarrow{\sim} \left\{ \begin{array}{c} \textit{finite index open} \\ \textit{subgroups of} \\ \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array} \right\} \xleftrightarrow{\sim} \left\{ \begin{array}{c} \textit{finite abelian} \\ \textit{extension of } K \end{array} \right\}$$

$$\mathrm{Nm}_{L/K}(L^\times) = X \longmapsto \overline{\theta_K(X)} \longmapsto \left(K^{\mathrm{ab}}\right)^{\overline{\theta_K(X)}} = L$$

To define the global reciprocity map, one can naively guess that for a global field K, the map is

$$\prod_v K_v^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

where v runs through all the places of K, and K_v denotes the completion of K at place v.

However, the product on the left is not locally compact.

9.2 Idèles

To fix the issue above, we introduce idèles. Let S be a finite set of places of K, and let S_∞ be the set of infinite/archimedean places. Assume that $S \supseteq S_\infty$. Consider

$$\mathbf{I}_S \coloneqq \prod_{v\in S} K_v^\times \times \prod_{v\notin S} \mathcal{O}_v^\times.$$

Since the first product on the right is a finite product of locally compact rings, it's locally compact. Moreover, the second product is a product of compact rings, which is compact by Tychonoff's theorem. Hence $\mathbf{I}_S$ is locally compact. Define the idèles of K to be

$$\mathbf{I}_K = \bigcup_{\substack{S \text{ finite} \\ S \supseteq S_\infty}} \mathbf{I}_S = \left\{ (a_v) \in \prod_v K_v^\times : a_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v \right\}.$$

Note that $\mathbf{I}_K$ is also locally compact as it inherit topologies from each $\mathbf{I}_S$.

Remark 97. One can also use restricted product to define idèles.

Remark 98. Even though $\mathbf{I}_K \subseteq \prod_v K_v^\times$ as sets, $\mathbf{I}_K$ does not inherit the product topology of $K_v^\times$.

There are two important embeddings, namely

$$\begin{aligned} K^\times &\to \mathbf{I}_K \\ a &\mapsto (\ldots, a, a, a, \ldots), \end{aligned}$$

and

$$\begin{aligned} K_v^\times &\to \mathbf{I}_K \\ a &\mapsto (\ldots, 1, a, 1, \ldots), \end{aligned}$$

where the a appears only at the v-th place.

We have the following commuting diagram

$$\begin{array}{ccc} \mathbf{I}_K & \xrightarrow{\theta_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \uparrow & & \uparrow \\ K_v^\times & \xrightarrow{\theta_{K_v}} & \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \end{array}$$

Moreover, suppose L/K is a finite abelian extension that is unramified at v, and w is a place lying above v, we can further extend the diagram

$$\begin{array}{ccccc} \mathbf{I}_K & \xrightarrow{\theta_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) & \xrightarrow{\mathrm{res}} & \mathrm{Gal}(L/K) \\ \uparrow & & \uparrow & & \uparrow \\ K_v^\times & \xrightarrow{\theta_{K_v}} & \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) & \xrightarrow{\mathrm{res}} & \mathrm{Gal}(L_w/K_v) \\ \\ \pi & \longmapsto & & & \mathrm{Frob}_v \\ \\ a & \longmapsto & & & (\mathrm{Frob}_v)^{v_v(a)} \end{array}$$

However, the map θ_K does not provide a global analogy to the correspondence in Theorem 96.

9.3 Classical Artin Reciprocity Map

We will recover the global reciprocity map from the classical Artin reciprocity map. Let L/K be a finite abelian extension. Let S be a finite set of places of K such that

$$S \supseteq \{\text{primes ramified in } L/K\} \cup S_\infty,$$

and let I_S be the abelian group generated by ideals of K not in S. We can define the classical Artin reciprocity map as

$$\begin{aligned}\theta : I_S &\to \mathrm{Gal}(L/K)\\ \mathfrak{p}_1^{r_1}\cdots\mathfrak{p}_s^{r_s} &\mapsto \mathrm{Frob}_{\mathfrak{p}_1}^{r_1}\cdots\mathrm{Frob}_{\mathfrak{p}_s}^{r_s}\end{aligned}$$

Connect this map with the obvious map form $\mathbf{I}_S$ to I_S, we get

$$\begin{aligned}\mathbf{I}_S \to I_S &\overset{\theta}{\mapsto} \mathrm{Gal}(L/K)\\ (a_\mathfrak{p}) &\mapsto \prod_\mathfrak{p} \mathrm{Frob}_\mathfrak{p}^{v_\mathfrak{p}(a_\mathfrak{p})}\end{aligned}$$

Our goal now is to extend this map to the whole $\mathbf{I}_K$.

Definition 99. Let G be a group, a homomorphism $\theta : I_S \to G$ is admissible if for any neighborhood N of $1 \in G$, there exists some $\delta > 0$ such that

$$\theta\left((a)^S\right) \in N$$

whenever $a \in K^\times$ and $|a-1|_v < \delta$ for all $v \in S$. Here $(a)^S$ means throwing away S-primes in the decomposition of fractional ideal.

Theorem 100. *If $I_S \to G$ is admissible, then there exists a unique*

$$\widetilde{\theta}\colon \mathbf{I}_K \to G$$

such that

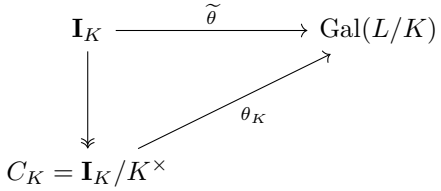
1. *$\widetilde{\theta}$ is continuous,*
2. *$\widetilde{\theta}(K^\times) = 1$,*
3. *$\widetilde{\theta}(a) = \theta\left((a)\right)$ for all $a = (a_v) \in \mathbf{I}_K$ such that $a_v = 1$ for all $v \in S$.*

Fact 101. *Let $S = \{\text{primes ramified in } L/K\} \cup S_\infty$. Then $\theta\colon I_S \to \mathrm{Gal}(L/K)$ is admissible.*

By Theorem 100, we get

$$\widetilde{\theta}\colon \mathbf{I}_K \to \mathrm{Gal}(L/K),$$

which is compatible with the one we got in Section 9.2. Moreover, this map factors through the idèle class group C_K.



Definition 102. We define the norm map on idèles $\mathrm{Nm}_{L/K}\colon \mathbf{I}_L \to \mathbf{I}_K$ coordinate-wise, i.e.

$$\mathrm{Nm}_{L/K} = \prod_w \mathrm{Nm}_{L_w/K_v}.$$

One can show

Theorem 103. *The map*

$$\theta_K\colon \mathbf{I}_K/\mathrm{Nm}_{L/K}(\mathbf{I}_L)K^\times \to \mathrm{Gal}(L/K)$$

is an isomorphism.

9.4 Artin (Global) Reciprocity Map

Theorem 104. *Let K be a global field. Then there exists a homomorphism*

$$\widetilde{\theta}\colon C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

and we call it the global reciprocity map.

Remark 105. Note that this is the global analogue of Theorem 95, and it gives rise to the global analogue of Theorem 96.

Theorem 106. *We have the following bijections:*

$$\left\{\begin{array}{c}\text{finite index open}\\ \text{subgroups of } C_K\end{array}\right\} \xleftrightarrow{\sim} \left\{\begin{array}{c}\text{finite index open}\\ \text{subgroups of}\\ \mathrm{Gal}(K^{\mathrm{ab}}/K)\end{array}\right\} \xleftrightarrow{\sim} \left\{\begin{array}{c}\text{finite abelian}\\ \text{extensions of } K\end{array}\right\}$$

$$K^\times \mathrm{Nm}_{L/K}(\mathbf{I}_L)/K^\times = X \longmapsto \theta_K(X) \longmapsto \left(K^{\mathrm{ab}}\right)^{\theta_K(X)} = L$$

9.5 Properties of C_K and θ_K

Proposition 107. $\mathbf{I}_K = \mathbf{I}_S K^\times$ *for S sufficiently large.*

Proof. Let S_1 be a finite set of primes that generates $\mathrm{Cl}(K)$ and let $S = S_1 \cup S_\infty$. We will show that

$$\mathbf{I}_K = \mathbf{I}_S K^\times.$$

Recall that we have the following map

$$\begin{aligned}\mathbf{I}_K &\to J_K\\ a &\mapsto \prod_{\mathfrak{p}<\infty} \mathfrak{p}^{v_\mathfrak{p}(a_\mathfrak{p})},\end{aligned}$$

where J_K is the group of fractional ideals. By the definition of the class group, there exists $k \in K^\times$ such that (ak) is generated by primes in S_1. Hence

$$v_\mathfrak{p}(ak) = 0 \text{ for } \mathfrak{p} \notin S \implies ak \in \mathbf{I}_S$$

Hence

$$\mathbf{I}_K = \mathbf{I}_S K^\times.$$

□

Corollary 108. *We have*

$$C_K = \mathbf{I}_K/K^\times = \mathbf{I}_S K^\times/K^\times = \mathbf{I}_S/K^\times \cap \mathbf{I}_S = \mathbf{I}_S/\mathcal{O}_S^\times.$$

Proposition 109 (Local–global compatibility)**.** *Let K be a global field and let v be a place. Then we have the following commuting diagram:*

$$\begin{array}{ccc} C_K & \xrightarrow{\theta_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \uparrow & & \uparrow \\ K_v^\times & \xrightarrow{\theta_{K_v}} & \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \end{array}$$

Proposition 110 (Local functoriality)**.** *Let L_w/K_v be a finite abelian extension. Then we have the following commuting diagram:*

$$\begin{array}{ccc} L_w^\times & \xrightarrow{\theta_{L_w}} & \mathrm{Gal}(L_w^{\mathrm{ab}}/L_w) \\ \Big\downarrow{\scriptstyle \mathrm{Nm}} & & \Big\downarrow{\scriptstyle \mathrm{res}} \\ K_v^\times & \xrightarrow{\theta_{K_v}} & \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \end{array}$$

Proposition 111 (Global functoriality)**.** *Let L/K be a finite abelian extension. Then we have the following commuting diagram:*

$$\begin{array}{ccc} C_L & \xrightarrow{\theta_L} & \mathrm{Gal}(L^{\mathrm{ab}}/L) \\ \Big\downarrow{\scriptstyle \mathrm{Nm}} & & \Big\downarrow{\scriptstyle \mathrm{res}} \\ C_K & \xrightarrow{\theta_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

10 Cohen–Lenstra Heuristics, lecture 3. Speaker: Jiuya Wang. Notes by John Yin.

10.1 Malle's conjecture for "admissible" Galois groups

In this section, we recall and extend some of the discussion from §§6.2 and 6.3.

Let Γ be a group. Then, for K a Γ-extension of $\mathbb{Q}$, its Hilbert class field H_K is a Cl_K-extension of K, and we get a short exact sequence of groups

$$1 \to \mathrm{Cl}_K \to \mathrm{Gal}(H_K/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \to 1.$$

Consider the case $\Gamma = C_2$. Since D_ℓ is the only admissible Galois group (see Example 74), we obtain a (non-canonical) $\#\mathrm{Aut}(C_\ell)$-to-1 map

$$\{M/K \mid \mathrm{Gal}(M/\mathbb{Q}) \cong D_\ell, M/K \text{ unramified}\} \to \mathrm{Surj}(\mathrm{Cl}_K, C_\ell)$$

by sending M to the map $\mathrm{Cl}_K \cong \mathrm{Gal}(H_K/K) \to \mathrm{Gal}(M/K) \cong C_\ell$ defined as follows. Fix an expression $M = K(\alpha)$; then the map sends an element $\sigma \in \mathrm{Gal}(H_K/K)$ to the element of $\mathrm{Gal}(M/K)$ which takes α to $\sigma(\alpha)$.

We wish to understand the statistics of $\#\mathrm{Surj}(\mathrm{Cl}_K, C_\ell)$. Continuing in the case $\Gamma = C_2$, the arguments above give that

$$\sum_{K \le X} \#\mathrm{Surj}(\mathrm{Cl}_K, C_\ell) = \frac{1}{\ell - 1} \cdot \#E(D_\ell, X^\ell)',$$

where $\sum_{K \le X}$ denotes the sum over quadratic extensions of $\mathbb{Q}$ of absolute discriminant $\le X$, and $'$ denotes that $I_p \cap C_\ell = \{e\}$ for all p.[23]

In this direction, we have the following result.

Theorem 112 (Davenport–Heilbronn)**.** *In the case where $\Gamma = C_2$ and $\ell = 3$, we have*

$$\frac{\sum_{K \le X, \pm} \#\mathrm{Surj}(\mathrm{Cl}_K, C_3)}{\sum_{K \le X, \pm} 1} = \begin{cases} 1, & \pm = + \\ 1/3, & \pm = -, \end{cases}$$

where $\sum_{K \le X,+}$ denotes the sum over imaginary quadratic number fields of absolute discriminant $\le X$, and $\sum_{K \le X,-}$ denotes the sum over real quadratic number fields of absolute discriminant $\le X$.

This is proven by studying Malle's conjecture for S_3-extensions.

We also have analogous results for groups Γ other than C_2.

Theorem 113 (Bhargava)**.** *In the case where $\Gamma = S_3$ and $\ell = 2$, we have*

$$\frac{\sum_{K \le X, \pm} \#\mathrm{Surj}(\mathrm{Cl}_K, C_2)}{\sum_{K \le X, \pm} 1} = \begin{cases} 1/2, & \pm = + \\ 1/4, & \pm = -, \end{cases}$$

where $\sum_{K \le X,+}$ denotes the sum over non–totally real cubic number fields of absolute discriminant $\le X$, and $\sum_{K \le X,-}$ denotes the sum over totally real cubic number fields of absolute discriminant $\le X$.

This is proven by studying Malle's conjecture for S_4-extensions.

Now consider the following setup. Let H be a 2-group, and let $\Gamma = C_2 \wr H$. It is a fact that any Γ-extension K contains a unique index-2 subextension, which we will denote F_K. Then the following holds.

[23] The appearance of X^ℓ is due to the fact that if M/K is unramified, one has $\mathrm{Disc}(M) = \mathrm{Disc}(K)^{[M:K]}$.

Theorem 114 (Lemke Oliver–Wang–Wood)**.**

$$\frac{\sum_{K \leq X,u} \#\mathrm{Surj}(\mathrm{Cl}_{K/F_K}, C_3)}{\sum_{K \leq X,u} 1} = 3^{-u},$$

where $\sum_{K \leq X,u}$ *denotes the sum over* K *as above such that* $\mathrm{rk}(\mathcal{O}_K^\times) - \mathrm{rk}(\mathcal{O}_{F_K}^\times) = u$.

This is proven by extending the ideas of Davenport–Heilbronn.

Our hope is that by gathering enough knowledge about the moments of $\#\mathrm{Cl}_K[\ell]$, we will understand the behavior of class groups. This gives us three main questions:

1. What behavior should we look for? In other words, what conjectures should we make?
2. How much knowledge is enough?
3. How do we gather this information?

10.2 Detour to counting abelian extensions

As discussed in §2.3, the Kronecker–Weber theorem says that for an abelian group A, the A-extensions of $\mathbb{Q}$ correspond to maps $\prod_p \mathbb{Z}_p^\times \to A$. Moreover, these maps also contain the information of ramification at all primes. Over general a number field K, however, maps $\prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^\times \to A$ specifying ramification information at the various primes will not capture all A-extensions of K. Indeed, there can exist nontrivial abelian everywhere unramified extensions of K (such as the Hilbert class field). So, one should include a finite set S of finite places such that maps $\prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^\times \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}}^\times \to A$ indeed exhaust all the A-extensions (e.g. we may take S to generate the class group of K). But now, not all such maps correspond to extensions. For example, if two primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ represent the same element in the class group, then they cannot represent different Frobenius elements $\mathrm{Frob}_{\mathfrak{p}_1}$ and $\mathrm{Frob}_{\mathfrak{p}_2}$ in the class field under the reciprocity map. In the end, what we have, from global class-field theory, is that maps of the form

$$\frac{\prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^\times \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}}^\times}{\mathcal{O}_S^\times} \to A$$

will parameterize abelian extensions. The slogan here is:

1. The image of $\mathcal{O}_{\mathfrak{p}}^\times$ under the reciprocity map is the inertia group.
2. The image of the uniformizer of $\mathcal{O}_{\mathfrak{p}}$ will be mapped to the Frobenius element, and so the image of $K_{\mathfrak{p}}^\times$ under the reciprocity map will be the decomposition group.

For more details on this, see the pretalk (§9), and for even more details, see https://kskedlaya.org/cft/sec_abstractcft3.html. With this setup, the unramified abelian extensions of K correspond to those maps $\prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^\times \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}}^\times \to A$ which are trivial on each $\mathcal{O}_{\mathfrak{p}}^\times$.

Turning toward the class group, we have a surjective map

$$\prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^\times / \mathcal{O}_{\mathfrak{p}}^\times \to \mathrm{Cl}_K$$

corresponding (in the sense of the previous paragraph) to the Hilbert class field. Since $\mathcal{O}_S^\times$ maps to the Galois group trivially, we in fact have an exact sequence

$$\mathcal{O}_S^\times \to \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^\times / \mathcal{O}_{\mathfrak{p}}^\times \to \mathrm{Cl}_K \to 0.$$

Now

$$\prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^\times / \mathcal{O}_{\mathfrak{p}}^\times \cong \mathbb{Z}^{\#S},$$

and, if K is imaginary quadratic,

$$\mathcal{O}_S^\times \cong \mathbb{Z}^{\#S} \times (\text{torsion}).$$

In this case, if we let M be the composition $\mathbb{Z}^{\#S} \cong \mathcal{O}_S^\times \to \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^\times/\mathcal{O}_\mathfrak{p}^\times \cong \mathbb{Z}^{\#S}$, we realize Cl_K as a the cokernel of M. Localizing at p, we have that $\mathrm{Cl}_K[p^\infty]$ is isomorphic to the cokernel of M, considered as a linear map $M\colon \mathbb{Z}_p^{\#S} \to \mathbb{Z}_p^{\#S}$.

Guess (following Ellenberg–Venkatesh): M is a random matrix.

10.3 Random matrices

We continue to assume K is imaginary quadratic.

Continuing from before, let $n \coloneqq \#S$. We now assume M is random with respect to the Haar measure ν on $n \times n$ matrices over $\mathbb{Z}_p$. We wish to calculate the A-moments of $\mathrm{Cl}_K[p^\infty]$ (assuming n is constant). By our assumption that M is random, this should be

$$\begin{aligned}
\mathbb{E}[\#\mathrm{Surj}(\mathrm{Coker}(M), A)] &= \int_M \#\mathrm{Surj}(\mathrm{Coker}(M), A)\, d\nu && (10.1)\\
&= \int_M \#\{f \in \mathrm{Surj}(\mathbb{Z}_p^n, A) \mid M\mathbb{Z}_p^n \subset \mathrm{Ker}(f)\}\, d\nu && (10.2)\\
&= \sum_{f:\mathbb{Z}_p^n \twoheadrightarrow A} \nu(\{M \mid \text{Column vectors of } M \text{ live in } \mathrm{Ker}(f)\}) && (10.3)\\
&= \#\mathrm{Surj}(\mathbb{Z}_p^n, A) \cdot \frac{1}{(\#A)^n} && (10.4)\\
&= \sum_{B\le A} \frac{\#\mathrm{Hom}(\mathbb{Z}_p^n, B) \cdot \mu(A,B)}{(\#A)^n} && (10.5)\\
&= \sum_{B\le A} \frac{(\#B)^n \cdot \mu(A,B)}{(\#A)^n} && (10.6)
\end{aligned}$$

where μ is the Möbius function, and we used the Möbius inversion formula in equation (10.5). As n approaches infinity, the expected value (10.1) approaches 1. In the real quadratic case, everything is very similar, except that $\mathcal{O}_S^\times \cong \mathbb{Z}^{n+1} \times (\text{torsion})$, and our matrices M are $(n+1)\times n$. So n will become $n+1$ in some expressions, and the expected value (10.1) will approach $1/\#A$ instead of 1.

The Cohen–Lenstra heuristics deal with something different. We want not the expected value, but the

probability that $\mathrm{Coker}(M) \cong A$. We compute this as follows:

$$\begin{aligned}
\mathbb{P}(\mathrm{Coker}(M) \cong A) &= \sum_{W \subseteq \mathbb{Z}_p^n, \mathbb{Z}_p^n/W \cong A} \mathbb{P}(\mathrm{Img}(M) = W) && (10.7)\\
&= \sum_{W \subseteq \mathbb{Z}_p^n, \mathbb{Z}_p^n/W \cong A} \mathbb{P}(\mathrm{Img}(M) = W) && (10.8)\\
&= \sum_{W \subseteq \mathbb{Z}_p^n, \mathbb{Z}_p^n/W \cong A} \mathbb{P}(\mathrm{Img}(M) \subseteq W) \cdot \mathbb{P}(\mathrm{Img}(M) = W \mid \mathrm{Img}(M) \subseteq W) && (10.9)\\
&= \sum_{W \subseteq \mathbb{Z}_p^n, \mathbb{Z}_p^n/W \cong A} \frac{1}{(\#A)^n} \prod_{i=1}^{n} \left(1 - \frac{1}{p^i}\right) && (10.10)\\
&= \#\{W \subseteq \mathbb{Z}_p^n : \mathbb{Z}_p^n/W \cong A\} \cdot \frac{1}{(\#A)^n} \prod_{i=1}^{n} \left(1 - \frac{1}{p^i}\right) && (10.11)\\
&= \frac{\#\mathrm{Surj}(\mathbb{Z}_p^n, A)}{\#\mathrm{Aut}(A)} \cdot \frac{1}{(\#A)^n} \prod_{i=1}^{n} \left(1 - \frac{1}{p^i}\right) && (10.12)\\
&= \frac{1}{\#\mathrm{Aut}(A)} \prod_{i=1}^{n} \left(1 - \frac{1}{p^i}\right) \sum_{B \leq A} \frac{(\#B)^n}{(\#A)^n} \cdot \mu(A, B) && (10.13)
\end{aligned}$$

where in the last equality, we used the same steps as equations (10.4)–(10.6) above. Taking n to infinity, we obtain $1/\#\mathrm{Aut}(A) \cdot \prod_{i \geq 1}(1 - p^{-i})$ as our final probability. The real quadratic case is similar and requires the same changes as above; taking n to infinity, we obtain $1/(\#A \cdot \#\mathrm{Aut}(A)) \cdot \prod_{i \geq 2}(1 - p^{-i})$ as our answer instead.

Heuristic 115 (Cohen–Lenstra heuristics)**.** *For an imaginary quadratic field number field K, we have $\mathbb{P}(\mathrm{Cl}_K[p^\infty] \cong A) \sim 1/\#\mathrm{Aut}(A)$; for a real quadratic number field K, we have $\mathbb{P}(\mathrm{Cl}_K[p^\infty] \cong A) \sim 1/(\#A \cdot \#\mathrm{Aut}(A))$.*

10.4 Cohen–Martinet heuristics

We now want to consider K which are not necessarily quadratic. The setup is similar to the above, except that we now have more actions of the Galois group on the class group. (In the quadratic case, there is only one action of the Galois group on the class group, leading us to look at only the dihedral group.)

In this case, we still have an exact sequence $\mathcal{O}_S^\times \to \prod_{\mathfrak{p} \in S} K_\mathfrak{p}^\times / \mathcal{O}_\mathfrak{p}^\times \to \mathrm{Cl}(K) \to 0$, where here we choose S such that all primes in S split in K. Then Γ acts on primes $\mathfrak{p}$ lying over p as an induced module, i.e.

$$\prod_{\mathfrak{p} \in S} K_\mathfrak{p}^\times / \mathcal{O}_\mathfrak{p}^\times \cong \prod_{p < \infty, \exists \mathfrak{p} \in S, \mathfrak{p} \mid p} \mathbb{Z}[\Gamma].$$

Then, using Dirichlet's unit theorem (for S-units),

$$(\mathcal{O}_S^\times \otimes \mathbb{Z}_p) \oplus \mathbb{Z}_p \cong \bigoplus_{\mathfrak{p} \in S(K) \cup S_\infty(K)} \mathbb{Z}_p \cong \mathrm{Ind}_{D_\infty}^\Gamma(\mathbb{Z}_p) \oplus \bigoplus_{p < \infty, \exists \mathfrak{p} \in S, \mathfrak{p} \mid p} \mathbb{Z}_p[\Gamma]. \tag{10.14}$$

So, we obtain in a similar way a linear map

$$M \colon \mathrm{Ind}_{D_\infty}^\Gamma(\mathbb{Z}_p) \oplus \bigoplus_{p < \infty, \exists \mathfrak{p} \in S, \mathfrak{p} \mid p} \mathbb{Z}_p[\Gamma] \to \prod_{p < \infty, \exists \mathfrak{p} \in S, \mathfrak{p} \mid p} \mathbb{Z}_p[\Gamma].$$

Let $n \coloneqq \#\{p < \infty \mid \exists \mathfrak{p} \in S, \mathfrak{p} \mid p\}$. Then M is a map from $\mathrm{Ind}_{D_\infty}^\Gamma(\mathbb{Z}_p) \oplus \mathbb{Z}_p[\Gamma]^n$ to $\mathbb{Z}_p[\Gamma]^n$. Now we use the fact that the image of the copy of $\mathbb{Z}_p$ in equation (10.14) in Cl_K must be 0 if $p \nmid \#\Gamma$. This is because $\mathbb{Q}$ has

class number 1, so Cl_K has no Γ-invariant elements. So, now we focus on the nontrivial part modeled by $\mathrm{Coker}(M)$ where M is random.

Let A be a Γ-module such that $A^\Gamma = \{1\}$. Then

$$\begin{aligned}
\mathbb{E}[\#\mathrm{Surj}_\Gamma(\mathrm{Coker}(M), A)] &= \int \#\{f \in \mathrm{Surj}(\mathbb{Z}_p[\Gamma]^n, A) \mid f(\mathrm{Img}(M)) = 0\}\, d\nu && (10.15)\\
&= \sum_f \nu(\{M \mid \mathrm{Img}(M) \subseteq \mathrm{Ker}(f)\}) && (10.16)\\
&= \sum_f \frac{1}{(\#A)^n} \cdot \frac{1}{\#A^{D_\infty}} && (10.17)\\
&= \#\mathrm{Surj}(\mathbb{Z}_p[\Gamma]^n, A) \cdot \frac{1}{(\#A)^n} \cdot \frac{1}{\#A^{D_\infty}} && (10.18)\\
&= \sum_{B \le A} \#\mathrm{Hom}(\mathbb{Z}_p[\Gamma]^n, B) \cdot \mu(A, B) \cdot \frac{1}{(\#A)^n} \cdot \frac{1}{\#A^{D_\infty}} && (10.19)\\
&= \sum_{B \le A} (\#B)^n \cdot \mu(A, B) \cdot \frac{1}{(\#A)^n} \cdot \frac{1}{\#A^{D_\infty}}, && (10.20)
\end{aligned}$$

where we used the fact that the image of $\mathrm{Ind}_{D_\infty}^\Gamma(\mathbb{Z}_p)$ mapping into the kernel of f is equivalent to $\mathrm{Ind}_{D_\infty}^\Gamma(\mathbb{Z}_p)$ mapping into the part of kernel of f which is Γ-invariant, since we are only considering Γ-equivariant maps (this is the universal property of Ind groups). Now the final expression approaches $1/\#A^{D_\infty}$ as n tends to ∞. More generally, if our base field F has more than one infinite place, we can write down $\mathcal{O}_S^\times$ as $\prod_{v|\infty} \mathrm{Ind}_{\Gamma_v}^\Gamma(\mathbb{Z}_p) \oplus \prod_{v \in \mathrm{Spec}(\mathcal{O}_F), \exists \mathfrak{v}|v, \mathfrak{v} \in S} \mathbb{Z}_p[\Gamma]$. This will lead to $\mathbb{E}[\#\mathrm{Surj}_\Gamma(\mathrm{Coker}(M), A)] \to 1/\prod_{v|\infty} \#A^{\Gamma_v}$.

10.5 Moments determine the distribution

Theorem 116 (Wang–Wood, Sawin–Wood)**.** *The Cohen–Martinet moments determine the probability distribution*

$$\mathbb{P}(\mathrm{Coker}(M) \cong A) \sim \frac{1}{\#\mathrm{Aut}_\Gamma(A)} \cdot \frac{1}{\prod_{v|\infty} \#A^{\Gamma_v}}.$$

This theorem implies that it is enough to understand the A-moment $\mathbb{E}[\#\mathrm{Surj}_\Gamma(\mathrm{Coker}(M), A)]$ for every $\mathbb{Z}_p[\Gamma]$-module A. That is, it's enough to prove

Conjecture 117. $\displaystyle\lim_{X \to \infty} \frac{\sum_{K \le X} \#\mathrm{Surj}(\mathrm{Cl}_K[p^\infty], A)}{\sum_{K \le X} 1} = \frac{1}{\prod_{v|\infty} \#A^{\Gamma_v}}.$

There are three issues to watch out for.

1. Summing over $K \le X$ doesn't always work. This is because there can be many K that are extensions of the same intermediate subfield. One way to fix this, following Bartel–Lenstra, is to use $\mathrm{rad}(K)$, the product of ramified primes.
2. Even using $\mathrm{rad}(K)$, one can have the same phenomenon over cyclotomic fields. To remedy this, Koymans–Pagano and Wang suggest restricting to K such that $K \cap \mathbb{Q}(\zeta_{\#\Gamma}) = \mathbb{Q}$.
3. When the base field contains p-th roots of unity, the A-moments are fundamentally different.

The first two issues affect the denominator, while the third affects the numerator.

11 Studying Class Groups as Selmer Groups in Quadratic Twist Families. Speaker: Alexander Slamen. Notes by Yen-Kang (Ted) Fu.

References for this pretalk: [Smi17], [Smi22b], [Smi22a], [MS22], and [MS24].

Recall from class-field theory that if $K/\mathbb{Q}$ is a quadratic extension, then we have

$$\mathrm{Cl}^+(K)[2] \simeq (\mathbb{Z}/2\mathbb{Z})^{|\mathrm{ram}(K)-1|},$$

where $\mathrm{Cl}^+(K)$ is the narrow class group.

Definition 118. The narrow class group $\mathrm{Cl}^+(K)$ of K is defined to be

$$\mathrm{Cl}^+(K) = I_K/P_K^+,$$

where I_K is the group of fractional ideals, and P_K^+ is the totally real principal ideals, i.e.

$$P_K^+ = \left\{a \in K^\times : \sigma(a) > 0 \text{ for all real embeddings } \sigma : K \to \mathbb{R}\right\}.$$

Remark 119. The narrow class groups are a special case of the ray class groups [Mil20b, p. 149].

When K is an imaginary quadratic field, Gerth suggested that $\mathrm{Cl}^+(K)[2^\infty]$ follows the Cohen–Lenstra distribution.

For $g \geq 1$, we have

$$r_{2^k}(K) = \mathrm{rk}_{2^k}(K) = \dim_{\mathbb{F}_q} 2^{t-1}\mathrm{Cl}^+(K)[2^k].$$

This implies

$$\mathrm{Cl}(K)[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^{r_2(K)-r_4(K)} \oplus (\mathbb{Z}/4\mathbb{Z})^{r_4(K)-r_8(K)} \oplus \cdots$$

Theorem 120. *[Smi22b, Theorem 1.9] For $r_4 \geq r_8 \geq \cdots$,*

$$\lim_{H\to\infty} \frac{\#\left\{d \in \mathbb{Z}_{>0} : d \text{ square free } d < H, r_{2^t}\left(\mathbb{Q}(\sqrt{-d})\right) = r_{2^t}, t \geq 2\right\}}{H}$$
$$= P^{\mathrm{Mat}}(r_4 \mid \infty)\prod_{t=3}^{\infty} P^{\mathrm{Mat}}(r_{2^t} \mid r_{2^{t-1}}),$$

where $P^{\mathrm{Mat}}(j \mid n)$ is the probability that a randomly chosen $n \times n$ matrix with $\mathbb{F}_2$ coefficients has kernel of rank j.

In other words, as d varies, the sequence

$$\left(r_4\left(\mathbb{Q}(\sqrt{-d})\right), r_8\left(\mathbb{Q}(\sqrt{-d})\right), \ldots\right)$$

behaves like a time-homogeneous Markov chain.

We can study class groups as a kind of Selmer group.

Let $M = \mathbb{Q}_\ell/\mathbb{Z}_\ell$ be a G_K module with trivial action. For each place v, let the local condition (see Definition 91) be

$$\mathcal{L}_v = H^1_{\mathrm{ur}}(G_v, M),$$

i.e. unramified everywhere.

Then we have

$$\begin{aligned}\mathrm{Sel}_K(M,(\mathcal{L}_v)_v) &= \ker\left(H^1(G_K,M)\to\prod_v H^1(G_v,M)/\mathcal{L}_v\right)\\ &= \mathrm{Hom}(\mathrm{Gal}(H_K/K),\mathbb{Q}_\ell/\mathbb{Z}_\ell)\\ &= \mathrm{Cl}^+(K)[\ell^\infty],\end{aligned}$$

where H_K is the Hilbert class field, by class field theory

Definition 121. The Hilbert class field H_K of K is the maximal abelian unramified extension of K.

Since $G_K \le G_{\mathbb{Q}}$, we get an induced module

$$\mathrm{Ind}_{K/\mathbb{Q}}M = \mathbb{Z}[G_{\mathbb{Q}}]\otimes_{\mathbb{Z}[G_K]} M.$$

Fact 122. *We have an isomorphism*

$$\mathrm{Sel}_K(M)\simeq \mathrm{Sel}_{\mathbb{Q}}(\mathrm{Ind}_{K/\mathbb{Q}}M).$$

Remark 123. This isomorphism works since the local conditions can be passed by Shapiro's lemma.

If $\ell\neq 2$, then

$$\begin{aligned}\mathrm{Ind}_{K/\mathbb{Q}}M &\simeq M\oplus M^\chi\\ 1\otimes m &\mapsto (m,m)\\ \sigma\otimes m &\mapsto (m,-m),\end{aligned}$$

where χ is a quadratic character of K. Hence

$$\mathrm{Cl}^+(K)[\ell^\infty]\simeq \mathrm{Cl}^+(\mathbb{Q})[\ell^\infty]\oplus \mathrm{Sel}_{\mathbb{Q}}(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^\chi.$$

On the other hand, when $\ell=2$, applying $H^\bullet$ to the short exact sequence

$$0\longrightarrow \tfrac{1}{2}\mathbb{Z}/\mathbb{Z}\longrightarrow \mathrm{Ind}_{K/\mathbb{Q}}M\longrightarrow M\oplus M^\chi\longrightarrow 0$$

we get a long exact sequence containing

$$\mathrm{Sel}_{\mathbb{Q}}\left(\tfrac{1}{2}\mathbb{Z}/\mathbb{Z}\right)\longrightarrow \mathrm{Cl}^+(K)[2^\infty]\longrightarrow \underbrace{\mathrm{Cl}^+(\mathbb{Q})[\ell^\infty]}_{=0}\oplus \mathrm{Sel}_{\mathbb{Q}}(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^\chi$$

In order to decompose $\mathrm{Cl}^+(K)[2^\infty]$, we will try to extend the exact sequence. Note that associated to the short exact sequence is a Cassels–Tate pairing (see Theorem 146)

$$\langle -,-\rangle_{\mathrm{CT}} : \mathrm{Sel}_{\mathbb{Q}}\left(M\oplus M^\chi\right)\times \mathrm{Sel}_{\mathbb{Q}}\left(\frac{1}{2}\mathbb{Z}/\mathbb{Z}\right)^\vee\to \mathbb{Q}/\mathbb{Z},$$

with

$$\ker_L = \mathrm{Im}\left(\mathrm{Sel}_{\mathbb{Q}}(\mathrm{Ind}_{K/\mathbb{Q}}M)\to \mathrm{Sel}_{\mathbb{Q}}\left(M\oplus M^\chi\right)\right).$$

This allows us to extend the long exact sequence by one term.

$$\mathrm{Sel}_{\mathbb{Q}}\left(\tfrac{1}{2}\mathbb{Z}/\mathbb{Z}\right)\longrightarrow \mathrm{Cl}^+(K)[2^\infty]\longrightarrow 0\oplus \mathrm{Sel}_{\mathbb{Q}}(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^\chi$$

$$\underbrace{\mathrm{Hom}\left(\mathrm{Sel}_{\mathbb{Q}}(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^\chi,\mathbb{Q}/\mathbb{Z}\right)}_{=0 \text{ by Hilbert 90}}$$

Theorem 124. *Let K be an imaginary quadratic extension. We have an exact sequence of Galois modules*

$$\begin{array}{ccccccc} 0 & & & & & & \\ \downarrow & & & & & & \\ \left(\mathrm{Cl}^+(K)\right)^{\mathrm{Gal}(K/\mathbb{Q})}[2^\infty] & \longrightarrow & \mathrm{Sel}_{\mathbb{Q}}\left(\tfrac{1}{2}\mathbb{Z}/\mathbb{Z}\right) & \longrightarrow & \mathrm{Cl}^+(K)[2^\infty] & \longrightarrow & \mathrm{Sel}_{\mathbb{Q}}(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^\chi \\ & & & & & & \downarrow \\ & & & & & & 0 \end{array}$$

Remark 125. The second term $\left(\mathrm{Cl}^+(K)\right)^{\mathrm{Gal}(K/\mathbb{Q})}[2^\infty]$ comes from genus theory (see §6) with fixed genus, and the fourth term $\mathrm{Sel}_{\mathbb{Q}}(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^\chi$ comes from the twist family.

12 The distribution of 2-Selmer groups in quadratic twist families, lecture 3. Speaker: Alexander Smith. Notes by William C. Newman.

12.1 2-Isogeny Selmer group's average size cont.

We continue with computing the average size of $\mathrm{Sel}^{\varphi} E$ from last lecture.

We can view V_0 as a Selmer group of the module μ_2 with local conditions given by

$$\mathcal{L}_\nu = \begin{cases} \mathcal{L}_\nu(E^d[\varphi]) & v \in \mathcal{V} \\ H^1(G_\nu.E[\varphi]) & v = p|d \\ H^1_{\mathrm{ur}}(G_\nu, E[\varphi]) & \text{other } \nu. \end{cases}$$

Then, the dual Selmer group has module μ_2 and local conditions given by

$$\mathcal{L}^\vee_\nu = \begin{cases} \mathcal{L}_\nu(E^d_0[\varphi_0]) & v \in \mathcal{V} \\ 0 & v = p|d \\ H^1_{\mathrm{ur}}(G_\nu, E[\varphi]) & \text{other } \nu. \end{cases}$$

By the Greenberg-Wiles formula, we have

$$\frac{\#\mathrm{Sel}(\mu_2, \mathcal{L}_\nu)}{\#\mathrm{Sel}(\mu_2, \mathcal{L}^\vee_\nu)} = 2^k \prod_{v \in \mathcal{V}} \left(\frac{\#\mathcal{L}(E^d[\varphi])}{\#\mathcal{L}(E^d_0[\varphi_0])} \right)^{\frac{1}{2}}.$$

Assumption (3) on the sets X gives that the dual Selmer group $\mathrm{Sel}(\mu_2, \mathcal{L}^\vee_\nu)$ is trivial, and so the left hand side equals $\#V_0$.

For a statement P, let $[P]$ be 1 if P is true and 0 if P is false. Then we can write

$$\begin{aligned} \sum_{d \in X} \#\mathrm{Sel}^{\varphi} E^d &= \sum_{d \in X} \sum_{v \in \mathcal{V}_0} [\mathcal{B}_d(v) \text{ obeys all of the local conditions}] \\ &= \sum_{d \in X} \sum_{v \in \mathcal{V}_0} \prod_{i \le k} [\mathcal{B}_d(v) \text{ obeys the local condition at } p_i]. \end{aligned}$$

From last time, we know that $\mathcal{B}_d(v)$ satisfies the local conditions at p_i if and only if $\mathcal{B}_d(v) \in (Q^\times_{p_i})^2$ or $a_2 d \mathcal{B}_d(v) \in (Q^\times_{p_i})^2$. Take $(a, T) \in V_0$, and recall $\mathcal{B}_d(a, T) = a \prod_{i \in T} p_i$. Let

$$\kappa_j := \begin{cases} a \prod_{i \in T} p_i & j \notin T \\ a_2 a \prod_{i \notin T} p_i & j \in T. \end{cases}$$

Then we can rewrite the above sum as

$$\sum_{v \in V_0} \sum_{d \in X} \prod_{i \le k} \frac{1}{2} \left(1 + \left(\frac{\kappa_i}{p_i} \right) \right) = \sum_{v \in V_0} \sum_{R \subseteq \{1, \ldots, k\}} \sum_{d \in X} 2^{-k} \prod_{i \in R} \left(\frac{\kappa_i}{p_i} \right).$$

Now, we use assumption (2) to cut down on the number of terms. For a fixed $v = (a, T)$ and R, the term will have a $\left(\frac{p_i}{p_j}\right)$ or $\left(\frac{p_j}{p_i}\right)$ factor so long as both T and R are not equal to $\varnothing, \{1, \ldots, k\}$. By assumption (2), these terms are not asymptotically significant.

The $T = \emptyset$ and $T = \{1, \ldots, k\}$ terms give contribution $2 \cdot 2^{-k} \#\mathcal{P}(\{1, \ldots, k\}) = 2\#X$. The $R = \emptyset$ and $R = \{1, \ldots, k\}$ terms, not counting the cases $T = \emptyset$ and $T = \{1, \ldots, k\}$, give contribution $(\#V_0 - 2) \cdot 2^{-k} \cdot 2 \cdot \#X$. Hence, using our formula for $\#V_0$, we have

$$\sum_{d \in X} \#\mathrm{Sel}^{\varphi} E^d \simeq 2\#X + 2\mathcal{T}\#X,$$

where

$$\mathcal{T} = \prod_{v \in \mathcal{V}} \left(\frac{\#\mathcal{L}(E^d[\varphi])}{\#\mathcal{L}(E_0^d[\varphi_0])} \right)^{\frac{1}{2}}.$$

This gives the Selmer moment, but we want to understand the entire Selmer distribution.

12.2 Higher Moments

One can modify the above to estimate the higher moments

$$\sum_{d \in X} \#(\mathrm{Sel}^{\varphi} E^d)^m$$

for some $m \geq 2$. One considers

$$\mathcal{B}_d : (\{a \in \mathbb{Z} : a | A\} \times \mathcal{P}(1, \ldots, k))^m \to H^1(G_{\mathbb{Q}}, E[\varphi])^m$$

which maps isomorphically onto the tuples of elements which are unramified outside of places in $\mathcal{V}$ and primes dividing d. Then, our sum becomes

$$\sum_{v \in V} \sum_{d \in X} [\mathcal{B}_d(v) \text{ parameterizes an } m\text{-tuple of } \varphi \text{ Selmer elements of } E^d]$$

which can also be written as

$$\sum_{v \in C_0} \sum_{R \in \mathcal{P}(\{1,\ldots,k\})^m} \sum_{d \in X} \langle v, r \rangle_d$$

where $\langle v, r \rangle_d$ is some pairing. As before, in evaluating this, one gets an explicit asymptotic expression, involving some Tamagawa ratios.

Thus, we can compute the higher moments of the Selmer distribution. Can one recover the whole distribution from just the moments? In the case of this distribution however, the answer is yes, but in the general theory of distributions, the answer is no, and this problem is subtle.

12.3 More general torsion types

This method applies to more general situations, such as the following example. Assume $E/\mathbb{Q}$ is an elliptic curve with no rational 2-torsion. We want to approximate

$$\sum_{d \in X} \#\mathrm{Sel}^2 E^d$$

with $X = X_1 \times \cdots \times X_k$ as before.

The following propositions indicate that the work done above generalizes to this situation.

Proposition 126. *For each $d \in X$, we can define a natural parameterization*

$$\mathcal{B}_d \colon V \xrightarrow{\sim} \{\phi \in H^1(G_{\mathbb{Q}}, E[2]) \mid \phi \text{ unramified outside of } \mathcal{V}, p | d\}$$

Proposition 127. *Given $w \in C$, and $i \leq k$, we can check whether $\mathcal{B}_d(W)$ satisfies the local conditions at p_i from the value of certain "generalized Legendre symbols" $[p_i, p_j]$.*

Proposition 128. *Given $i \neq j$, a function $c \colon X_i \to [-1, 1]$ and any function $f \colon \to [-1, 1]$ with average 0, we have*

$$\sum_{p_i \in X_i} \left| \sum_{p_j \in X_j} c(p_i) F([p_i, p_j]) \right| \leq \max(X_i) \max(X_j) (\max(X_i)^{-\varepsilon} + \max(X_j)^{-\varepsilon})$$

for some natural large sieve assumptions on X.

12.4 Gridding

We have shown how to find the asymptotic distribution of of the sizes of Selmer groups over d in a grid $X = X_1 \times \cdots \times X_k$. But we would like to calculate the distribution over d in $\mathbb{N}$. The idea is that we can say that the distributions are actually the same, if we can show that the grid approximates the numbers $\leq H$ well enough.

Proposition 129. *Choose H very large. Suppose*

$$\frac{1}{|X|}\sum_{d\in X}(\#\mathrm{Sel}^2 E^d)^m \simeq \zeta$$

for all $X = X_1 \times \cdots \times X_k$ satisfying

1. *$k \simeq \log\log H$*
2. *For $i \leq k$, either*
$$X_i = \{p_i\},\ \textit{with } p_i \leq \exp^{(3)}\left(\frac{1}{3}\log^{(3)} H\right)$$
or X_i is all primes in $[B, B(1+\exp^{(3)}(\frac{1}{3}\log^{(3)} H)^{-1}]$ satisfying a congruence condition mod A, where
$$\exp^{(3)}\left(\frac{1}{3}\log^{(3)} H\right) \leq B \leq H.$$
3. *5 more conditions, which we omit here (see [Smi22b, Section 8] for these conditions).*

Then

$$\frac{1}{|H|}\sum_{d\leq H}(\#\mathrm{Sel}^2 E^2)^m = \zeta$$

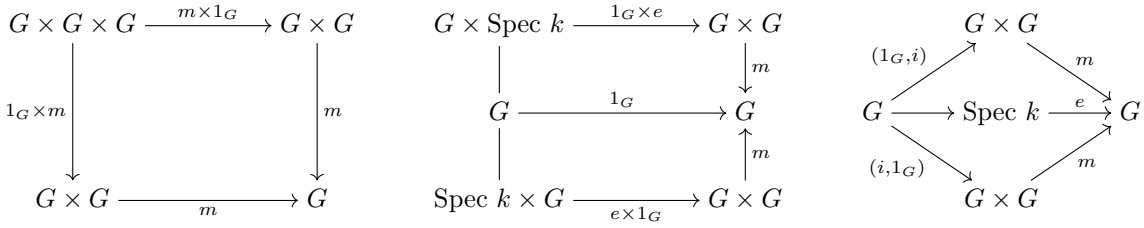
Now, these grids do not satisfy assumption (2), because they allow for small primes. If X_i is a singleton and we need to control $[p_i, p_j]$ for X_j not a singleton, we use the unconditional Chebotarev density theorem.

13 Weil Pairing. Speaker: Shiva Chidambaram. Notes by Santak Panda.

The goal of this pre-talk is to define the Weil pairing on a polarized abelian variety (X, λ) and use this to say something about the image of the ℓ-adic Galois representations for primes ℓ not dividing the degree of λ. This would generalize the familiar Weil pairing in the case of elliptic curves (see §III.8 of [Sil09]).

13.1 Definitions and some properties of abelian varieties

Let K be a field. A group scheme over S is a scheme $\mathcal{G}$ over S with morphisms $e\colon S \to \mathcal{G}$, $i\colon \mathcal{G} \to \mathcal{G}$, $m\colon \mathcal{G} \times \mathcal{G} \to \mathcal{G}$ satisfying the following commutative diagrams:



Example 130. $\mathbb{G}_m = \operatorname{Spec}(\mathbb{Z}[T, T^{-1}])$ is a group scheme together with $e\colon \mathbb{Z}[T, T^{-1}] \to \mathbb{Z}$ sending $T \mapsto 1$, $i\colon \mathbb{Z}[T, T^{-1}] \to \mathbb{Z}[T, T^{-1}]$ sending $T \mapsto T^{-1}$ and $m\colon \mathbb{Z}[T, T^{-1}] \to \mathbb{Z}[T_1, T_1^{-1}, T_2, T_2^{-1}]$ sending $T \mapsto T_1 T_2$.

Definition 131. An abelian variety/K is a reduced connected projective[24] group scheme/K.

An elliptic curve over K is an abelian variety (cf. group law algorithm 2.3 in §III.2 and proposition 1.1 in §II.1 of [Sil09]). Consequently, a finite product $E_1 \times \cdots \times E_g$ of elliptic curves $E_1, \cdots, E_g$ is an abelian variety of dimension g. From a curve C/K of genus g we can get an abelian variety $\operatorname{Jac}(C)/K$ of dimension g, called the Jacobian of C.

If $K = \mathbb{C}$, then topologically X is a complex torus[25] (cf. §I of [Mum70]). Even when $K \neq \mathbb{C}$, an abelian variety has properties similar to those enjoyed by a complex torus; in particular, of all projective curves, only the curves of genus 1 can have an algebraic group law defined on them (cf. §III.6.3 in [Sha15]). Thus any abelian variety of dimension 1 has genus 1, that is, elliptic curves are the only abelian varieties of dimension 1. The following proposition justifies the prefix *abelian*.

Proposition 132. *Any abelian variety A/K is commutative.*

Proof. To prove this it is enough to show that the map $\varphi\colon A(\overline{K}) \times A(\overline{K}) \to A(\overline{K})$ sending $(x, y) \to xyx^{-1}y^{-1}$ is the constant map with image equal to the identity e. Clearly $\varphi(A \times \{e\}) = \varphi(\{e\} \times A) = \{e\}$. The claim then follows from the following quite general lemma. □

Lemma 133. *Let $\varphi\colon A \times B \to C$ be a morphism of varieties/K. Suppose A is proper and $\varphi(A \times \{b\}) = \varphi(\{a\} \times B) = \{c\}$ for some a, b, c. Then $\varphi(A \times B) = \{c\}$.*

This lemma follows from the Rigidity Lemma (Form I) as stated in [Mum70] on page 43.

13.2 Isogenies, Duals, and Polarizations

Definition 134. A K-isogeny $\varphi\colon X \to Y$ is a surjective morphism of complete group varieties over K with $\ker \varphi$ being finite. The degree of φ is defined to be $\deg(\varphi) = [K(X) : K(Y)]$ (here $K(X)$ becomes a finite algebraic extension of $K(Y)$ via the map $\varphi^\sharp : \mathcal{O}_Y \to \varphi_* \mathcal{O}_X$, since the generic point of X is mapped to the generic point of Y as φ is surjective).

[24] that is, there exists $n \geq 0$ and a closed immersion $X \hookrightarrow \mathbb{P}^n_K$.
[25] A familiar fact for elliptic curves over $\mathbb{C}$!

Example 135. The multiplication by n map, $[n] : A \to A$, $a \mapsto na$, is an isogeny for all $n \in \mathbb{Z} \setminus \{0\}$. This is a non-trivial claim and amounts to saying that A is a divisible group, and for all $n \geq 1$, $\ker([n])$ is finite. For details see *Application 2* on page 62 of [Mum70].

Proposition 136. $[n]^*\mathcal{L} \cong \mathcal{L}^{\otimes \frac{n^2+n}{2}} \otimes \left([-1]^*\mathcal{L}\right)^{\otimes \frac{n^2-n}{2}}$.

Proof. See Corollary 3 on page 59 of [Mum70]. □

Proposition 137. $\deg([n]) = n^{2g}$.

Proof. In characteristic zero we can reduce to the complex case, in that case $A(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ and so $A(\mathbb{C})[n] = \frac{1}{n}\Lambda/\Lambda \cong (\mathbb{Z}/2\mathbb{Z})^{2g}$, and the assertion follows. For the general case we fix $\mathcal{L}$, a symmetric (that is $[-1]^*\mathcal{L} = \mathcal{L}$) very ample line bundle on our abelian variety A. Let D be the corresponding Cartier divisor of $\mathcal{L}$, so that $\mathcal{L} = \mathcal{O}(D)$. As $\mathcal{L}$ is symmetric, proposition (136) shows that $[n]^*D = D^2$. The intersection product satisfies (cf. definition 23.70, proposition 23.77 in [GW23]) the following:

$$\begin{aligned}\deg[n](\underset{g\times}{D\cdots D}\cdot\mathcal{O}_A) = [n]^*(\underset{g\times}{D\cdots D}\cdot\mathcal{O}_A) = (\underset{g\times}{[n]^*D\cdots[n]^*D}\cdot\mathcal{O}_A)\\ = (\underset{g\times}{n^2D\cdots n^2D}\cdot\mathcal{O}_A) = n^{2g}(\underset{g\times}{D\cdots D}\cdot\mathcal{O}_A).\end{aligned}$$

Our ampleness assumption implies $(\underset{g\times}{D\cdots D}\cdot\mathcal{O}_A) \neq 0$ and we can conclude that $\deg[n] = n^{2g}$. □

Definition 138. A pair $(A^\vee, \mathcal{P})$ is said to be dual to A if $A^\vee$ is an abelian variety/K and $\mathcal{P}$ is a line bundle on $A \times A^\vee$ (called the Poincare line bundle) such that

1. $\mathcal{P}|_{A_b} \in \mathrm{Pic}^0(A_b)$, where $A_b := A \times b$, and $t_a^*\mathcal{P}|_{A_b} \cong \mathcal{P}|_{A_b}$ for all $a, b \in A$.
2. $\mathcal{P}|_{\{0\}\times A^\vee}$ is trivial.
3. the pair is universal with respect to the first two properties.

Remark 139. We should think of $A^\vee$ as parametrizing translation invariant line bundles of degree 0 on A (as is suggested by condition (1) in the definition above).

Mumford's construction. Let $\mathcal{L}$ be a line bundle on $A_{\overline{K}}$, then the map

$$\lambda_{\mathcal{L}} : A \to A^\vee,\ a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1},$$

defines an isogeny (to see that the line bundle defined above is translation invariant, one uses the Theorem of the square, see Corollary 4 on page 59 of [Mum70]).

Definition 140. A K-polarization on A is a K-isogeny $A \to A^\vee$ such that over $\overline{K}$, φ is of the form $\lambda_{\mathcal{L}}$ for some line bundle $\mathcal{L}$ on $A_{\overline{K}}$. The polarization is said to be principal if $\deg(\varphi) = 1$.

13.3 Weil Pairing

Fix $n \geq 1$. We are familiar with the Weil pairing for elliptic curves, we have a bilinear map

$$E[n] \times E[n] \to \mu_n,$$

satisfying some nice properties. More generally, for an abelian variety, we shall define a bilinear map

$$e_n : A[n] \times A^\vee[n] \to \mu_n,$$

satisfying similar properties (listed below, following the construction of this map). The pairing is defined as follows: let $a \in A[n]$ and $\mathcal{L} \in A^\vee[n]$ (we have that $\mathcal{L}^{\otimes n} \cong \mathcal{O}$). Since $\mathcal{L} \in \mathrm{Pic}^0(A)$, we see that $[-1]^*\mathcal{L} = \mathcal{L}^\vee$

and so by proposition (136) we find that $[n]^* = \mathcal{L}^{\otimes n}$. Thus we have an isomorphism $u : [n]^*\mathcal{L} \to \mathcal{O}$. Now for $a \in A[n]$, we consider the map

$$t_a^* u : t_a^*[n]^*\mathcal{L} \to t_a^*\mathcal{O} \cong \mathcal{O}.$$

As a is n-torsion we see that $t_a^*[n]^* = ([n] \circ t_a)^* = [n]^*$. Thus $t_a^* u$ is another isomorphism between $[n]^*\mathcal{L}$ and $\mathcal{O}$! This shows that $(t_a^* u)^{-1} u$ is an automorphism on $\mathcal{O}$. Since A is a complete variety, this automorphism is just multiplication by some scalar $\zeta \in \overline{K}^\times$. We can check that for each $m \geq 1$, $(t_{ma}^* u)^{-1} u$ is the multiplication by ζ^m. Since $na = 0$, it follows that $\zeta \in \mu_n$. We define $e_n(a, \mathcal{L})$ to be this number ζ.

Using this we now define a pairing $A[n] \times A[n] \to \mu_n$. Suppose (A, λ) is a polarized abelian variety, then we define

$$e_n^\lambda : A[n] \times A[n] \to \mu_n,\ e_n^\lambda(P, Q) := e_n(P, \lambda(Q)).$$

The following properties are satisfied by the pairings defined above.

1. e_n is a perfect pairing.
2. e_n is Galois equivariant, that is, $\sigma(e_n(P, Q)) = e_n(\sigma(P), \sigma(Q))$ for all $\sigma \in G_K = \mathrm{Gal}(\overline{K}/K)$, $P \in A[n]$ and $Q \in A^\vee[n]$.
3. $e_{mn}(P, Q)^m = e_n(mP, mQ)$.
4. If $\varphi : A \to B$, $\varphi^\vee : B^\vee \to A^\vee$, then $e_n(P, \varphi^\vee(Q)) = e_n(\varphi(P), Q)$ for all $P \in A[n]$, $Q \in B^\vee[n]$.
5. e_n^λ is skew-symmetric.
6. e_n^λ is perfect if $(\deg(\lambda), n) = 1$.

13.4 Galois representations

Let $\sigma \in G_K = \mathrm{Gal}(\overline{K}/K)$ and $P \in A$, then $\sigma([n]P) = [n]\sigma(P)$, and so G_K acts on $A[n]$. We therefore get a representation

$$\rho_n : G_K \to \mathrm{Aut}_{\mathbb{Z}/n\mathbb{Z}}(A[n]).$$

If $(\mathrm{char}(k), n) = 1$, then we have that $\mathrm{Aut}_{\mathbb{Z}/n\mathbb{Z}}(A[n]) \cong \mathrm{GL}(2g, \mathbb{Z}/n\mathbb{Z})$. We fix ℓ co-prime to $\mathrm{char}(k)$. On taking inverse limit over the representations $\{\rho_{\ell^n}\}_{n \geq 0}$, we get the ℓ-adic representation

$$\rho_{\ell^\infty} : G_K \to \mathrm{GL}(2g, \mathbb{Z}_\ell).$$

As the Weil pairing we constructed was Galois equivariant, we can in fact say something more about the image of ρ_{ℓ^∞}.

Let V be a free module of finite rank over a ring R with $\langle \cdot, \cdot \rangle$ an alternating perfect pairing. Then we define

$$\mathrm{GSp}(V, \langle \cdot, \cdot \rangle) := \{M \in \mathrm{GL}(V) \mid \langle Mv, Mw \rangle = \chi_{\mathrm{sim}}(M)\langle v, w \rangle \ \forall\ v, w \in V\},$$

where $\chi_{\mathrm{sim}} : \mathrm{GSp}(V, \langle \cdot, \cdot \rangle) \to R^\times$ is the similitude character.

Now we fix a symplectic basis $\langle P_1, \ldots, P_g, Q_1, \ldots, Q_g \rangle$ of $A[n]$ with respect to e_n^λ, such that for some $\zeta \in \mu_n$ we have

$$e_n^\lambda(P_i, Q_j) = \begin{cases} \zeta & \text{if } i = j \\ 1 & \text{if } i \neq j. \end{cases}$$
$$e_n^\lambda(P_i, P_j) = e_n^\lambda(Q_i, Q_j) = 1.$$

Then $\rho_n \colon G_K \to \mathrm{GSp}(2g, \mathbb{Z}/n\mathbb{Z}) \coloneqq \{M \in \mathrm{GL}(2g, \mathbb{Z}/n\mathbb{Z}) \mid M^t J M = \chi_{\mathrm{sim}}(M) J\}$, where

$$J = \begin{bmatrix} 0 & \mathrm{Id}_g \\ -\mathrm{Id}_g & 0 \end{bmatrix}.$$

Now if we fix a compatible collection of ℓ-power roots of unity $(\zeta_{\ell^m})_{m \geq 1}$ and a symplectic basis of $T_\ell(A)$, then we see that

$$\rho_{\ell^\infty} : G_K \to \mathrm{GSp}(2g, \mathbb{Z}_{2\ell}).$$

The Galois group acts on μ_{ℓ^∞} by the ℓ-adic cyclotomic character $\chi_\ell : G_K \to \mathbb{Z}_\ell^\times$, that is, for $\sigma \in G_K$, $\sigma(\zeta) = \zeta^{\chi_\ell(\sigma)}$. By equivariance we find that

$$\chi_{\mathrm{sim}} \circ \rho_{\ell^\infty} = \chi_\ell.$$

Example 141. Let $K = \mathbb{F}_q$, and suppose $\mathrm{char}(\mathbb{F}_q) = p \neq \ell$. Then $\chi_\ell(\mathrm{Frob}_q) = q$ and $\rho_{\ell^\infty}(\mathrm{Frob}_q)$ lies in some coset of $\mathrm{Sp}(2g, \mathbb{Z}_\ell)$ inside $\mathrm{GSp}(2g, \mathbb{Z}_\ell)$ with similitude q.

14 The Number Field–Function Field Analogy, lecture 4. Speaker: Jiuya Wang. Notes by John Yin.

14.1 Number field and function field analogies

We have the following "dictionary" for number fields and function fields.

number fields	**function fields**
$\mathbb{Q}$	$\mathbb{F}_q(t)$
$\mathbb{Z}$	$\mathbb{F}_q[t]$
prime numbers	irreducible monic polynomials
infinite place	prime ideal $(1/t) \subseteq \mathbb{F}_q[1/t]$
$\mathrm{Disc}(K)$	$\approx q^{2g-2}$

Here g is the genus of the curve associated to K (recall that every function field has an associated curve, i.e. a smooth projective irreducible variety of dimension 1). Malle's conjecture for function fields then ask for the asymptotics of the following as m tends to infinity:

$$E(G,m) \coloneqq \#\{K/\mathbb{F}_q(t) \mid \mathrm{Gal}(K/\mathbb{F}_q(t)) = G, \mathrm{Disc}(K) \leq q^m\}.$$

Although we cannot hope that $\lim_{m\to\infty} E(G,m)/q^m$ exists in general, we can talk about its upper and lower bounds. That is, for fixed a, b we may ask whether $E(G,m)$ is bounded above (or below) by $cm^b q^{ma}$ for some constant $c > 0$.

Klüners showed that the value Malle originally conjectured for b is not large enough for $G = C_3 \wr C_2$ over $\mathbb{Q}$, due to such extensions containing $\mathbb{Q}(\zeta_3)$. Ellenberg–Venkatesh showed that this should be the only problem in the function-field setting. In other words, by restricting to G-extensions over $\mathbb{F}_q(t)$ containing no constant extension (i.e. $\overline{\mathbb{F}_q}(t) \cap K = \mathbb{F}_q(t)$), then the conjectured b is correct. Their idea is this (assume $Z(G) = \{1\}$):

$$\begin{gathered} G\text{-extensions over } \mathbb{F}_q(t) \text{ with } \mathrm{Disc}(K) = q^m \\ \Longleftrightarrow \\ G\text{-covers of } \mathbb{P}_1/\mathbb{F}_q \text{ with degree of ramification } q^m \\ \Longleftrightarrow \\ \mathcal{H}_{G,m}(\mathbb{F}_q), \end{gathered}$$

where $\mathcal{H}_{G,m}$ is the Hurwitz variety for G-covers of $\mathbb{P}^1$ with m branch points.

Theorem 142 (Lang–Weil)**.** *If X is an irreducible variety over $\mathbb{F}_q$ of dimension m, then* $\lim_{q\to\infty} \#X(\mathbb{F}_q)/q^m = 1$.

Therefore, if we assume q is large enough, then understanding $\#X(\mathbb{F}_q)$ is reduced to understanding the number of connected components of X, and the constant a in Malle's conjecture is simply the dimension of $\mathcal{H}_{G,m}$. This is now a combinatorial question. Fortunately, $\mathcal{H}_{G,m}$ is naturally a finite étale cover of Conf_m, the configuration space of m points in $\mathbb{P}^1$. By Galois theory, the number of connected components equals the number of orbits for the action of the fundamental group of Conf_m acting on $\mathcal{H}_{G,m}$.

14.2 Combinatorial Question

Fix $c = \{c_1, \ldots, c_m\}$, a multiset of conjugacy classes in G (i.e. Nielson class), which records ramification behavior. We say c is $\mathbb{F}_q$*-rational* if $c_i^q = c_i$ for each i.

(*Aside:* Another way to describe this is to consider the character $\chi_{cyc}\colon \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to \mathrm{End}(G)$, defined by $\mathrm{Frob} \mapsto (x \mapsto x^q)$. In fact, this map may be precomposed with the canonical map $\mathrm{Gal}(\overline{\mathbb{F}_q(t)}/\mathbb{F}_q(t)) \to \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ to obtain a character of $\mathrm{Gal}(\overline{\mathbb{F}_q(t)}/\mathbb{F}_q(t))$.)

Now, for each $\mathbb{F}_q$-rational class c, we may consider the subvariety $\mathcal{H}_{c,m} \subseteq \mathcal{H}_{G,m}$ which will record the type of ramification at the m points (specifically, the conjugacy class of the monodromy element around the points of ramification).

Let $X \coloneqq \{(g_1, \dots, g_m) \mid g_i \in c_i, \prod_i g_i = 1, \langle g_1, \dots, g_m \rangle = G\}$. Then there is an action of the braid group Br_m, which is isomorphic to $\pi_1(\mathrm{Conf}_m(\mathbb{C}))$ on X. It is given by $\sigma_i((g_1, \dots, g_m)) = (g_1, \dots, g_i g_{i+1} g_i^{-1}, g_i, \dots, g_m)$. Now we may ask for the number of orbits $\#(X/\mathrm{Br}_m)$, which will turn out to be the number of connected components.[26]

Now, it is a fact that $\#(X/\mathrm{Br}_m)$ can be approximated with m is large enough. In fact, it is bounded as m tends to infinity. Since we don't care about the constant, when we look at the generating series for the number of extensions,

$$\sum_n \frac{\#\{\text{extensions of discriminant } n\}}{q^{ns}} \approx \sum_n \frac{\#\{\mathbb{F}_q\text{-rational classes } c\} \cdot q^n}{q^{ns}},$$

which is the Malle–Bhargava series. This means that it now suffices to get an upper or lower bound on the number of $\mathbb{F}_q$-rational Nielsen classes, which would give us the b-constant. This turns out to correspond exactly to the definition b-constant defined in the first lecture.

Türkelli computed the b-constant for certain G extensions which may contain larger field of constants. Even though his conjecture is not always true for number field, due to existence problems, we may still be inspired by his ideas.

EVW, Wood, and LZBW tell us how accurately we may carry out the calculation of $\#(X/\mathrm{Br}_m)$. Landesmann–Levy turn the above heuristic into a theorem.

14.3 Class group problem

Due to the connections between Malle's conjecture and the class group problem, our current understanding in the class group problem is also progressing.

Friedman–Washington: Given a function field, we may look at its Jacobian, which always acts linearly on the p^∞-torsion points. Thus, we may view the Frobenius element Frob as a matrix M in $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. Moreover, its determinant is always q by the existence of the Weil pairing. The heuristic is that Frob_q should be equidistributed among all elements with determinant q. If $q \equiv 1 \bmod \ell$, i.e. the ℓth root of unity are in the base field, then $M \bmod \ell$ actually lies in $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. In other words, $\mathrm{Coker}(\mathrm{Frob} - I)$ varies mod ℓ.

Achter: The above heuristic is a theorem.

[26] Here is an rough intuitive explanation. Given a branched cover of $\mathbb{P}^1(\mathbb{C})$, its deformations (in $\mathcal{H}_{G,m}(\mathbb{C})$) are uniquely determined by moving the branch points. (This is the intuitive meaning of the fact that $\mathcal{H}_{G,m}$ is a finite étale cover of Conf_m.) So if two covers are in the same connected component of $\mathcal{H}_{G,m}(\mathbb{C})$, one can go from the first to the second by moving around the branch points, and such a motion defines an element of the braid group. The monodromy data of the second cover is then determined from the monodromy data of the first via the braid-group action defined above.

15 Weil pairing definition of the Cassels–Tate pairing. Speaker: Ariel Weiss. Notes by Mehmet Basaran.

Let $E/\mathbb{Q}$ be an elliptic curve. There are two generalizations that we can make, but will not in this talk: We can take a general number field K instead of $\mathbb{Q}$ and we can take an abelian variety A instead of an elliptic curve E. In the first case most results in these notes still hold true, but in the second case we would have to be more careful.

Recall the definition of the Selmer group of E for an integer $n \geq 2$:

$$\mathrm{Sel}^n(E) = \ker\left(H^1\left(G_{\mathbb{Q}}, E[n]\right) \to \prod_v \frac{H^1\left(G_{\mathbb{Q}}, E[n]\right)}{\mathrm{im}E\left(\mathbb{Q}_v\right)}\right).$$

Theorem 143 (Mordell–Weil)**.**

$$E(\mathbb{Q}) \cong \mathbb{Z}^{\mathrm{rk}(E)} \oplus E(\mathbb{Q})_{\mathrm{tor}}$$

We want to understand the rank $\mathrm{rk}(E)$ of the elliptic curve E. For $n \geq 2$, we have the exact sequence

$$0 \longrightarrow \tfrac{E(\mathbb{Q})}{nE(\mathbb{Q})} \longrightarrow \mathrm{Sel}^n(E) \longrightarrow Ш(E)[n] \longrightarrow 0,$$

where $Ш(E)$ is the Tate–Shafarevich group of E. Therefore we get

$$\#E(\mathbb{Q})[n] \cdot n^{\mathrm{rk}(E)} = \#\frac{E(\mathbb{Q})}{nE(\mathbb{Q})} \leq \#\mathrm{Sel}^n(E),$$

and we have equality if and only if $Ш(E)[n]$ is trivial. This gives us a tool to bound the rank $\mathrm{rk}(E)$.

Conjecture. *The Tate–Shafarevich group* $Ш(E)$ *is finite.*

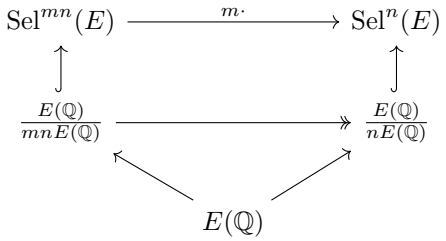
Corollary 144. *We can choose* n *such that* $Ш(E)[n] = 1$*.*

Corollary 145. *There is an integer* n *such that* $nШ(E) = 0$*.*

Idea: Let $m, n \geq 2$. Then the map

$$E[mn] \xrightarrow{m\cdot} E[n]$$

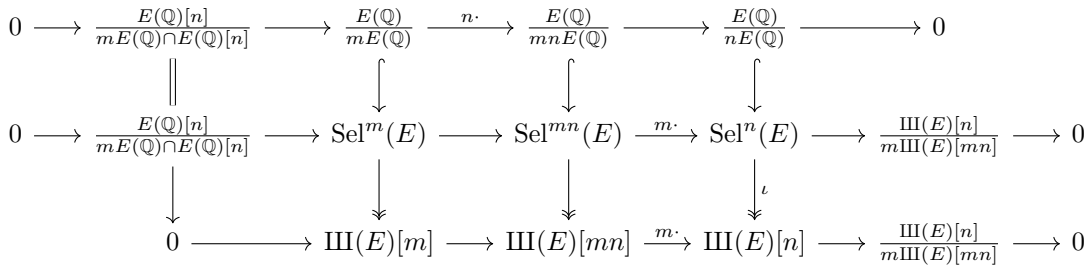
induces a map on Selmer groups and we get the diagram



Hence, the image $\mathrm{im}(E(\mathbb{Q}))$ of $E(\mathbb{Q})$ in $\mathrm{Sel}^n(E)$ is contained in $m\mathrm{Sel}^{mn}(E) \subset \mathrm{Sel}_n(E)$. We get a better bound if $m\mathrm{Sel}^{mn}(E) \subsetneq \mathrm{Sel}_n(E)$.

Question: Let $m, n \geq 2$. What is the image of $\mathrm{Sel}^{mn}(E) \xrightarrow{m\cdot} \mathrm{Sel}^n(E)$? More precisely, given $x \in \mathrm{Sel}^n(E)$, how can we detect if there is a $x_0 \in \mathrm{Sel}^m(E)$ with $x = mx_0$?

We can draw the diagram



From commutativity we can see that for $x \in \mathrm{Sel}^n(E)$ we have $x \in m\mathrm{Sel}^{mn}(E)$ if and only if $\iota(x) \in m Ш(E)$. So we can reformulate our question.
Question: Given $x \in Ш(E)$, how can we detect if $x \in mШ(E)$?

Theorem 146 ([Cas62b, Theorem 1.1])**.** *There exists an alternating bilinear pairing, called the Cassels–Tate pairing,*

$$\langle \cdot, \cdot \rangle_{\mathrm{CT}} : Ш(E) \times Ш(E) \to \mathbb{Q}/\mathbb{Z}$$

such that for all $x \in Ш(E)$

$$x \in mШ(E) \iff \langle x, y \rangle_{\mathrm{CT}} = 0 \text{ for all } y \in Ш(E)[m].$$

Corollary 147. *Let* $x \in \mathrm{Sel}^n(E)$*. Then*

$$x \in m\mathrm{Sel}^{mn}(E) \iff \langle \iota(x), \iota(y) \rangle_{\mathrm{CT}} = 0 \text{ for all } y \in \mathrm{Sel}^m(E).$$

Definition 148. Let $\alpha \colon V \times W \to \mathbb{Q}/\mathbb{Z}$ be a bilinear map. The left kernel and the right kernel of α are

$$\begin{aligned} \ker_L(\alpha) &\coloneqq \{v \in V \colon \langle v, w \rangle = 0 \text{ for all } w \in W\} \\ \ker_R(\alpha) &\coloneqq \{w \in W \colon \langle v, w \rangle = 0 \text{ for all } v \in V\}. \end{aligned}$$

The map α is called a perfect pairing, if both kernels are trivial.

Corollary 149. *Assume that* $Ш(E)$ *is finite. Then* $\langle \cdot, \cdot \rangle_{\mathrm{C}}$ *is a perfect pairing.*

Proof. Let $m = \#Ш(E)$, and take $x \in \ker_L(\langle \cdot, \cdot \rangle_{\mathrm{C}})$. Then $\langle x, y \rangle_{\mathrm{CT}} = 0$ for all $y \in Ш(E)$, and thus $x \in mШ(E) = 0$. So $\ker_L(\langle \cdot, \cdot \rangle_{\mathrm{C}})$ is trivial. Since the pairing is alternating, we have $\langle x, y \rangle_{\mathrm{CT}} = -\langle x, y \rangle_{\mathrm{CT}}$ and thus the right kernel $\ker_R(\langle \cdot, \cdot \rangle_{\mathrm{CT}})$ is trivial by the same reasoning. □

The Cassels–Tate pairing has the following properties:

(1) We can consider the restriction

$$\langle \cdot, \cdot \rangle_{\mathrm{CT}} : Ш(E)[n] \times Ш(E)[m] \to \mathbb{Q}/\mathbb{Z}$$

which has left kernel and right kernel

$$\begin{aligned} \ker_L(\langle \cdot, \cdot \rangle_{\mathrm{CT}}) &= \{x \in Ш(E)[n] \colon \langle x, y \rangle_{\mathrm{CT}} = 0 \text{ for all } y \in Ш(E)[m]\} \\ &= \{x \in Ш(E)[n] \colon x \in mШ(E)\} \\ &= mШ(E)[mn] \\ \ker_R(\langle \cdot, \cdot \rangle_{\mathrm{CT}}) &= nШ(E)[mn]. \end{aligned}$$

(2) We can extend to a pairing

$$\langle \cdot, \cdot \rangle_{\mathrm{CT}} : \mathrm{Sel}^n(E) \times \mathrm{Sel}^m(E) \to \mathbb{Q}/\mathbb{Z},$$

which has left kernel and right kernel

$$\begin{aligned} \ker_L(\langle \cdot, \cdot \rangle_{\mathrm{CT}}) &= m\mathrm{Sel}^{mn}(E) \\ \ker_R(\langle \cdot, \cdot \rangle_{\mathrm{CT}}) &= n\mathrm{Sel}^{mn}(E). \end{aligned}$$

Using this extension, we can go back to our original question.
Question: Given $x \in \mathrm{Sel}^n(E)$, when does there exist $x_0 \in \mathrm{Sel}^{mn}(E)$ with $x = mx_0$?
Answer: This happens if and only if $\langle x, y \rangle_{\mathrm{CT}} = 0$ for all $y \in \mathrm{Sel}_m(E)$.

15.1 The Tate Pairing

We define a pairing

$$(\cdot,\cdot)_p : H^1(\mathbb{Q}_p, E[m]) \times H^1(\mathbb{Q}_p, E[m]) \to \mathbb{Q}/\mathbb{Z}$$

as follows: To define $(\delta, \delta')_p$, we

1. first define $\lambda \in H^2\left(\mathbb{Q}_p, \overline{\mathbb{Q}}_p^{\times}\right)$ as
$$\lambda(\sigma,\tau) = e_m\left(\delta(\sigma), \sigma \cdot \delta'(\tau)\right),$$
where e_m is the Weil pairing, and then
2. use the fact
$$H^2\left(\mathbb{Q}_p, \overline{\mathbb{Q}}_p^{\times}\right) \simeq \mathbb{Q}/\mathbb{Z}.$$

This pairing enjoys the following properties:

(1) The group $\frac{E(\mathbb{Q}_p)}{mE(\mathbb{Q}_p)}$ is self-dual under the pairing, i.e.

$$\frac{E(\mathbb{Q}_p)}{mE(\mathbb{Q}_p)} = \left(\frac{E(\mathbb{Q}_p)}{mE(\mathbb{Q}_p)}\right)^{\perp}.$$

(2) (Part of) the Poitou-Tate sequence is

$$\begin{array}{ccccc} H^1(\mathbb{Q}, E[m]) & \longrightarrow & \prod_p' H^1(\mathbb{Q}_p, E[m]) & \longrightarrow & H^1(\mathbb{Q}, E[m])^* \\ & & (\xi_p)_p & \longmapsto & \sum_p (\xi_p, \mathrm{Res}_p(-))_p \end{array},$$

where $\prod'$ is the restricted product, where all but finitely many elements in any sequence are in the unramified cohomology $H^1(I_p, E[m])$.

Theorem 150. *Let $(\xi_p)_p \in \prod_p' H^1(\mathbb{Q}_p, E[m])$. There exists an element $\xi \in H^1(\mathbb{Q}, E[m])$ with*

$$\mathrm{Res}_p(\xi) = \xi_p \text{ in } \frac{H^1(\mathbb{Q}_p, E[m])}{\mathrm{im}\left(E(\mathbb{Q}_p)\right)} \text{ for all } p$$

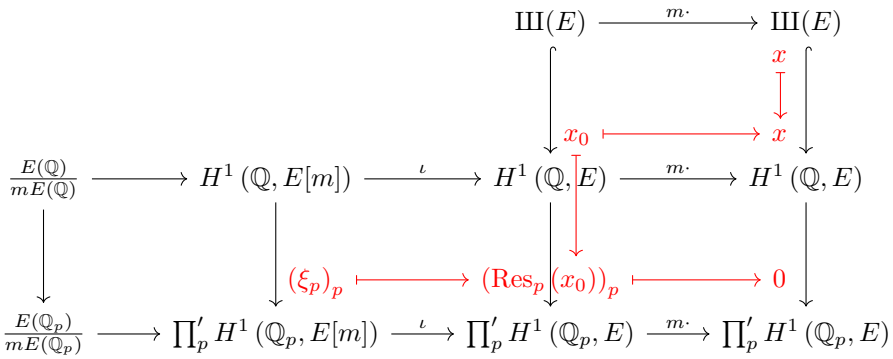
if and only if

$$\sum_p (\xi_p, \mathrm{Res}_p(y))_p = 0 \text{ for all } y \in \mathrm{Sel}^m(E).$$

15.2 Construction of the Cassels–Tate pairing

Let $x \in Ш(E) = \ker\left(H^1(\mathbb{Q}, E) \to \prod_p' H^1(\mathbb{Q}_p, E)\right)$. We recall an earlier question.
Question: When is $x \in mШ(E)$?

From now on we assume that there is a $x_0 \in H^1(\mathbb{Q}, E)$ such that $mx_0 = x$. This is true if m is prime, and in particular if $m = 2$. We have the diagram



With this diagram, we can reformulate our question to:
Question: Does there exist a $\xi \in H^1(\mathbb{Q}, E[m])$ such that $x_0 + \iota(\xi) \in Ш(E)$?

If we can find such a ξ, then for the element $x_1 \coloneqq x_0 + \iota(\xi) \in Ш(E)$ we have $mx_1 = x$. Starting on the top right, through the right vertical arrow we can consider x as an element in $H^1(\mathbb{Q}, E)$. Then by our assumption we have $x_0 \in H^1(\mathbb{Q}, E)$ such that $mx_0 = x$. Then the image of x_0 in $H^1(\mathbb{Q}_p, E)$ is $\mathrm{Res}_p(x_0)$, which maps to 0 when multiplied by m because of commutativity of the diagram. Therefore, by Theorem 150 we can find $(\xi_p) \in \prod'_p H^1(\mathbb{Q}_p, E[m])$ such that $\iota(\xi_p) = \mathrm{Res}_p(x_0)$. This leads to a new question.
Question: When does there exist an element $\xi \in H^1(\mathbb{Q}, E[m])$ such that for all p

$$\mathrm{Res}_p(\xi) = \xi_p \text{ in } \frac{H^1(\mathbb{Q}_p, E[m])}{\mathrm{im}(E(\mathbb{Q}_p))}?$$

Theorem 151. *Such a ξ exists (and thus x is divisible by m in $Ш(E)$) if and only if*

$$\sum_p (\xi_p, \mathrm{Res}_p(y))_p = 0$$

for all $y \in \mathrm{Sel}^m(E)$.

Definition 152. Let $x \in Ш(E)[n]$ and $y \in Ш(E)[m]$. Choose $\widetilde{y} \in \mathrm{Sel}^m(E)$ lifting y. We define the Cassels-Tate pairing by

$$\langle x, y \rangle_{\mathrm{CT}} = \sum_p (\xi_p, \mathrm{Res}_p(\widetilde{y}))_p .$$

Theorem 153. *This definition is independent of the choice of lift $\widetilde{y}$.*

Proof. Refer to [Cas62b, Section 3]. □

16 Getting at higher Selmer groups, lecture 4. Speaker: Alexander Smith. Notes by Mehmet Basaran.

16.1 4-Selmer Example

Let $E/\mathbb{Q}$ be an elliptic curve and assume that $E(\mathbb{Q})[2] = (\mathbb{Z}/2\mathbb{Z})^2$ as $G_{\mathbb{Q}}$-modules. Let V be the set of primes at which E has bad reduction together with the primes 2 and ∞. We also define A to be the product of all primes of bad reduction and the prime 2.

We take $X_1, \ldots, X_k$ disjoint finite sets of primes, $X = \prod X_i$, such that $X_i \cap V = \varnothing$ and we have the following assumptions.

(1) For all $a|A$, we have
$$\left(\frac{a}{p_i}\right) = \left(\frac{a}{p_i'}\right) \text{ for all } p_i, p_i' \in X_i.$$

(2) For all $i \neq j$, we have
$$\left(\frac{p_i}{p_j}\right) = \left(\frac{p_i'}{p_j'}\right) \text{ for all } p_i, p_i' \in X_i, p_j, p_j' \in X_j.$$

(3) For all $d \in X$, under the map $\mathrm{Sel}^2\left(E^d\right) \subset H^1\left(G_{\mathbb{Q}}, E^d[2]\right) \cong \mathbb{Q}^\times/\left(\mathbb{Q}^\times\right)^2 \times \mathbb{Q}^\times/\left(\mathbb{Q}^\times\right)^2$, the group
$$\frac{\mathrm{Sel}^2\left(E^d\right)}{\mathrm{img}\left(E_{\mathrm{tor}}\left(\mathbb{Q}\right)\right)}$$
is generated by $(p_1, 1)$ and $(1, p_2)$.

Statistical question: How does $\langle (p_1,1),(1,p_2)\rangle_{\mathrm{CT},d}$ vary, as $d = (p_1, \ldots, p_k)$ varies in X?
Guess: This is
$$\begin{cases} \frac{1}{2} & \text{for } \approx 50\% \text{ of } d \\ 0 & \text{for } \approx 50\% \text{ of } d. \end{cases}$$

This means
$$r_4\left(E^d\right) = \begin{cases} 0 & \text{for } \approx 50\% \text{ of } d \in X \\ 2 & \text{for } \approx 50\% \text{ of } d \in X. \end{cases}$$

Calculation: Compare the pairing for $d = (p_1, p_2, p_3)$ and $d = (p_1, p_2, p_3')$. Let $x \in H^1\left(G_{\mathbb{Q}}, E^d[2]\right) \cong H^1\left(G_{\mathbb{Q}}, E^{d'}[2]\right)$[27] associated to $(p_1, 1)$. Choose $x_0 \in H^1\left(G_{\mathbb{Q}}, E^d[4]\right)$ such that $2x_0 = x$. Assume that there is some $\gamma\colon G_{\mathbb{Q}} \to E[2]$ such that $d\gamma = \chi_{p_3p_3'} \cup x$ with $\chi_{p_3p_3'} \in Z^1\left(G_{\mathbb{Q}}, \{\pm 1\}\right)$ and $x \in H^1\left(G_{\mathbb{Q}}, E^d[2]\right)$. Here, $d\gamma(\sigma,\tau) \coloneqq \sigma\cdot\gamma(\tau) + \gamma(\sigma) - \gamma(\sigma\tau)$. Let $\beta_d\colon E^d \to E$ be an isogeny. Then $dx_0 = 0$ but $d\beta_d x_0 \neq 0$. If we take
$$x_0' = \beta_{d'}^{-1} \circ \beta_d\left(x_0\right) + \beta_{d'}^{-1}(\gamma),$$
then $dx_0' = 0$, i.e. $x_0' \in H^1\left(G_{\mathbb{Q}}, E^{d'}[4]\right)$, and also $2x_0' = x$. We have
$$\langle (p_1,1),(1,p_2)\rangle_d = \sum_p \left(\mathrm{Res}_p\left(x_0\right) - \xi_p, \mathrm{Res}_p(y)\right)_p$$
and
$$\langle (p_1,1),(1,p_2)\rangle_{d'} = \sum_p \left(\mathrm{Res}_p\left(x_0'\right) - \xi_p, \mathrm{Res}_p(y)\right)_p.$$

[27] This is true since $E^d[2] \cong E^{d'}[2]$ as $G_{\mathbb{Q}}$-modules.

They match up at all primes but p_2, since we have ramification at p_2. Thus, the difference of these two pairings is

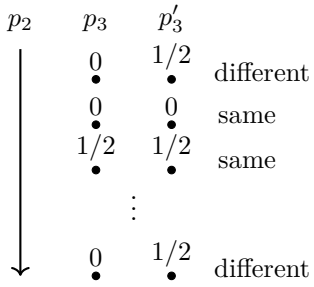
$$\mathrm{inv}_{p_2}\left(\mathrm{Res}_{p_2}(\gamma) \cup \mathrm{Res}_{p_2}(y)\right),$$

which is determined by $\gamma(\mathrm{Frob}_{p_2})$. If X_2 is large enough so that Chebotarev density holds, then this expression is

$$\begin{cases} \frac{1}{2} & \text{for 50\% of } p_2 \\ 0 & \text{for 50\% of } p_2. \end{cases}$$

Corollary 154. *In $\{p_1\} \times X_2 \times \{p_3, p_3'\}$, the 4-Selmer rank is 0 for a proportion between 25% and 75%.*

Proof. We look at the different possibilities of the above expression that can happen with p_3 and p_3'. We get the image



The 4-Selmer rank is zero if both columns have a 0 in the same row, which happens with a proportion between 25% and 75%. □

We can also look at

$$\{p_1\} \times X_2 \times \{p_3, p_3', p_3'', p_3''', p_3''''\}$$

and the same argument gives a proportion between 30% and 70%.

16.2 History

16.2.1 2-Selmer groups

Gerth ([Ger84], 1984): Found the distribution of $2\#\mathrm{Cl}\left(\mathbb{Q}\left[\sqrt{-d}\right]\right)[4]$ in grids of d satisfying assumption (2).
Heath-Brown ([HB94], 1994): Computed $\mathrm{Sel}^2\left(y^2 = x^3 - d^2x\right)$ as d varies.
Swinnerton-Dyer ([SD08], 2008): Studied $\mathrm{Sel}^2\left(E^d\right)$ for $E(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$ for grids.
Fouvry-Klüners ([FK11], 2011): Studied $2\#\mathrm{Cl}\left(\mathbb{Q}\left[\sqrt{-d}\right]\right)[4]$.
Klagsbrun-Mazur-Rubin ([KMR13], 2013): Removed the torsion assumption for grids.
Kane ([Kan13], 2013): Inspected the distribution of $\mathrm{Sel}^2\left(E^d\right)$ satisfying $E(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$ for natural families of d.

16.2.2 4-Selmer groups

Theorem 155 (Redei, Stevenhagen, [Ste22])**.** *Given any $0 \neq d \in \mathbb{Z}$ one can find a Galois extension $L/\mathbb{Q}$ such that for any prime $p \nmid 2d$ we can determine $\mathrm{Cl}\left(\mathbb{Q}\left(\sqrt{dp}\right)\right)[8]$ from $\mathrm{Frob}_p \subset \mathrm{Gal}(L/\mathbb{Q})$.*

We then similarly have such an L for $\mathrm{Sel}^2\left(E^{dp}\right)$ by the same Cassels-Tate argument by Hemmenway.

16.3 A Hint of 8-Selmer groups

Let $k = 3$ and $d \in \{p_1, p_1'\} \times \{p_2, p_2'\} \times \{p_3, p_3'\}$. We write

$$d_\varnothing = p_1p_2p_3,\ d_1 = p_1'p_2p_3,\ d_{12} = p_1'p_2'p_3, \ldots.$$

Proposition 156. *Suppose we can choose a lift $x_S \in \mathrm{Sel}^4\left(E^{d_S}\right)$ of x for all $S \subset \{1,2,3\}$ except for $S = \{1,2,3\}$. Suppose further that*

$$\begin{aligned} 0 &= \beta_\varnothing x_\varnothing + \beta_1 x_1 + \beta_2 x_2 + \beta_{12} x_{12} \\ 0 &= \beta_\varnothing x_\varnothing + \beta_1 x_1 + \beta_3 x_3 + \beta_{13} x_{13} \\ 0 &= \beta_\varnothing x_\varnothing + \beta_2 x_2 + \beta_3 x_3 + \beta_{23} x_{23}. \end{aligned}$$

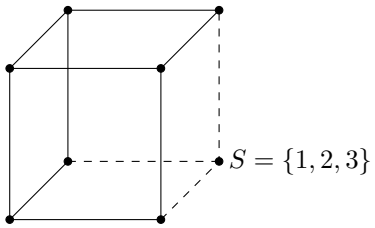
Then:

(i) The element

$$x_{123} = \sum_{S \subsetneq \{1,2,3\}} \beta_{123}^{-1} \circ \beta_S x_S \in \mathrm{Sel}^4 E^{d_{123}},$$

lifts x.

(ii) We can write $\sum_S \langle x_S, y\rangle_{d_S}$ as something controllable using the Chebotarev density theorem. We can draw a cube where each vertex corresponds to some $S \subset \{1,2,3\}$. For seven vertices we have a cocycle such that their sums on each face is equal to zero. The theorem says that we can find a cocycle for the remaining eighth vertex.



Question: How does $\mathrm{Cl}\left(K\left[2^\infty\right]\right)$ behave in the set of quadratic extensions of $\mathbb{Q}(i)$?

References

[Alb24] Brandon Alberts, Explicit analytic continuation of Euler products, arXiv preprint 2406.18190 (2024). 10

[BKL+15] Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra, Jr., Bjorn Poonen, and Eric Rains, Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves, Camb. J. Math. **3** (2015), no. 3, 275–321. MR 3393023 19

[Cas62a] J. W. S. Cassels, Arithmetic on curves of genus 1. III. The Tate-šafarevič and Selmer groups, Proc. London Math. Soc. (3) **12** (1962), 259–296. MR 163913 18

[Cas62b] J.W.S. Cassels, Arithmetic on curves of genus 1. iv. proof of the hauptvermutung., Journal für die reine und angewandte Mathematik **211** (1962), 95–112. 58, 60

[Del01] Christophe Delaunay, Heuristics on Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$, Experiment. Math. **10** (2001), no. 2, 191–196. MR 1837670 19

[FK11] Étienne Fouvry and Jürgen Klüners, Weighted distribution of the 4-rank of class groups and applications, Int. Math. Res. Not. IMRN (2011), no. 16, 3618–3656. MR 2824840 62

[Ger84] Frank Gerth, III, The 4-class ranks of quadratic fields, Invent. Math. **77** (1984), no. 3, 489–515. MR 759260 62

[Gol79] Dorian Goldfeld, Conjectures on elliptic curves over quadratic fields, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), Lecture Notes in Math., vol. 751, Springer, Berlin, 1979, pp. 108–118. MR 564926 17

[GW23] Ulrich Görtz and Torsten Wedhorn, Algebraic geometry ii: Cohomology of schemes, Springer Studium Mathematik, Springer Spektrum Wiesbaden, 2023. 52

[HB94] D.R. Heath-Brown, The size of selmer groups for the congruent number problem, ii., Inventiones mathematicae **118** (1994), no. 2, 331–370. 62

[Hua82] Loo Keng Hua, Introduction to number theory, Springer-Verlag, Berlin-New York, 1982, Translated from the Chinese by Peter Shiu. MR 665428 5

[Jut75] Matti Jutila, On mean values of dirichlet polynomials with real characters, Acta Arithmetica **27** (1975), no. 1, 191–198. 34

[Kan13] Daniel Kane, On the ranks of the 2-selmer groups of twists of a given elliptic curve, Algebra & Number Theory **7** (2013), no. 5, 1253–1279. 62

[KMR13] Zev Klagsbrun, Barry Mazur, and Karl Rubin, Disparity in selmer ranks of quadratic twists of elliptic curves, Annals of Mathematics **178** (2013), no. 1, 287–320. 62

[KS24] Peter Koymans and Alexander Smith, Sums of rational cubes and the 3-selmer group, 2024. 20

[KW22] Jürgen Klüners and Jiuya Wang, ℓ-torsion bounds for the class group of number fields with an ℓ-group as Galois group, Proc. Amer. Math. Soc. **150** (2022), no. 7, 2793–2805. MR 4428868 24

[Mil20a] James S. Milne, Algebraic number theory (v3.08), 2020, Available at www.jmilne.org/math/, p. 166. 27

[Mil20b] J.S. Milne, Class field theory (v4.03), 2020, Available at www.jmilne.org/math/, pp. 287+viii. 28, 29, 45

[MS22] Adam Morgan and Alexander Smith, The cassels-tate pairing for finite galois modules, 2022. 45

[MS24] Adam Morgan and Alexander Smith, Field change for the Cassels–Tate pairing and applications to class groups, Research in Number Theory **10** (2024), no. 3, 61 (en). 45

[Mum70] David Mumford, Abelian varieties, Tata Institute of Fundamental Research Studies in Mathematics, Oxford University Press, 1970. 51, 52

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, Cohomology of number fields, Grundlehren der mathematischen Wissenschaften, Springer Berlin, Heidelberg, 2008. 31

[PTBZ25] Lillian B. Pierce, Caroline L. Turnage-Butterbaugh, and Asif Zaman, A guide to tauberian theorems for arithmetic applications, 2025. 4

[Rob96] Derek J. S. Robinson, A course in the theory of groups, Graduate Texts in Mathematics, Springer New York, NY, 1996. 21, 23

[SD08] Peter Swinnerton-Dyer, The effect of twisting on the 2-Selmer group, Math. Proc. Cambridge Philos. Soc. **145** (2008), no. 3, 513–526. MR 2464773 62

[Sha15] Igor R. Shafarevich, Basic algebraic geometry 1, Springer Berlin, Heidelberg, 2015. 51

[Sil09] Joseph H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, Springer New York, NY, 2009. 51

[Smi17] Alexander Smith, 2^∞-selmer groups, 2^∞-class groups, and goldfeld's conjecture, 2017. 45

[Smi22a] ———, The distribution of ℓ^∞-selmer groups in degree ℓ twist families ii, 2022. 45

[Smi22b] ———, The distribution of ℓ^∞-selmer groups in degree ℓ twist families i, 2022. 19, 45, 50

[Smi25] ———, The birch and swinnerton-dyer conjecture implies goldfeld's conjecture, 2025. 17, 18

[Ste22] Peter Stevenhagen, Redei reciprocity, governing fields and negative Pell, Math. Proc. Cambridge Philos. Soc. **172** (2022), no. 3, 627–654. MR 4416572 62

[SU14] Christopher Skinner and Eric Urban, The Iwasawa main conjectures for GL_2, Invent. Math. **195** (2014), no. 1, 1–277. MR 3148103 18

[Wri89] David J. Wright, Distribution of discriminants of abelian extensions, Proc. London Math. Soc. (3) **58** (1989), no. 1, 17–50. MR 969545 9