Langlands Corespondence and Bezrukavnikov's Equivalence

Anna Romanov

June 4, 2019

This document contains notes from Geordie Williamson's course at the University of Sydney in the first term of 2019. For course details (and lecture notes that were actually written by Geordie), see the course webpage:

`http://www.maths.sydney.edu.au/u/geordie/LanglandsAndBezrukavnikov/`

The primary goal of these lectures to give an informal introduction to what the Langlands program is about, from an arithmetical point of view. We assume the audience (like the lecturer) is a beginner in this subject, but had a first course in complex analysis, Galois theory, topology and representation theory. At times we also assume background in algebraic geometry. Not much is proved, but we try to give enough detail to convince the reader that there is a lot of marvellous mathematics here. We assume that the reader is willing to take some things on faith, and have tried to be honest. Audience members were encouraged to do exercises throughout, and this wouldn't be bad advice for any potential reader either. At the end of the lectures, the reader will find a list of sources from which most of this material was drawn, and which the reader is encouraged to consult.

1 Lecture 1 (March 8, 2019): Reciprocity Laws

If you do nothing else with this course this semester beyond attending the first lecture, you should at least try to read [Lan90].

1.1 Reciprocity Laws

We start at the natural starting place: an equation. Consider the equation

$$x^2 + 1 = 0.$$

If p is a prime, one might wonder: how many solutions does this equation have, modulo p? Some calculations will reveal the following table.

p	2	3	5	7	11	13	17	19	23	
# of sol's mod p	1	0	2	0	0	2	2	0	0	...
p mod 4	2	3	1	3	3	1	1	3	3	

We see a pattern. The prime 2 is weird, so we ignore it. But for the rest, it seems that

$$\#\text{ of solutions mod } p \neq 2 = \begin{cases} 2 & \text{if } p = 1 \mod 4 \\ 0 & \text{if } p = 3 \mod 4 \end{cases}.$$

This pattern is surprising. It appears to be saying that there is a global rule governing the number of solutions mod p; that is, that the different primes somehow "talk to one another."

Here we can give a simple proof of why our claim above must be true. Assume $p \neq 2$. We have a short exact sequence

$$1 \to (\mathbb{F}_p^\times)^2 \to \mathbb{F}_p^\times \to \{\pm 1\} \to 1,$$

where the third arrow is given by $x \mapsto x^{\frac{p-1}{2}}$. Therefore,

$$-1 \text{ is a square mod } p \iff (-1)^{\frac{p-1}{2}} = 1 \iff \frac{p-1}{2} \text{ is even} \iff p = 1 \mod 4.$$

Let's do another example. Consider the equation

$$x^2 - 3 = 0.$$

We ask the same question and compute:

p	2	3	5	7	11	13	17	19	23	29	31	
# of sol's mod p	1	1	0	0	2	2	0	0	2	0	0	...
p mod 12	2	3	5	7	11	1	5	7	11	5	7	

Again, we have some small weird primes (2 and 3), so we throw them out. For the rest, we make a guess:

$$\#\text{ of solutions mod } p \neq 2,3 = \begin{cases} 2 & \text{if } p = 1, 11 \mod 12 \\ 0 & \text{if } p = 5, 7 \mod 12 \end{cases}.$$

To prove that this is indeed the case, we introduce a little more technology. Let $p \neq 2$ be a prime. Define

$$\epsilon(p) = \begin{cases} 0 & \text{if } p = 1 \mod 4 \\ 1 & \text{if } p = 3 \mod 4 \end{cases},$$

and the Legendre symbol

$$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \mod p = \begin{cases} 1 & \text{if } x \text{ is a square mod } p \\ -1 & \text{if } x \text{ is not a square mod } p \end{cases}.$$

(For example, we saw above that $\left(\frac{-1}{p}\right) = (-1)^{\epsilon(p)}$.)

Theorem 1.1. (**Gauss's Law**) Let p, q be distinct primes $\neq 2$. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\epsilon(p)\epsilon(q)}.$$

With this we can prove that our guess was correct. Assume $p \neq 2, 3$. Then

$$\begin{aligned} x^2 - 3 \text{ has 2 solutions mod } p &\iff \left(\frac{3}{p}\right) = 1 \\ &\iff \left(\frac{p}{3}\right)(-1)^{\epsilon(p)\epsilon(3)} = 1 \\ &\iff \left(\frac{p}{3}\right)(-1)^{\epsilon(p)} = 1 \\ &\iff \begin{cases} p = 1 \mod 3 \text{ and } p = 1 \mod 4 \\ p = 2 \mod 3 \text{ and } p = 3 \mod 4 \end{cases} \\ &\iff p = 1 \text{ or } -1 \mod 12. \end{aligned}$$

These are examples of **reciprocity laws**. All polynomials of degree 2 can be worked out analogously to the ones above using quadratic reciprocity (Gauss's law). There was much activity on this problem starting with Gauss's work, which finally led to Artin's reciprocity law. This implied all known reciprocity laws at the time, and in particular treats polynomials of degree 3 and 4. However, we get stuck at 5. For example, consider

$$x^5 + 20x + 16 = 0.$$

We can construct a table

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
# of sol's mod p	1	0	1	2	2	0	2	0	1	2	0	1	2	2	0	0

...

but no obvious pattern emerges. (For a table that goes much further than this one, see the sheet on the course website.) It turns out that there is a pattern, but it is very well-hidden, and to find it, we need analysis.

1.2 Higher dimensional varieties

We could ask similar questions for polynomials in two variables. Consider the equation

$$y^2 = x^3 + 1.$$

How many solutions does this equation have modulo p? Let's try to answer this for one specific prime. Let p=5, and we can compile our results in the following table:

$y\backslash x$	0	1	2	3	4
0	×	×	×	×	✓
1	✓	×	×	×	×
2	×	×	✓	×	×
3	×	×	✓	×	×
4	✓	×	×	×	×

So here we found that there are five solutions modulo 5. In general, how many solutions do we expect? Well, the map $x \mapsto x^3 + 1$ in $\mathbb{F}_p$ is "roughly random," about half the elements of $\mathbb{F}_p$ are squares, and for every square we get two solutions, so we expect *approximately p solutions.* But how often is this actually the case? We can measure the accuracy of this estimation by studying the **Sato-Tate error term**:

$$ST(p) = p - \#(\text{solutions modulo } p).$$

Here is another table.

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
# ST(p)	0	0	0	-4	0	2	0	8	0	0	-4	-10	0	8	0	0

...

Notice how frequently the Sato-Tate error term is zero! We can now study this table and see if any patterns emerge. This is the content of the **Sato-Tate conjecture**, which is basically known thanks to recent work of Harris, Taylor, Clozel, and many others.

1.3 What is going on here? What does this have to do with representation theory?

Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial with integral coefficients. We can consider the **splitting field** of f:

$$K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n),$$

and the associated **Galois group**

$$\Gamma = \mathrm{Gal}(K/\mathbb{Q}),$$

which acts on the set of roots $\{\alpha_1, \ldots \alpha_n\}$. As representation theorists, our natural instinct when we see a group action is to linearize. Doing this here results in the **permutation representation**

$$\Gamma \circlearrowright H = \bigoplus_{i=1}^{n} \mathbb{C}\alpha_i.$$

We can also consider the reduction of f modulo p, $\bar{f}(x) \in \mathbb{F}_p[x]$, as we did in the previous section. In general, $\bar{f}$ will be reducible. If $p \nmid \Delta(f)$ (that is, p is not one of the "weird" primes we encountered earlier), then $\bar{f}(x)$ has n roots, $\overline{\alpha}_1, \ldots, \overline{\alpha}_n \in \mathbb{F}_{p^n}$. Recall that the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z}$ is generated by the Frobenius map

$$\overline{\mathrm{Frob}}_{\mathrm{p}} : x \mapsto x^p.$$

Then $\mathbb{F}_p = (\mathbb{F}_{p^n})^{\overline{\mathrm{Frob}}_{\mathrm{p}}}$, and the number of solutions of $\bar{f}$ is the number of fixed points of $\overline{\mathrm{Frob}}_{\mathrm{p}}$ on $\{\overline{\alpha}_1, \ldots, \overline{\alpha}_n\}$. For such a p ("unramified") and after a choice ("prime in $\mathbb{O}$ above p"), we get a bijection

$$\{\alpha_1, \ldots, \alpha_n\} \longrightarrow \{\overline{\alpha}_1, \ldots \overline{\alpha}_n\},$$

and an element $\mathrm{Frob}_{\mathrm{p}} \in \Gamma$ such that the action of $\mathrm{Frob}_{\mathrm{p}}$ on $\{\alpha_1, \ldots, \alpha_n\}$ aligns with the action of $\overline{\mathrm{Frob}}_{\mathrm{p}}$ on $\{\overline{\alpha}_1, \ldots, \overline{\alpha}_n\}$ under the bijection above.

Remark 1.2. Different choices of "prime in $\mathbb{O}$ over p" result in conjugate $\mathrm{Frob}_{\mathrm{p}}$'s. Hence, it is best to think of $\mathrm{Frob}_{\mathrm{p}}$ as a conjugacy class instead of an individual element.

The upshot of the discussion above is that

$$\begin{aligned} \#\text{ solutions modulo p } &= \#\text{ fixed points of } \overline{\mathrm{Frob}}_{\mathrm{p}} \text{ on } \{\overline{\alpha}_1, \ldots, \overline{\alpha}_n\} \\ &= \#\text{ of fixed points of } \mathrm{Frob}_{\mathrm{p}} \text{ on } \{\alpha_1 \ldots, \alpha_n\} \\ &= \mathrm{Tr}(\mathrm{Frob}_{\mathrm{p}}, H), \end{aligned}$$

where H is the permutation representation introduced at the beginning of this section. The number $\mathrm{Tr}(\mathrm{Frob}_{\mathrm{p}}, H)$ is completely canonical - it doesn't depend on any of our choices! So we've reduced our question of finding solutions of polynomials modulo p to computing something that looks very much like the character of a representation.

The Punchline: If $p \nmid \Delta(f)$,

$$\#\text{ solutions of } f \text{ mod p } = \mathrm{Tr}(\mathrm{Frob}_{\mathrm{p}}, H).$$

1.4 Schematic picture of the Langlands correspondence

DO NOT WORRY IF THIS MAKES NO SENSE. A caricature of the Langlands correspondence is captured in the diagram below.

$$\begin{tikzcd}
\text{"geometric" reps } V \text{ of } \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[r] & \text{"character" } \mathrm{Tr}(\mathrm{Frob}_{\mathrm{p}}, V) \arrow[d] & \text{automorphic forms} \arrow[dl] \\
& L\text{-functions (analytic)} &
\end{tikzcd}$$

From any "geometric" representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we can take the trace of Frobenius, as we did in the previous section for the permutation representation H. We should think of this procedure as taking the character of the representation. To $\mathrm{Tr}(\mathrm{Frob}_{\mathrm{p}}, V)$, we can attach the associated "L-function," which is an analytic object. (For example, when we start with the trivial representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the resulting L-function is the Riemann ζ-function.) On the other hand, there is also a procedure for constructing L-functions from automorphic forms. The Langlands correspondence is an attempt to align these two sources of L-functions.

This is very deep. For example, two-dimensional representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ result in Hecke L-functions, and the corresponding automorphic forms are modular forms. It turns out that working out the correspondence for 2-dimensional representations is enough to prove Fermat's last theorem.

1.5 Chebotarev density theorem

If we talk of $\mathrm{Tr}(\mathrm{Frob_p}, H)$ as a "character," we would like to know at least that the set $\{\mathrm{Frob_p}\}$ for all p unramified cover the set of all conjugacy classes of Γ. This is a deep theorem.

Theorem 1.3. (Chebotarev density theorem) Fix a conjugacy class $C \subset \Gamma$. Then

$$\{p \text{ unramified} \mid \mathrm{Frob_p} = C\}$$

has density $|C|/|\Gamma|$.

Here density refers to either the natural density or the analytic density of the set of primes.

Example 1.4. Let $f(x) = x^2 + 1 \in \mathbb{Z}[x]$. The set of roots of $f(x)$ is $\{i, -i\}$. The splitting field is $K = \mathbb{Q}(i)$ and $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} = \{id, s\}$. In this example, all $p \neq 2$ are unramified. Then for such an unramified p,

$$\mathrm{Frob_p} : i \mapsto i^p.$$

Hence,

$$\mathrm{Frob_p} = \begin{cases} id & \text{if } p = 1 \mod 4 \\ s & \text{if } p = 3 \mod 4 \end{cases}.$$

Exercise 1.5. (Mandatory) Check that $\mathrm{Frob_p}$ is indeed given as above!

Exercise 1.6. (Harder) By considering cyclotomic extensions (i.e. $\mathbb{Q}(e^{2\pi i/m})$), show that Chebotarev's density theorem implies Dirichlet's theorem on primes in arithmetic progression.

At the beginning of today's lecture, we discussed patterns in the number of solutions of a given polynomial modulo p. There is a sheet on the course webpage which shows tables of these patterns for the polynomials $x^2+1, x^2-3, x^2+x+1, x^2+2x+3$, and x^2-x-1. A somewhat mysterious feature of these tables was the modulus appearing in the patterns. (For example, we showed that $x^2 - 3$ has two solutions modulo $p \neq 2, 3$ if and only if $p = 1$ or $11 \mod 12$. Where did 12 come from?) We'll complete today's lecture with an example to demonstrate where this modulus comes from.

Example 1.7. Consider the polynomial $f(x) = x^2 - x - 1$. We can see from the patterns on the handout that $f(x)$ has 2 solutions mod p if $p = 1$ or $9 \mod 10$ and $f(x)$ has 0 solutions mod p if $p = 3$ or $7 \mod 10$ (for p unramified). In this example, the splitting field is $K = \mathbb{Q}(\phi)$, where $\phi = \frac{1+\sqrt{5}}{2} = 2\cos(\pi/5)$ is the golden ratio, and $\mathrm{Gal}(\mathbb{Q}(\phi)/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} = \langle s \rangle$. Note that $\phi = \zeta + \overline{\zeta}$, where $\zeta = e^{\pi i/5}$ is a fifth root of unity. Hence we can embed

$$K \hookrightarrow \mathbb{Q}(e^{2\pi i/10}) = \mathbb{Q}(\zeta)$$

via $\phi \mapsto \zeta + \overline{\zeta}$. As in the last example, for unramified p,

$$\mathrm{Frob_p} : \zeta \mapsto \zeta^p.$$

Hence,

$$\mathrm{Frob_p} : \begin{cases} \phi \mapsto \phi & \text{if } p = 1 \text{ or } 9 \mod 10 \\ \phi \mapsto s(\phi) & \text{if } p = 3 \text{ or } 7 \mod 10 \end{cases}.$$

In general, the modulus for quadratic fields are determined by embeddings of the splitting field into cyclotomic fields:

$$K \hookrightarrow \mathbb{Q}(e^{2\pi i/\text{modulus}}).$$

Remark 1.8. Consider the degree 5 polynomial $f(x) = x^5 + 20x + 16$ we discussed in the first section. In all of the primes that occurred in our table, $f(x)$ had either 0 or 2 solutions. However, we would expect that for certain primes, $f(x)$ should have 5 solutions by Chebotarev's theorem. Anthony asked if we should be worried that we haven't seen any 5's in our chart. Geordie reassured us that we shouldn't be worried. In this example, $\Gamma = A_5$ has order 60. Then, by our discussion earlier,

$$\begin{aligned} \#\text{ solutions modulo } p = 5 &\iff \text{all solutions in } \mathbb{F}_{p^m} \text{ are defined over } \mathbb{F}_p \\ &\iff \text{all solutions are fixed by } \overline{\mathrm{Frob_p}} \\ &\iff \mathrm{Frob_p} = id. \end{aligned}$$

Since id is in its own conjugacy class, we expect $f(x)$ to have 5 solutions modulo p about 1/60th of the time by Chebotarev's density theorem. We included fewer than 60 primes in our table, so we shouldn't be surprised that we haven't seen this happen yet.

It may seem like considering the number of solutions of a polynomial over a finite field is a cute, but not particularly important problem. However, it is actually of fundamental importance in number theory. A **number field** is a finite extension of $\mathbb{Q}$. All number fields (which are Galois extensions) are splitting fields of polynomials $f(x) \in \mathbb{Z}[x]$. One of the the most basic open questions in number theory is the following:

Question 1.9. How many number fields are there?

We can determine the field extension K corresponding to the polynomial $f(x)$ by reducing mod p:

Theorem 1.10. The set $\{p \mid p \text{ unramified and } f(x) \text{ splits completely mod } p\}$ completely determines K.

So our motivational problem may have been cute, but it certainly isn't unimportant.

1.6 Solutions to Exercises

Exercise 1.5. Check that in Example 1.4, $\mathrm{Frob_p} : i \mapsto i^p$, as claimed.

Proof. We'll start by checking this for two specific primes: $p = 3$ and $p = 5$. Since $3 = 3 \mod 4$, $\bar{f}(x)$ has no roots in $\mathbb{F}_3$. Therefore, it must have two roots in $\mathbb{F}_9$. Recall that in general (that is, for $p \neq 2$ arbitrary and $k \in \mathbb{Z}_+$), $\mathbb{F}_{p^k} \simeq \mathbb{F}_p[x]/(g(x))$, where $g(x)$ is an irreducible degree k polynomial in $\mathbb{F}_p[x]$. This is how we can explicitly realize elements of finite fields whose order is not prime. Using this, we can see that the nine elements of $\mathbb{F}_9$ can be realized as the following set:

$$\{0, 1, 2, i, 2i, 1 + i, 1 + 2i, 2 + i, 2 + 2i\}.$$

In this set, the roots of $x^2 + 1$ are $\{i, 2i\}$, and $\overline{\mathrm{Frob}_3} : x \mapsto x^3$ acts on the set of roots by sending $i \mapsto 2i$ and $2i \mapsto i$. Therefore, Frob_3 must act on the set $\{i, -i\}$ by sending $i \mapsto -i$ and $-i \mapsto i$. Since $i^3 = -i$, we see that indeed $\mathrm{Frob}_3 : i \mapsto i^3$.

Now consider $p = 5$. Since $5 = 1 \mod 4$, $\bar{f}(x)$ has two roots in $\mathbb{F}_5$, namely $\{2, 3\}$. On these roots, $\overline{\mathrm{Frob}_5} : x \mapsto x^5$ sends $2 \mapsto 2$ and $3 \mapsto 3$. Therefore, Frob_5 must send $i \mapsto i = i^5$ and $-i \mapsto (-i)^5$, so again, $\mathrm{Frob}_5 : i \mapsto i^5$.

From these two examples we can see the general pattern. Let $p \neq 2$ be arbitrary, and let $\overline{\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p) = \mathbb{Z}/2\mathbb{Z} = \{\overline{id}, \bar{s}\}}$. We have two possibilities for $\overline{\mathrm{Frob_p}}$: either $\overline{\mathrm{Frob_p}} = \overline{id}$ or $\overline{\mathrm{Frob_p}} = \bar{s}$. Then

$$\overline{\mathrm{Frob_p}} = \overline{id} \iff x^p = x \text{ for all roots } x \text{ of } \bar{f} \iff x \in \mathbb{F}_p \iff p = 1 \mod 4,$$

and

$$\overline{\mathrm{Frob_p}} = \bar{s} \iff x^{p^2} = x \text{ but } x^p \neq x \text{ for all roots } x \text{ of } \bar{f} \iff x \notin \mathbb{F}_p \iff p = 3 \mod 4.$$

Since $\mathrm{Frob_p}$ acts on $\{i, -i\}$ as $\overline{\mathrm{Frob_p}}$ acts on the set of roots of $\bar{f}$ in $\mathbb{F}_{p^2}$, there are also only two possibilities for $\mathrm{Frob_p}$: either $\mathrm{Frob_p} = id$ (which happens exactly when $\overline{\mathrm{Frob_p}} = \overline{id}$; i.e. $p = 1 \mod 4$), or $\mathrm{Frob_p} = s$ (which happens exactly when $\overline{\mathrm{Frob_p}} = \bar{s}$; i.e. $p = 3 \mod 4$). In either case, we see that $\mathrm{Frob_p} : i \mapsto i^p$, since $i^p = i$ for $p = 1 \mod 4$ and $(-i)^p = i$ for $p = 3 \mod 4$. □

Exercise 1.5. By considering cyclotomic extensions (i.e. $\mathbb{Q}(e^{2\pi i/m})$), show that Chebotarev's density theorem implies Dirichlet's theorem on primes in arithmetic progression.

Proof. Consider the cyclotomic extension $\mathbb{Q}(e^{2\pi i/m})$ of $\mathbb{Q}$. This is the splitting field of the polynomial

$$\Phi_m(x) = \prod_{1 \leq k \leq m, (k,m)=1} (x - e^{2\pi i k/m}).$$

Note that $\Phi_m(x) | x^m - 1$, so for any root α of Φ_m or $\overline{\Phi}_m$ for any prime p, $\alpha^m = 1$. The Galois group of this extension is $\Gamma = (\mathbb{Z}/m\mathbb{Z})^\times$. Since Γ is abelian, conjugacy classes are singletons. The order of Γ is $\varphi(m) = \#\{k : 1 \leq k \leq m \text{ and } (k, m) = 1\}$. For any element $x \in \Gamma$, Chebotarev's density theorem implies that the set $\{p | \mathrm{Frob_p} = x\}$ has density $1/\varphi(m)$ in the set of all primes. If p and q are distinct primes which are both congruent to a modulo

m, then $\overline{\mathrm{Frob}_\mathrm{p}} = \overline{\mathrm{Frob}_q}$, since for any root $\overline{\alpha}$ of $\overline{\Phi}_m$, $\alpha^p = \alpha^q = \alpha^a$. Since Frob_p acts on the set of roots of Φ_m as $\overline{\mathrm{Frob}_\mathrm{p}}$ acts on the set of roots of $\overline{\Phi}_m$, this implies that $\mathrm{Frob}_\mathrm{p} = \mathrm{Frob}_q$. Similarly, if $\mathrm{Frob}_\mathrm{p} = \mathrm{Frob}_q$ for two primes $p \neq q$, then $\alpha^p = \alpha^q$ for any root α of $\overline{\Phi}_m$, and $p = q \mod m$. Hence,

$$p = q \mod m \iff \mathrm{Frob}_\mathrm{p} = \mathrm{Frob}_q$$

So by Chebotarev's density theorem, for any two coprime positive integers a, m, the set of primes congruent to a modulo m has density $1/\varphi(m)$ in the set of all primes. Since the set of all primes is infinite, this implies that there are infinitely many primes congruent to a modulo m, which is the statement of Dirichlet's theorem on primes in progression. □

2 Lecture 2 (March 15, 2019): Review of some algebraic number theory

Last time we discussed how by Chebotarev's density theorem, the equation $f(x) = x^5 + 20x + 16$ should have five solutions modulo p about $1/60^{th}$ of the time. Joel (+ a computer) computed that in the set of all primes below $500,000$, there are $16,613$ where $f(x)$ has no solutions, $10,367$ where $f(x)$ has one solution, $13,885$ with two solutions, and 673 with five solutions. In this case, we know that the Galois group is A_5, so it is order 60, but if we didn't know the Galois group, we could use this data to predict its order.

Exercise 2.1. Check the consistency of the numbers above with Chebotarev's density theorem.

The goal of today's lecture is to give the necessary background in algebraic number theory to continue. It is roughly based on a lecture by Dick Gross [Gro11].

2.1 Number fields

A **number field** is a finite extension of $\mathbb{Q}$. Given a number field $K/\mathbb{Q}$ of degree n (in this lecture, our field extensions will always be degree n), there is an associated **ring of integers** $\mathbb{O} \subset K$ consisting of all elements of K which satisfy a monic polynomial with coefficients in $\mathbb{Z}$. The ring of integers $\mathbb{O}$ is a free $\mathbb{Z}$-module of rank n, as well as a Dedekind domain (i.e. Noetherian, normal, Krull dimension 1).

Exercise 2.2. Show that the following field extensions have the following rings of integers:

1. $K = \mathbb{Q}(i)$, $\mathbb{O} = \mathbb{Z}[i]$.
2. $K = \mathbb{Z}(\sqrt{2})$, $\mathbb{O} = \mathbb{Z}[\sqrt{2}]$.
3. $K = \mathbb{Q}(\sqrt{5})$, $\mathbb{O} = \mathbb{Z}[\phi]$, where $\phi = \frac{1+\sqrt{5}}{2}$.

Generally, for a complicated extension, it is not easy to find $\mathbb{O}$.

We can measure how complicated a number field is using something called the **discriminant**. It is defined as follows. Let $K/\mathbb{Q}$ be a number field. Given $x \in K$, we get a $\mathbb{Q}$-linear map $x\cdot : K \to K$. Using this we define

$$\begin{aligned} \mathrm{Tr} :& K \to \mathbb{Q} \\ \mathrm{Nm} :& K^\times \to \mathbb{Q}^\times \end{aligned}$$

by $\mathrm{Tr}(x) := \mathrm{Tr}(x\cdot)$, $\mathrm{Nm}(x) := \det(x\cdot)$. This gives us a bilinear form called the **trace form**:

$$\begin{aligned} K \times K &\to \mathbb{Q} \\ (x, y) &:= \mathrm{Tr}(xy). \end{aligned}$$

The trace form is nondegenerate because $\mathrm{Tr}(1) = n$, hence $\mathrm{Tr}(xx^{-1}) = n \neq 0$. Since any element of $\mathbb{O}$ satisfies a monic polynomial with integer coefficients, the trace form restricts to a map $\mathbb{O} \times \mathbb{O} \to \mathbb{Z}$. Choose a $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ for $\mathbb{O}$. Then the **discriminant** of the field K is

$$\mathrm{Disc}(K) := \det((\alpha_i, \alpha_j)).$$

This is a close relative of the discriminant of a polynomial.

Remark 2.3. We have no idea how many number fields there are, so it is useful to have a measurement of how complicated a number field is. This is one of the reasons the discriminant is so useful.

Example 2.4. Let $K = \mathbb{Q}(i)$. Then $\mathbb{O} = \mathbb{Z}[i]$ has basis $\{\alpha_1, \alpha_2\} = \{1, i\}$. We can compute

$$((\alpha_i, \alpha_j)) = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix},$$

so $\mathrm{Disc}(K) = \det((\alpha_i, \alpha_j)) = -4$.

Exercise 2.5. 1. Let $\alpha \in \mathbb{Z}$ be square-free. Let $K = \mathbb{Q}(\sqrt{\alpha})$. Then

$$\mathbb{O} = \begin{cases} \mathbb{Z}[\sqrt{\alpha}] & \text{if } \alpha \neq 1 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{\alpha}}{2}\right] & \text{if } \alpha = 1 \mod 4 \end{cases}.$$

Hence, calculate

$$\mathrm{Disc}(K) = \begin{cases} 4\alpha & \text{if } \alpha \neq 1 \mod 4 \\ \alpha & \text{if } \alpha = 1 \mod 4 \end{cases}.$$

2. Calculate the discriminant of $\mathbb{Q}(e^{2\pi i/3})$.

Let $K/\mathbb{Q}$ be an étale $\mathbb{Q}$-algebra (i.e. a finite separable extension of $\mathbb{Q}$). Then $K \otimes_{\mathbb{Q}} \mathbb{R}$ is an étale $\mathbb{R}$-algebra, so $K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, where $n = r_1 + 2r_2$. The field K is **totally real** if $r_2 = 0$ (or, equivalently, if every embedding $K \hookrightarrow \mathbb{C}$ lands in $\mathbb{R}$). For example, this happens if it is the splitting field of a polynomial with real roots.

Exercise 2.6. Show that the signature of the trace form on K totally real is $(r_1 + r_2, r_2)$. In particular,

$$K \text{ is totally real} \iff r_2 = 0 \iff (\cdot,\cdot) \text{ is positive definite.}$$

2.2 An analogy

Next we will explore a useful analogy which will be a theme of this course.

$$\left\{ \begin{array}{c} \text{finite extensions} \\ K \text{ of } \mathbb{C}(x) = \mathrm{Frac}\mathbb{C}[x] \\ \text{(called } \textbf{function fields}\text{)} \end{array} \right\} \leftarrow \left\{ \begin{array}{c} \text{smooth complex} \\ \text{projective curves} \\ C \text{ over } \mathbb{P}^1\mathbb{C} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{compact Riemann} \\ \text{surfaces with a} \\ \text{map to } \mathbb{P}^1\mathbb{C} \end{array} \right\}$$

The first arrow going left is given by taking the function field of the curve. We can also go in the other direction. Given

$$\begin{tikzcd}
K \arrow[r, hookleftarrow] \arrow[d] & \mathbb{O} \arrow[d] \\
\mathbb{C}(x) \arrow[r, hookleftarrow] & \mathbb{C}[x]
\end{tikzcd}$$

we obtain a map $\operatorname{Spec}\mathbb{O} \to \operatorname{Spec}\mathbb{C}[x] = \mathbb{A}^1$, so we have a unique compactification and an equivalence between the first two sets.

Similarly, there is a bijection

$$\left\{ \begin{array}{c} \text{finite extensions} \\ K \text{ of } \mathbb{F}_p(x) \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{smooth projective} \\ \text{curves } C \text{ over } \mathbb{P}^1_{\mathbb{F}p} \end{array} \right\}.$$

Classically, people worked on problems in number theory in the algebraic world. Artin moved to the geometric world and proved deep results there. Many people in modern number theory work on the geometric side and hope to prove something about number fields. Here is a (very rough) schematic of difficulty:

$$\text{function fields over } \mathbb{C} << \text{function fields over } \mathbb{F}_p << \text{ number fields}$$

For a very inspiring reference for all of this, see André Weil's letter to his sister Simone Weil on the role of analogy in mathematics [Kri05].

Exercise 2.7. (Use of Google allowed.) Show that Fermat's last theorem is true in function fields; i.e. if $f, g, h \in k[x]$ are relatively prime and $f^n + g^n = h^n$, then $n = 2$.

2.3 The fundamental exact sequence

Let $K/\mathbb{Q}$ be a number field and $\mathbb{O}$ the ring of integers of K. A **fractional ideal** is a finitely generated $\mathbb{O}$-submodule of K. Given two fractional ideals I, J, we can construct their product:

$$IJ := \left\{ \sum \alpha_i \beta_j | \alpha_i \in I, \beta_j \in J \right\}.$$

(This is the "union" in the sense of algebraic geometry.) Since $\mathbb{O}$ is a Dedekind domain,

- every prime ideal $\mathfrak{p} \neq 0$ is maximal, and
- every fractional ideal has a unique factorization $I = \prod \mathfrak{p}_i^{e_i}$, where $\mathfrak{p}_i$ are prime ideals.

Denote by $\mathcal{J} = \bigoplus_{\mathfrak{p}\neq 0 \text{ prime}} \mathbb{Z}\mathfrak{p}$ the group of nonzero fractional ideals under this product. We have the following fundamental exact sequence:

$$\{1\} \to \mathbb{O}^\times \hookrightarrow K^\times \to \mathcal{J} \to \mathcal{C}\ell(K) \to 0.$$

Here $\mathcal{C}\ell(K)$ is the **ideal class group** of K, which measures the failure of $\mathbb{O}$ to be a PID. The ideal class group is difficult to calculate, and we know very little about it in general. The image of the second map in this exact sequence is $\mathcal{P}$, the set of all principal ideals (that is, ideals of the form $x\mathbb{O}$ for some $x \in K^\times$) of K.

Theorem 2.8. (Fundamental finiteness theorems)

1. The ideal class group $\mathcal{C}\ell(K)$ is finite.
2. The group $\mathbb{O}^\times$ is finitely generated of rank $r_1 + r_2 - 1$.

Exercise 2.9. Compute $\mathbb{O}^\times$ for $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$. (Hint: Pell's equation)

We can study an analogue of this exact sequence for a smooth projective curve. Let C be a compact Riemann surface. Then under the analogy,

$$0 \neq \mathfrak{p} \text{ prime ideals } = \text{ maximal ideals} \leftrightarrow \text{ points of } C,$$

and we have the following exact sequence:

$$\{1\} \to \mathbb{C}^\times \to K^\times \to \mathcal{P} \hookrightarrow \bigoplus_{x \in C} \mathbb{Z}x \twoheadrightarrow \operatorname{Pic}(C) \to 0.$$

Here K is the function field of C, $\mathcal{P}$ is the set of divisors of meromorphic functions ("principal divisors"), and $\operatorname{Pic}(C)$ is the Picard group of C (isomorphism classes of line bundles on C).

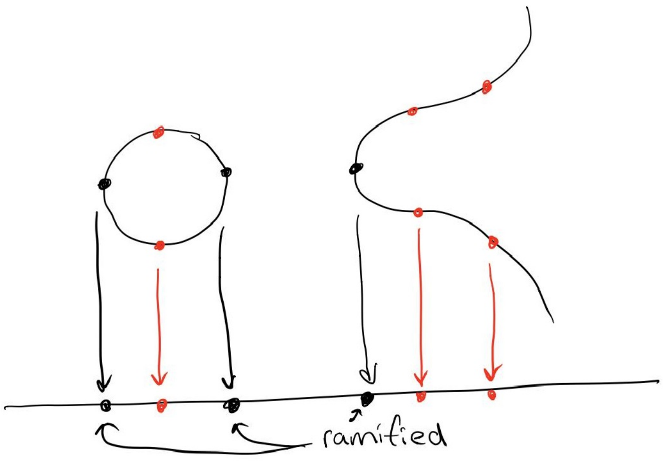
Remark 2.10. The group $\operatorname{Pic}(C) = \operatorname{Jac}(C) \times \mathbb{Z}$ is very far from finite. Also, $\mathbb{C}^\times$ is not finitely generated. So in this setting, neither of the fundamental finiteness theorems hold.

Exercise 2.11. (For those who know some algebraic geometry) Show that the analogues of $\mathcal{C}\ell(K)$ and $\mathbb{O}^\times$ are finite if C is an affine curve defined over a finite field.

Exercise 2.12. (If you know what K_0 is) Show that $K_0(\mathbb{O}) = \mathbb{Z} \oplus \mathcal{C}\ell(K)$.

2.4 Ramification

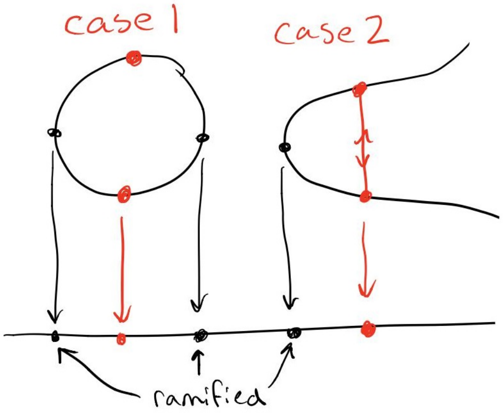
First consider a smooth projective curve $C \xrightarrow{f} \mathbb{P}^1\mathbb{C}$ (e.g. $y^2 = f(x)$ for some polynomial $f(x)$ without repeated roots.) After deleting a finite set of points from $\mathbb{P}^1\mathbb{C}$ (the "discriminant" of f), then f is étale, and hence gives us a finite covering of open sets $U \subset \mathbb{P}^1\mathbb{C}$. So all fibres are "the same" away from finitely many points where f is "ramified." A picture:



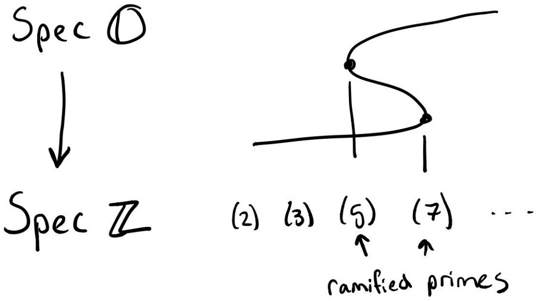
Over finite fields, almost the same thing happens. Again, if we have a smooth projective curve $C \xrightarrow{f} \mathbb{P}^1_{\mathbb{F}_p}$, f is étale after deleting finitely many points. For example, consider $C = \operatorname{Spec} \mathbb{F}_p[x,y]/(y^2 = x^3+1) \to \operatorname{Spec} \mathbb{F}_p[x]$. Fibres of this map over a point $x = \lambda$ are singular if λ is a third root of unity, or else

$$\mathbb{F}_p[x,y]/(y^2 = x^3+1) \otimes_{\mathbb{F}_p[x]} \mathbb{F}_p = \mathbb{F}_p[y]/(y^2 = \lambda^3+1) = \begin{cases} \mathbb{F}_p \times \mathbb{F}_p & \text{if } \lambda^3+1 \text{ is a square} \\ \mathbb{F}_{p^2} & \text{if } \lambda^3+1 \text{ is not a square} \end{cases}.$$

A picture:



A similar picture holds for number fields:



We can make this picture rigorous. Let $K/\mathbb{Q}$ be a number field and $\mathbb{O}$ its ring of integers. For each prime $p \in \mathbb{Z}$, the corresponding ideal in $\mathbb{O}$ decomposes into the product of prime ideals in $\mathbb{O}$:

$$(p) = \prod_{i=1}^{g_p} \mathfrak{p}_i^{e_i}.$$

We say the primes $\mathfrak{p}_i$ appearing in this decomposition are the "primes above (p)." The number e_i is the **ramification index** of $\mathfrak{p}_i$. For each $\mathfrak{p}_i$, the field $\mathbb{O}/\mathfrak{p}_i$ is a finite extension of $\mathbb{F}_p$ (so $\mathbb{O}/\mathfrak{p}_i = \mathbb{F}_{p^{f_i}}$ for some f_i), and the degree f_i of this extension is the **inertia degree**.

Exercise 2.13. (Important!) Show that $n = \sum_{i=1}^{g_p} e_i f_i$.

Definition 2.14. (a) The ideal (p) is **unramified** if all $e_i = 1$. Otherwise it is **ramified**.

(b) The ideal (p) **splits completely** if $f_i = e_i = 1$ for all i.

(c) The ideal (p) is **inert** if $g_p = 1$ and $e_1 = 1$.

Theorem 2.15. The ideal (p) is unramified in $\mathbb{O}$ if and only if $p \nmid \operatorname{Disc}(K)$.

Exercise 2.16. Prove Theorem 2.15. (Hint: Show that a finite-dimensional commutative $\mathbb{F}_p$-algebra is étale if and only if its trace form is nondegenerate.)

Example 2.17. Let $K = \mathbb{Q}(i)$, so $\mathbb{O} = \mathbb{Z}[i]$ and $\operatorname{Disc}(K) = -4$. (See Exercise 2.4.) Since $(1+i)^2 = 1 + 2i - 1 = 2i$, we see that the ideal $(2) \subset \mathbb{O}$ decomposes as $(2) = (1+i)^2$, and is therefore ramified. By Theorem 2.15, all other primes are unramified. Let $p \neq 2$ be prime. Then to determine if (p) splits, we notice that

$$\mathbb{Z}[i]/(p) = \mathbb{Z}[x]/(x^2+1, p) = \mathbb{F}_p[x]/(x^2+1) = \begin{cases} \mathbb{F}_p \times \mathbb{F}_p & \text{if } \left(\frac{-1}{p}\right) = 1 \\ \mathbb{F}_{p^2} & \text{if } \left(\frac{-1}{p}\right) = -1 \end{cases}.$$

Therefore (p) splits completely if and only if $p = 1 \mod 4$ (for example, $(5) = (2+i)(2-i)$), and (p) is inert if and only if $p = 3 \mod 4$.

We can adapt the strategy of Example 2.17 to determine splitting behavior in general. Let $K/\mathbb{Q}$ be a number field, and choose a primitive element (i.e. a generating element) θ of K. We can assume without loss of generality that $\theta \in \mathbb{O}$. Then θ satisfies a monic polynomial $f(x) \in \mathbb{Z}[x]$ of degree n, so $\mathbb{Z}[\theta] \subset \mathbb{O}$ is of finite index m. Then for p such the $p \nmid m$ and $p \nmid \operatorname{Disc}(K)$,

$$\mathbb{O}/(p) = \mathbb{Z}[\theta]/(p) = \mathbb{Z}[x]/(p, f(x)) = \mathbb{F}_p[x]/(f(x)) = \mathbb{F}_{p^{f_1}} \times \cdots \times \mathbb{F}_{p^{f_k}},$$

where f_i's are the degrees of irreducible factors of $f(x)$ modulo p. So in particular,

$$\begin{aligned} (p) \text{ splits completely} &\iff f \text{ is reducible modulo } p \\ (p) \text{ is inert} &\iff f \text{ is irreducible modulo } p. \end{aligned}$$

Hence we could have (and probably should have) phrased last week's lecture in terms of splitting of primes in a ring of integers.

2.5 The case of Galois extensions

Assume $K/\mathbb{Q}$ is a Galois extension, with Galois group $\operatorname{Gal}(K/\mathbb{Q}) = G$. Then G acts on $\mathbb{O}$, and Frobenius proved the following result.

Theorem 2.18. If $(p) = \prod \mathfrak{p}_i^{e_i}$, then G acts transitively on the primes $\mathfrak{p}_i$.

Therefore, all e_i (resp. f_i) are equal. Denote their common value e (resp. f). Exercise 2.13 ($n = \sum e_i f_i$) implies that $n = efg_p$. Fix a prime $\mathfrak{p}_i =: \mathfrak{p}$ lying over (p). Denote by $G_\mathfrak{p}$ the stabilizer of $\mathfrak{p}$ in G (the "decomposition group"). Then

$$|G/G_\mathfrak{p}| = \#\text{ primes over p } = g_p,$$

so $|G_\mathfrak{p}| = ef$. Let $I_\mathfrak{p}$ be the subgroup of $G_\mathfrak{p}$ which acts trivially on $\mathbb{O}_\mathfrak{p}$ (the "inertia group"). This group has order e. We have the following exact sequence

$$1 \to I_\mathfrak{p} \to G_\mathfrak{p} \twoheadrightarrow \mathrm{Aut}(\mathbb{O}/\mathfrak{p}) \simeq \mathbb{Z}/f\mathbb{Z}.$$

Since $\mathbb{O}/\mathfrak{p} \simeq \mathbb{F}_{p^f}$, the group $\mathrm{Aut}(\mathbb{O}/\mathfrak{p})$ is generated by $\overline{\mathrm{Frob}_\mathrm{p}} : x \mapsto x^p$. If p is unramified (i.e. $p \nmid \mathrm{Disc}(K)$), then $e = 1$, so $I_\mathfrak{p}$ is trivial and $G_\mathfrak{p} \simeq \mathbb{Z}/f\mathbb{Z}$. In this case, $\mathrm{Frob}_\mathrm{p} \in G_\mathfrak{p}$ is defined to be the element that maps to $\overline{\mathrm{Frob}_\mathrm{p}} \in \mathrm{Aut}(\mathbb{O}/\mathfrak{p})$. A different choice of $\mathfrak{p}$ lying over p results in conjugate $G_\mathfrak{p}$ and conjugate Frob_p. This explains rigorously the Frob_p from the last lecture.

2.6 Solutions to exercises

Exercise 2.1. Joel computed that of the primes below 500,000, there are 16,613 such that $f(x) = x^5 + 20x + 16$ has zero solutions, 10,367 one solution. 13,885 two solutions, and 673 five solutions. Check the consistency of these numbers with Chebotarev's density theorem.

Solution: There are 41,538 primes less than 500,000. There are five conjugacy classes in A_5, of sizes 1, 12, 12, 15, and 20. If $f(x)$ has five solutions modulo p, then $\overline{\mathrm{Frob}_\mathrm{p}}$ must fix all roots of $\bar{f}(x)$ in $\mathbb{F}_5$, so $\mathrm{Frob}_\mathrm{p} = id$ is in the single-element conjugacy class. By Chebotarev's density theorem, this should happen about $1/60 \approx 0.0167$ of the time. In our example, it happened $673/41,538 \approx 0.0162$ of the time. Chebotarev's density theorem predicts that Frob_p will lie in a conjugacy class C about $|C|/|\Gamma|$ of the time. We see that in our computation,

$$\begin{aligned}
&16,613/41,538 \approx 0.3999 \text{ (prediction: } 24/60 = 0.4),\\
&10,367/41,538 \approx 0.2495 \text{ (prediction: } 15/60 = 0.25),\\
&13,885/41,538 \approx 0.3343 (\text{ prediction: } 20/60 \approx 0.333).
\end{aligned}$$

So these numbers align very closely with the predictions made by Chebotarev's density theorem.

Exercise 2.2. Show that the following field extensions have the following rings of integers:

1. $K = \mathbb{Q}(i)$, $\mathbb{O} = \mathbb{Z}[i]$.
2. $K = \mathbb{Z}(\sqrt{2})$, $\mathbb{O} = \mathbb{Z}[\sqrt{2}]$.
3. $K = \mathbb{Q}(\sqrt{5})$, $\mathbb{O} = \mathbb{Z}[\phi]$, where $\phi = \frac{1+\sqrt{5}}{2}$.

Solution: See Exercise 2.5.

Exercise 2.5.

1. Let $\alpha \in \mathbb{Z}$ be square-free. Let $K = \mathbb{Q}(\sqrt{\alpha})$. Then
$$\mathbb{O} = \begin{cases} \mathbb{Z}[\sqrt{\alpha}] & \text{if } \alpha \neq 1 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{\alpha}}{2}\right] & \text{if } \alpha = 1 \mod 4 \end{cases}.$$
Hence, calculate
$$\operatorname{Disc}(K) = \begin{cases} 4\alpha & \text{if } \alpha \neq 1 \mod 4 \\ \alpha & \text{if } \alpha = 1 \mod 4 \end{cases}.$$

2. Calculate the discriminant of $\mathbb{Q}(e^{2\pi i/3})$.

Solution: Let $\alpha \in \mathbb{Z}$ be square-free, and let $K = \mathbb{Q}(\alpha)$. Consider $a + b\sqrt{\alpha} \in K$. The minimal polynomial of $a + b\sqrt{\alpha}$ is
$$p_{a,b}(x) = x^2 - 2ax + (a^2 - \alpha b^2).$$
(Why? Because $p_{a,b}(x)$ is a monic polynomial with rational coefficients with irrational roots $a + b\sqrt{\alpha}, a - b\sqrt{\alpha}$, so it must be irreducible.) Then,
$$\begin{aligned} a + b\sqrt{\alpha} \in \mathbb{O} &\iff p_{a,b}(x) \in \mathbb{Z}[x] \\ &\iff 2a \in \mathbb{Z} \text{ and } a^2 - \alpha b^2 \in \mathbb{Z}. \end{aligned}$$
If $a + b\sqrt{\alpha} \in \mathbb{O}$ and $a \notin \mathbb{Z}$, then $2a \in \mathbb{Z}$ must be an odd integer, so $2a = 2j + 1$ for some $j \in \mathbb{Z}$, and
$$a^2 - \alpha b^2 = \frac{4j^2 + 4j + 1 - 4\alpha b^4}{4}.$$
Thus if $b \in \mathbb{Z}$, $a^2 - \alpha b^2$ is not an integer, and if $2b \notin \mathbb{Z}$, then $a^2 - \alpha b^2$ if not an integer. (Or else $(2b)^2$ would be expressible as $\frac{\gamma}{\alpha}$ for some integer $\gamma = 1 \mod 4$, which is impossible since α is square-free.) So $2b \in \mathbb{Z}$ is odd, $2b = 2k + 1$ for some $k \in \mathbb{Z}$. Hence
$$a^2 - \alpha b^2 = \frac{4(j^2 + j - \alpha k^2 - \alpha k) + 1 - \alpha}{4},$$
which is an integer if and only if $\alpha = 1 \mod 4$. We conclude that there exists an algebraic integer $a + b\sqrt{\alpha} \in \mathbb{O}$ with $a, b \notin \mathbb{Z}$ if and only if $\alpha = 1 \mod 4$. In this case, $\frac{1+\sqrt{\alpha}}{2} \in \mathbb{O}$, since this is a root of the monic polynomial $x^2 - x + \frac{1-\alpha}{4} \in \mathbb{Z}[x]$, and $\mathbb{Z}\left[\frac{1+\sqrt{\alpha}}{2}\right] = \mathbb{O}$. If $\alpha \neq 1 \mod 4$, then $p_{a,b} \in \mathbb{Z}[x]$ if and only if $a, b \in \mathbb{Z}$, so $\mathbb{Z}[\sqrt{\alpha}] = \mathbb{O}$.

Once we know this, it is easy to calculate the discriminant of K. If $\alpha \neq 1 \mod 4$, the set $\{1, \sqrt{\alpha}\}$ is a basis for $\mathbb{O} = \mathbb{Z}[\sqrt{\alpha}]$. With this choice of basis, the three matrices corresponding to multiplication by $1, \sqrt{\alpha}$, and α are:
$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, M_{\sqrt{\alpha}} = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}, M_\alpha = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}.$$
From this, we calculate that the discriminant of K is
$$\operatorname{Disc}(K) = \det \begin{pmatrix} 2 & 0 \\ 0 & 2\alpha \end{pmatrix} = 4\alpha.$$

If $\alpha = 1 \mod 4$, then $\left\{1, \frac{1+\sqrt{\alpha}}{2}\right\}$ is a basis for $\mathbb{O} = \mathbb{Z}\left[\frac{1+\sqrt{\alpha}}{2}\right]$. With this choice of basis, the three matrices corresponding to multiplication by 1, $\frac{1+\sqrt{\alpha}}{2}$, and $\left(\frac{1+\sqrt{\alpha}}{2}\right)^2$ are

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, M_{\frac{1+\sqrt{\alpha}}{2}} = \begin{pmatrix} 0 & \frac{\alpha-1}{4} \\ 1 & 1 \end{pmatrix}, M_{\left(\frac{1+\sqrt{\alpha}}{2}\right)^2} = \begin{pmatrix} \frac{\alpha-1}{4} & \frac{\alpha-1}{4} \\ 1 & \frac{\alpha+3}{4} \end{pmatrix}.$$

From this, we calculate that the discriminant of K is

$$\operatorname{Disc}(K) = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{\alpha+1}{2} \end{pmatrix} = \alpha.$$

Exercise 2.6. Show that the signature of the trace form on K totally real is $(r_1 + r_2, r_2)$. In particular,

$$K \text{ is totally real } \iff r_2 = 0 \iff (\cdot, \cdot) \text{ is positive definite.}$$

Exercise 2.7. (Use of Google allowed.) Show that Fermat's last theorem is true in function fields; i.e. if $f, g, h \in k[x]$ are relatively prime and $f^n + g^n = h^n$, then $n = 2$.

Exercise 2.9. Compute $\mathbb{O}^\times$ for $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$. (Hint: Pell's equation)

Exercise 2.11. (For those who know some algebraic geometry) Show that the analogues of $\mathcal{C}\ell(K)$ and $\mathbb{O}^\times$ are finite if C is an affine curve.

Exercise 2.12. (If you know what K_0 is) Show that $K_0(\mathbb{O}) = \mathbb{Z} \oplus \mathcal{C}\ell(K)$.

Exercise 2.13. (Important!) Let $K/\mathbb{Q}$ be a number field of degree n, and

$$(p) = \prod_{i=1}^{g_p} \mathfrak{p}_i^{e_i}$$

the decomposition from section 2.4 of the prime ideal $(p) \subset \mathbb{O}$. Show that $n = \sum_{i=1}^{g_p} e_i f_i$, where e_i is the ramification index of $\mathfrak{p}_i$ and f_i is the inertia degree.

Exercise 2.16. Prove Theorem 2.15. (Hint: Show that a finite-dimensional commutative $\mathbb{F}_p$-algebra is étale if and only if its trace form is nondegenerate.)

3 Lecture 3 (March 21, 2019): L-functions

Last class we reviewed some algebraic number theory. This class we will review some analytic number theory. The motivation for this lecture is the following. We start with an arithmetic problem (for example, counting the number of $x \in \mathbb{F}_p$ such that $x^5 + 20x + 16 = 0$), and assign to it an L-function (which should be thought of as a "character"), which can be studied analytically.

3.1 The Riemann ζ-function

Define

$$\zeta(s) = \sum_{n \geq 1} n^{-s},$$

where $s \in \mathbb{C}$ is a complex variable. We can compare this sum to the integral

$$\int_1^\infty x^{-s} dx,$$

which converges to $\frac{1}{s-1}$ for real $s > 1$. When viewed as a holomorphic function, the integral converges absolutely for $s \in \mathbb{C}$ such that $\Re(s) > 1$. Hence the sum $\zeta(s)$ converges for all $s \in \mathbb{C}$ such that $\Re(s) > 1$.

This function has a rich history. Euler computed special values (e.g. $\zeta(2) = \frac{\pi^2}{2}$), and noticed that the ζ-function may also be given as the Euler product:

$$\sum_{n \geq 1} n^{-s} = (1 + 2^{-s} + (2^2)^{-s} + \cdots)(1 + 3^{-s} + (3^2)^{-s} + \cdots) \cdots = \prod_{p \text{ prime}} \left(\frac{1}{1 - p^s} \right).$$

This product relates an analytic object, $\zeta(s)$, to the prime numbers. *This relationship lets us study properties of primes using analysis!* For example, the Euler product immediately gives us two proofs of the infinitude of primes: (1) the divergence of $\sum_{n \geq 1} \frac{1}{n}$ implies the product on the right hand side must be infinite, and (2) since $\zeta(2) = \frac{\pi^2}{2}$, the irrationality of π^2 also implies that the right hand product must be infinite.

Riemann showed that ζ admits a meromorphic continuation to all of $\mathbb{C}$. This is the **Riemann zeta function**. He also showed that $\zeta(s)$ has a simple pole at $s = 1$ (Exercise: Show that $\zeta(s) - \frac{1}{1-s}$ converges for $\Re(s) > 0$), and "trivial zeros" at $-2, -4, \ldots$. Furthermore, he established the **functional equation**: $\Lambda(s) := \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$ satisfies

$$\Lambda(s) = \Lambda(1 - s).$$

Here $\Gamma(s) = \int_o^\infty x^{s-1} e^{-x} dx$ is the gamma function. And finally, he proposed the following conjecture, which eventually became a millenium question.

Riemann hypothesis: If z is a zero of $\zeta(z)$, then $\Re(z) = \frac{1}{2}$.

The Riemann hypothesis is known to be true for the first 10^{12} zeros of $\zeta(s)$.

3.2 Why do we care?

Here's the slogan of this story: "The zeros of the Riemann zeta function are the Fourier modes of the primes." We will spend the rest of the lecture trying to make this precise.

One of Riemann's motivations was the following theorem, which was a conjecture during his lifetime.

Theorem 3.1. (**Prime Number Theorem**) Let $\pi(x)$ be the number of primes less than or equal to $x \in \mathbb{R}$. Then

$$\pi(x) \sim \frac{x}{\log x}.$$

Here $\sim$ means that $\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$. Riemann was interested in two questions about the Prime Number Theorem:

- Why?
- What is the error term?

Instead of considering $\pi(x)$ directly, we can examine the **von Mangoldt function**, which "makes noise at prime powers":

$$\Lambda_{vm}(n) = \begin{cases} \log p & \text{if } n = p^m \\ 0 & \text{otherwise} \end{cases}.$$

Define

$$\psi(n) = \sum_{m \le n} \Lambda_{vm}(m).$$

Exercise 3.2. Show that the Prime Number Theorem is equivalent to $\psi(n) \sim n$.

Riemann discovered an explicit formula for $\psi(x)$ at non-integers.

Theorem 3.3. (Riemann) For $x \in \mathbb{R} - \mathbb{Z}$, there is equality

$$\psi(x) = x - \sum_{\rho} \frac{x^\rho}{\rho} - \log(2\pi),$$

where the sum is taken over all zeros ρ of the Riemann ζ-function.

In other words,

$$x - \psi(x) = \log(2\pi) + \sum_{\rho} \frac{x^\rho}{\rho},$$

so *the zeros of the Riemann ζ-function measure the error term in the prime number theorem.* We can examine what effect the different types of zeros have on the right hand side of the equality above.

- **Trivial zeros**: The function $\frac{x^{-2n}}{-2n} = -\frac{1}{2nx^n}$ decays very quickly, so for large x, trivial zeros have almost no effect on the formula.

- **A pair ρ, $\bar{\rho}$ of non-trivial conjugate zeros**: Each such pair contribues

$$\lambda \cdot x^{\Re(\rho)} \cdot \cos(\gamma + \log x),$$

where λ and γ depend in a simple way on ρ and $\bar{\rho}$. So $\Re(\rho)$ is crucial in the contribution of ρ and $\bar{\rho}$ to the error term, and if the Riemann hypothesis is true, the growth of this contribution looks roughly like the product of $\cos(x)$ and $x^{1/2}$. Also, as $\Im(\rho)$ gets bigger, λ gets smaller. Thus, if the Riemann hypothesis is true, small zeros will contribute larger variations. A counterexample to the Riemann hypothesis would cause huge fluctuations in $x - \psi(x)$, so it would be very visible eventually. We haven't see it yet.

Exercise 3.4. (a) Show that the Prime Number Theorem is equivalent to $\zeta(s)$ having no zeros z with $\Re(z) = 1$.

(b) Show that the Riemann hypothesis is equivalent to $x - \psi(x) \in O(x^{1/2})$.

(c) Find the error term in $\pi(x) - \frac{x}{\log x}$ assuming the Riemann hypothesis.

Remark 3.5. It is unknown whether there exist non-trivial zeros ζ of $\zeta(s)$ with $\Re(z) = 1 - \epsilon$ for *any* $\epsilon > 0$.

3.3 Dirichlet L-functions

It's natural to ask questions about primes satisfying certain properties. For example, fix $m \in \mathbb{Z}_{\geq 0}$, and $a \in (\mathbb{Z}/m\mathbb{Z})^{\times}$. Consider the set

$$\{p \text{ prime } | p = a \mod m\}.$$

Is this set infinite? Is there an analogue to the Prime Number Theorem in this setting? A naive attempt to show that this set is infinite would be to consider the product

$$\prod_{p} \frac{1}{1 - p^{-s}}$$

taken over all primes p such that $p = a \mod m$ and recreate one of the arguments for the infinitude of primes given in the previous section. However, there is no Euler product in this setting, so this approach fails. Another approach is representation theory.

What do we learn from representation theory?

Consider the set of all functions from

$$(\mathbb{Z}/m\mathbb{Z})^{\times} \to \mathbb{C}.$$

This set has two natural bases:

1. Indicator functions: $x \mapsto \delta_{x,a}$ for $a \in (\mathbb{Z}/m\mathbb{Z})^{\times}$
2. Irreducible characters: $x \mapsto e^{2\pi i j/\phi(m)}$ for $j = 0, \ldots, \phi(m) - 1$, where $\phi(m) = |(\mathbb{Z}/m\mathbb{Z})|$.

In many ways, the basis of characters is more natural. Dirichlet borrowed this idea of characters to adapt our naive attempt above into something that works.

Definition 3.6. A **Dirichlet character modulo m** is a character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ extended by zero to all of $\mathbb{Z}$. In other words, it is a function $\chi : \mathbb{Z} \to \mathbb{C}^\times$ such that $\chi(n) = 0$ if $(n, m) > 1$, $\chi(n)$ depends only on $n \mod m$ and χ induces a character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$.

Such a function χ has the property that $\chi(nn') = \chi(n)\chi(n')$. Using these characters, Dirichlet defined a **Dirichlet L-function**:

$$L(\chi, s) = \sum_{n \geq 1} \chi(n) n^{-s} = \prod_{p \text{ prime}} \frac{1}{1 - \chi(p)p^{-s}}.$$

With this adjustment by a character, the sum *does* admit an Euler product, as well as a meromorphic extension to all of $\mathbb{C}$, and a (rather complicated) functional equation. If χ is trivial, we recover the Riemann ζ-function. If χ is not trivial, then $L(\chi, s)$ is entire.

Dirichlet's theorem (that $\{p | p = a \mod m\}$ is infinite, with distribution $\frac{1}{\phi(m)} \frac{\pi}{\log x}$) is an easy consequence of the fact that $L(\chi, 1) \neq 0$ if χ is not trivial. Furthermore, there is an analogue of the Riemann hypothesis in this setting, usually called the "generalized Riemann hypothesis," and all non-trivial zeros of $L(\chi, s)$ lie on the critical line (i.e. satisfy $\Re(z) = \frac{1}{2}$).

3.4 Dedekind ζ-functions

Another natural question of this flavor is how primes behave in $\mathbb{Z}[i]$, or other rings of integers. To answer this question, Dedekind introduced his version of a ζ-function.

Return to the setting of last week: Let $K/\mathbb{Q}$ be a number field with ring of integers $\mathbb{O}$. For a nontrivial fractional ideal $I \subset \mathbb{O}$, let $\mathbb{N}I = \#\mathbb{O}/I$. (For example, if $K = \mathbb{Q}$, $\mathbb{N}(p) = p$.) The **Dedekind ζ-function** is

$$\zeta_K(s) = \sum_{0 \neq I \subset \mathbb{O}} (\mathbb{N}I)^{-s} = \prod_{\mathfrak{p} \subset \mathbb{O} \text{ prime}} \frac{1}{1 - \mathbb{N}\mathfrak{p}^{-s}}.$$

This sum admits an Euler product because of the uniqueness of factorization of ideals in $\mathbb{O}$. Again, we have a meromorphic continuation and functional equation in this setting. (Historical note: The functional equation first appeared in Hecke's thesis in the 1920's, but the proof was very complicated in Hecke's work. A much simpler proof was given by Tate in his thesis in 1950.) The key example is the following.

Example 3.7. Let $K = \mathbb{Q}(i) \supset \mathbb{O} = \mathbb{Z}[i]$. Then

$$\begin{aligned}
\zeta_K(s) &= \prod_{\mathfrak{p}\subset\mathbb{O} \text{ prime}} \frac{1}{1-\mathbb{N}\mathfrak{p}^{-s}} \\
&= \left(\frac{1}{1-2^{-s}}\right) \prod_{\mathfrak{p} \text{ s.t. } (p) \text{ splits}} \left(\frac{1}{1-\mathbb{N}\mathfrak{p}^{-s}}\right)\left(\frac{1}{1-\mathbb{N}\mathfrak{p}^{-s}}\right) \prod_{\mathfrak{p} \text{ s.t. } (p) \text{ is inert}} \left(\frac{1}{1-\mathbb{N}\mathfrak{p}^{-2s}}\right) \\
&= \left(\frac{1}{1-2^{-s}}\right) \prod_{p=1 \mod 4} \left(\frac{1}{1-p^{-s}}\right)^2 \prod_{p=3 \mod 4} \left(\frac{1}{1-p^{-s}}\right)\left(\frac{1}{1+p^{-s}}\right) \\
&= \prod_p \left(\frac{1}{1-p^{-s}}\right) \prod_{p\neq 2} \left(\frac{1}{1-\chi(p)p^{-s}}\right) \\
&= \zeta(s)L(\chi, s),
\end{aligned}$$

where

$$\chi(p) = \begin{cases} 1 & \text{if } p = 1 \mod 4 \\ -1 & \text{if } p = 3 \mod 4 \end{cases}$$

is a Dirichlet character on $\mathbb{Z}/4\mathbb{Z}$. The moral of this example is that *we can understand $\mathbb{Z}(i)$ in terms of $\mathbb{Z}$!* We are witnissing the beginnings of **class field theory**.

3.5 Walking across the bridge

Next we will cross our bridge of analogy and see what happens in the geometric world. Recall that the objects analogous to a ring of integers $\mathbb{O}$ contained in a number field K are smooth projective curves over $\mathbb{F}_p$ and their function fields over $\mathbb{F}_p$.

Example 3.8. The simplest example of such a smooth projective curve is $\mathbb{P}^1_{\mathbb{F}_p}$. Instead we'll work with $\mathbb{A}^1\mathbb{F}_p$, where the analogue of a ring of integers is $\mathcal{O}(\mathbb{A}^1\mathbb{F}_p) = \mathbb{F}_p[x]$. Here,

$$\begin{aligned}
\zeta_{\mathbb{A}^1\mathbb{F}_p}(s) &= \sum_{o\neq I\subset\mathbb{F}_p[x]} (\mathbb{N}I)^{-s} \\
&= \sum_{f \text{ monic}} (\mathbb{N}(f))^{-s} \\
&= \sum_{d\geq 1} \left(\sum_{f \text{ monic degree } d} (p^d)^{-s} \right) \\
&= \sum_{d\geq 0} p^d (p^d)^{-s} \\
&= \sum_{d\geq 0} (p^{-s+1})^d \\
&= \frac{1}{1-p^{-s+1}}.
\end{aligned}$$

So $\zeta_{\mathbb{A}^1_{\mathbb{F}_p}}(s)$ is a rational function with a unique pole at $s = 1$ and *no zeros*. Since $\zeta_{\mathbb{A}^1_{\mathbb{F}_p}}(s)$ measures the error term of the prime number theorem, this means that we can count primes exactly in this setting! In fact, we have (Gauss)

$$\#\text{ irred. polys of degree d} = \frac{1}{d}\sum_{m|d}\mu\left(\frac{d}{m}\right)p^m.$$

Here μ is the Mobius function (i.e. $\mu(n)$ is the sum of the primitive n^{th} roots of unity). So in this setting, we know exactly how many primes there are in a given interval.

Our example was a little too simple, so we should bump it up a notch. In Artin's thesis (1923), he instead considered $X = \mathbb{F}_p[x, y]/(y^2 - f(x))$ for $f(x)$ square free. (Under our analogy, this is the analogue of a quadratic field $\mathbb{Q}(\sqrt{a})$ for a square free.) Artin showed that

$$\zeta_X(s) = \frac{(1 - \alpha p^s)(1 - \bar{\alpha}p^s)}{1 - p^{-s+1}}$$

is again a rational function, with $\alpha \in \mathbb{C}$ of norm $p^{1/2}$. *Hence all zeros of $\zeta_X(s)$ have $\Re z = \frac{1}{2}$, and the Riemann hypothesis is true in this setting.* However, unlike the zeros of $\zeta(s)$, the zeros of $\zeta_X(s)$ are distributed evenly along the critical line.

The analogue to this statement for all curves was proven by Weil, and the case of arbitrary varieties was completed by Deligne (∼1970). These accomplishments were some of the crowning glories of 20^{th} century mathematics.

3.6 Artin L-functions

Now we enter the non-abelian world. The year is 1927, about 31 years after Frobenius started developing the theory of group characters. Let $K/\mathbb{Q}$ be a Galois extension, with $G = \mathrm{Gal}(K/\mathbb{Q})$, and $d_K = \mathrm{Disc}(K)$. Recall from previous lectures that:

- p is unramified if and only if $p \nmid d_K$, for unramified p,
- a choice of prime $\mathfrak{p}$ over p results in an element $\mathrm{Frob}_\mathrm{p} \in G$, and
- different choices of $\mathfrak{p}$ lead to conjugate Frob_p.

Fix a finite dimensional complex representation

$$\rho : G \to GL(V)$$

of the Galois group. Notice that the conjugacy class of $\rho(\mathrm{Frob}_\mathrm{p})$ is completely determined by its characteristic polynomial $\det(1 - t\,\mathrm{Frob}_\mathrm{p}|_V)$. The (first approximation) of an **Artin L-function** is

$$L_{ur}(V, s) = \prod_{p\nmid d_K}\frac{1}{\det(1 - p^{-s}\,\mathrm{Frob}_\mathrm{p}|_V)}.$$

Example 3.9. (a) V is the trivial representation. Then

$$L(V,s) = \prod_{p \nmid d_K} \frac{1}{1-p^{-s}} = \zeta(s) \text{ up to finitely many factors.}$$

So the Artin L-function recovers the Riemann ζ-function as a special case.

(b) Let $K = \mathbb{Z}(\sqrt{\alpha})/\mathbb{Q}$ be a quadratic field, $G = \{\pm 1\}$, and $\rho : G \to GL_1(C)$ be the identity map $\{\pm 1\} \mapsto \{\pm 1\}$. Then for $p \nmid d_K$,

$$\rho(\mathrm{Frob_p}) = \begin{cases} 1 & \text{if } p \text{ splits } \left(\iff \left(\frac{p}{\alpha}\right) = 1\right) \\ -1 & \text{if } p \text{ is inert } \left(\iff \left(\frac{p}{\alpha}\right) = -1\right) \end{cases}.$$

Therefore, by quadratic reciprocity,

$$\begin{aligned} L_{ur}(\rho, s) &= \prod_p \left(1 - \left(\frac{p}{\alpha}\right) p^{-s}\right)^{-1} \\ &= \prod_p (1 - \chi(p)p^{-s})^{-1} \\ &= L(\chi, s) \text{ up to finitely many factors} \end{aligned}$$

for some Dirichlet character $\chi : \mathbb{Z}/4\alpha\mathbb{Z} \to \mathbb{C}^\times$. So Artin L-functions also recover Dirichlet L-functions.

Exercise 3.10. (a) Show that $L_{ur}(V_1 \oplus V_2, s) = L_{ur}(V_1, s)L_{ur}(V_2, s)$.

(b) Show that $L(V,s)$ converges absolutely for $\Re s > 1$. (Hint: Compare it to a product of $\dim V$ copies of the ζ-function.)

(c) (Beautiful! Do it!) For a Galois extension $K/\mathbb{Q}$, let V_{reg} be the regular representation of G. Show that $L_{ur}(V_{reg}, s) = \zeta_K(s)$ up to finitely many factors.

A consequence of the exercise is the **Artin decomposition**:

$$\zeta_K(s) = \prod_{V \text{ irrep of } G} L_{ur}(V,s)^{\dim V} \text{ (up to finitely many factors).}$$

Hence $\zeta_{\mathbb{Q}}(s)$ always divides $\zeta_K(s)$! This is a generalization of the factorization $\zeta_{\mathbb{Q}(i)}(s) = \zeta(s)L(\chi, s)$ that we saw in Example 3.7.

The Moral: All of the difficulty in K is contained in the difficulty of $\mathbb{Q}$ if we allow for "non-abelian" difficulty (i.e. general representations of the Galois group).

Remark 3.11. We can get rid of the "up to finitely many factors" caveat in all of these statements by modifying $L_{ur}(V,s)$ with "general local factors" at ramified primes. See Geordie's hand-written lecture notes or Gus's lecture for a description of this procedure.

3.7 Solutions to exercises

Exercise 3.2. Show that the Prime Number Theorem is equivalent to $\psi(n) \sim n$.

Solution: Recall that $\psi(n) = \sum_{m \leq n} \Lambda(n)$, where $\Lambda(p^k) = \log p$ for prime powers, and $\Lambda(n) = 0$ otherwise. Writing out some values of this function,

$$\begin{array}{llllllll}
\psi(2) = & \log 2 & & & & & & \\
\psi(3) = & \log 2 & + \log 3 & & & & & \\
\psi(4) = & & \log 3 & + \log 4 & & & & \\
\psi(5) = & & \log 3 & + \log 4 & + \log 5 & & & \\
\psi(6) = & & \log 3 & + \log 4 & + \log 5 & & & \\
\psi(7) = & & \log 3 & + \log 4 & + \log 5 & + \log 7 & & \\
\psi(8) = & & \log 3 & & + \log 5 & + \log 7 & + \log 8 & \\
\psi(9) = & & & & \log 5 & + \log 7 & + \log 8 & + \log 9
\end{array}$$

so we see that we can write $\psi(n) = \sum_{p \leq n} \log(p^k)$, where the k in each summand is such that $p^k \leq n < p^{k+1}$. Hence we have

$$\psi(n) = \sum_{p \leq n} \log(p^k) \leq \sum_{p \leq n} \log n = \pi(n) \log n$$

which is one side of the bound we need. The other is a little more tricky: fix a positive integer r. Then

$$\psi(n) = \sum_{p \leq n} \log(p^k) \geq \sum_{p \leq n} \log p \geq \sum_{n^{1-\frac{1}{r}} \leq p \leq n} \log p$$

Since for each summand, $\log p \geq (1 - \frac{1}{r}) \log n$, and there are more than $\pi(n) - n^{1-\frac{1}{r}}$ summands, we have

$$\psi(n) \geq \left(1 - \frac{1}{r}\right) (\pi(n) - n^{1-\frac{1}{r}}) \log n$$

which together with the upper bound imply that $\psi(n) \sim n$ if and only if $\pi(n) \log n \sim n$.

Exercise 3.4.

(a) Show that the Prime Number Theorem is equivalent to $\zeta(s)$ having no zeros z with $\Re(z) = 1$.

(b) Show that the Riemann hypothesis is equivalent to $x - \psi(x) \in O(x^{1/2})$.

(c) Find the error term in $\pi(x) - \frac{x}{\log x}$ assuming the Riemann hypothesis.

Exercise 3.10.

(a) Show that $L_{ur}(V_1 \oplus V_2, s) = L_{ur}(V_1, s) L_{ur}(V_2, s)$.

(b) Show that $L(V, s)$ converges absolutely for $\mathrm{Re} s > 1$.

(c) (Beautiful! Do it!) For a Galois extension $K/\mathbb{Q}$, let V_{reg} be the regular representation of G. Show that $L_{ur}(V_{reg}, s) = \zeta_K(s)$ up to finitely many factors.

Solution (to part (c)): Assume $p \in \mathbb{Z}$ is unramified. Recall that for any prime $\mathfrak{p} \subset \mathbb{O}$ above p, we have a bijection

$$G_{\mathfrak{p}} \to \mathrm{Aut}(\mathbb{O}/\mathfrak{p}),$$

and $\mathrm{Frob}_\mathrm{p} \in G$ is defined to be the element that maps to $\overline{\mathrm{Frob}_\mathrm{p}} : x \mapsto x^p \in \mathrm{Aut}(\mathbb{O}/\mathfrak{p})$ under this bijection. Furthermore, $\mathbb{O}/\mathfrak{p} \simeq \mathbb{F}_{p^f}$, so Frob_p has order f, and $\mathbb{N}\mathfrak{p} = \#\mathbb{O}/\mathfrak{p} = p^f$.

The regular representation of G is the representation $\rho : G \to GL(V_{reg})$, where the vector space $V_{reg} = \mathbb{C}[G]$ is the group algebra of G, and $\rho(g)$ is given by left multiplication by g. For any vector $v_1 \in V_{reg}$, repeated action by $\phi = \rho(\mathrm{Frob}_\mathrm{p})$ generates an f-dimensional subspace $V_1 \subset V_{reg}$ with basis $\{v_1, \phi v_1, \dots \phi^{f-1} v_1\}$. We can choose any vector $v_2 \notin V_1$, and again repeated action by ϕ generates a f-dimensional subspace V_2 with basis $\{v_2, \phi v_2, \dots, \phi^{f-1} v_2\}$. Continuing this process, we obtain a basis for V_{reg} of the form

$$\{v_1, \phi v_1, \dots, \phi^{f-1} v_1, v_2, \phi v_2, \dots, \phi^{f-1} v_2, \dots, v_{g_p}, \phi v_{g_p}, \dots, \phi^{f-1} v_{g_p}\},$$

where g_p is the number of primes over p. (Recall that the degree of the extension $K/\mathbb{Q}$ is $n = f g_p$.) With this choice of basis, ϕ acts on the subspace $V_i \subset V_{reg}$ by the cycle matrix

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Since $\phi^f = 1$, the characteristic polynomial of this $f \times f$ matrix is $ch_\phi(x) = \det(xI - \phi|_{V_i}) = x^f - 1$. Therefore,

$$\det(I - p^{-1}\phi|_{V_i}) = p^{-fs} \det(p^s I - \phi|_{V_i}) = p^{-fs} ch_\phi(p^s) = p^{-fs}((p^s)^f - 1) = 1 - p^{-fs}.$$

Hence each $p \in \mathbb{Z}$ contributes

$$\prod_{g_p \text{ times}} \frac{1}{1 - p^{-fs}} = \left(\frac{1}{1 - p^{-fs}}\right)^{g_p}$$

to $L_{ur}(V_{reg}, s)$. We conclude that

$$L_{ur}(V_{reg}, s) = \prod_{p \nmid d_K} \frac{1}{\det(I - p^{-s}\phi)} = \prod_{p \nmid d_K} \left(\frac{1}{1 - p^{-fs}}\right)^{g_p} = \prod_{\mathfrak{p} \subset \mathbb{O} \text{ prime}} \frac{1}{1 - \mathbb{N}\mathfrak{p}^{-s}} = \zeta_K(s),$$

where the second-to-last equality is up to finitely many factors.

4 Lecture 4 (April 12, 2019): The Sato-Tate conjecture

This will be our final lecture of global motivation before we zoom in on the local story. The goal of today's lecture is to describe the **Sato-Tate conjecture** and it's relationship to the global Langlands picture. We will see that seemingly innocuous statements in the Langlands correspondence can have very powerful repurcussions.

4.1 Equidistribution in representation theory

We say that the real numbers $\alpha_1, \alpha_2, \ldots \in [0,1]$ are **equidistributed** if

$$\lim_{n\to\infty} \frac{1}{n} \#\{\alpha_i \mid \alpha_i \in (a,b) \text{ for } i = 1, \ldots, n\} = b - a = \int_0^1 1_{(a,b)} dx$$

for any interval $(a,b) \subset [0,1]$. Here $1_{(a,b)}$ is the indicator function on (a,b). Because indicator functions are dense in complex-valued Riemann integrable functions on $[0,1]$, this condition is equivalent to saying that the discrete average of any function on this set and continuous average of the same function agree; that is,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} f(\alpha_i) = \int_0^1 f(x) dx$$

for all Riemann integrable $f : [0,1] \to \mathbb{C}$. Now we can approximate any Riemann integrable $f : [0,1] \to \mathbb{C}$ with a Fourier series, so this is in turn equivalent to

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} e(m\alpha_i) = \int_0^1 e(mx) dx = \begin{cases} 1 & \text{if } m = 0 \\ 0 & \text{otherwise} \end{cases}$$

for all $m \in \mathbb{Z}$. Here $e(x) = \exp(2\pi i x)$. The condition above always holds for $m = 0$, so to check if $\alpha_1, \alpha_2, \ldots$ are equidistributed, it suffices to check that for $m \neq 0$,

$$\lim_{n\to\infty} \sum_{i=1}^{n} e(m\alpha_i) = 0.$$

Here's an application of this observation. Let $\xi \in \mathbb{R}$ be irrational. Consider $(\xi), (2\xi), (3\xi), \ldots$ where $(m\xi) := m\xi \mod 1$. Are these numbers equidistributed? Weyl used the observation above to show that they are. Choose $m \neq 0$, and let $\eta = m\xi$. Then

$$\left| \frac{1}{n} \sum_{j=1}^{n} e(mj\xi) \right| = \left| \frac{1}{n} (e(\eta) + e(2\eta) + \cdots e(n\eta)) \right| = \left| \frac{1}{n} \frac{e((n+1)\eta) - e(\eta)}{e(\eta) - 1} \right| \leq \frac{1}{n} \left| \frac{2}{e(\eta) - 1} \right| \to 0$$

as $n \to \infty$.

Remark 4.1. This leads to many questions of a similar flavor (e.g. what about $(\xi), (4\xi), (9\xi), \ldots$?) Weyl's paper [Wey16] gives an affirmative answer for polynomials $f(x) \in n\mathbb{R}[n]$ whose coefficients are not all rational!

We can reinterpret equidistribution via representation theory. The above reasoning shows (after identifying integers mod 1 with S^1) that a sequence $z_1, z_2, \ldots \in S^1 \subset \mathbb{C}$ **equidistributes** if for every nontrivial rational character χ of S^1 (e.g. $\chi : z \mapsto z^m$ for $m \neq 0$),

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} \chi(z_i) = 0.$$

If this condition holds, we say that the sum is "little o of n," and write

$$\sum_{i=1}^{n} \chi(z_i) = o(n).$$

Now suppose G is a compact group with Haar measure μ, and let X denote the space of conjugacy classes of G. (Recall that the **Haar measure** is the unique left (and then necessarily also right) G-invariant measure on G with $\mu(G) = 1$.) Let $C(X)$ be the Banach space of continuous complex-valued functions on X. Two properties of irreducible characters on compact groups are the following:

Theorem 4.2. (**The Peter-Weyl Theorem**) The irreducible characters span a dense subspace of $C(X)$.

Theorem 4.3. (**Orthogonality of characters**) If χ, χ' are irreducible characters, then

$$\int_G \chi(g)\overline{\chi'(g)} d\mu = \begin{cases} 1 & \text{if } \chi = \chi' \\ 0 & \text{otherwise} \end{cases}.$$

Hence, we have the following theorem about equidistribution of sequences in G.

Theorem 4.4. A sequence $\alpha_1, \alpha_2, \ldots \in X$ is equidistributed with respect to the (push forward of the) Haar measure if and only if

$$\sum_{i=1}^{n} \chi(\alpha_i) = o(n)$$

for all irreducible nontrivial characters χ.

Example 4.5. Let $G = S_3$. The conjugacy classes are determined by cycle type: $C_1 = \{id\}$, $C_2 = \{(12), (23), (13)\}$, $C_3 = \{(123), (132)\}$. The character table of S_3 is

Haar measure	#C$_i$	conj. class	triv	nat	sgn
1/6	1	C$_1$	1	2	1
1/2	3	C$_2$	1	0	-1
1/3	2	C$_3$	1	-1	1

We can see from this table that for a sequence to be equidistributed, it should spend twice the time in C_3 as it does in C_1 (as dictated by the column corresponding to the natural representation), and should spend as much time in C_2 as in $C_1 \cup C_3$ (as dictated by the column corresponding to the sign representation).

Example 4.6. Let $G = SU(2)$. Since all matrices in $SU(2)$ are diagonalizable, conjugacy classes are determined by eigenvalues, which come in conjugate pairs. So $X = \{(\gamma, \bar{\gamma}) | \gamma \in S_1\}$ can be identified with $S^1_+ = \{z \in S^1 | \Re(z) \geq 0\} \simeq [0, \pi]$. By the Weyl character formula for $SU(2)$, irreducible characters are of the form

$$\chi_m(z) = z^m + z^{m-2} + \cdots + z^{-m},$$

where $z = e^{i\theta} \in S^1$. (Here we are using the identification $X \simeq S^1_+$ when defining these characters.) The Haar measure on the space of conjugacy classes (after identifying S^1 with $[0, 2\pi]$ via the exponential function) is then

$$\frac{2}{\pi} \sin^2 \theta d\theta.$$

Exercise 4.7. Check that this is correct by showing that

$$\frac{2}{\pi} \int_0^\pi \sin^2 \theta d\theta = 1$$

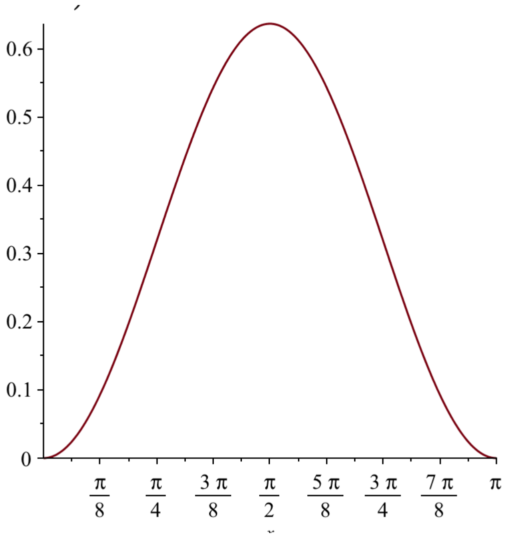
and

$$\int_0^\pi \chi_m(e^{i\theta}) \sin^2 \theta d\theta = 0$$

for $m \neq 0$.

The figure below is a plot of $\frac{2}{\pi} \sin^2 \theta$. From this we see the distribution of eigenvalues of matrices in $SU(2)$. A first observation is that there are many matrices in $SU(2)$ with eigenvalues $\{i, -i\}$ (corresponding to $\theta = \frac{\pi}{2}$), and very few matrices with eigenvalues $\{1, 1\}$ and $\{-1, -1\}$ (corresponding to $\theta = 0$ and $\theta = \pi$, respectively). In fact, there is exactly one matrix in each case: I and $-I$.

Remark 4.8. This demonstrates that it is more likely for matrices in $SU(2)$ to have eigenvalues which are "far away" (meaning that the angle between them in the complex plane is large), an important fact in random matrix theory.



Hence if you had a sequence of suspected eigenvalues which you suspect are the eigenvalues of random matrices in $SU(2)$, you could tell pretty quickly whether or not it was plausible.

4.2 Elliptic curves and the Sato-Tate conjecture

Next we discuss elliptic curves. (This seems to be completely unrelated, but we should have faith that it will come full circle.) Let k be a field, and E an elliptic curve. (That is, a smooth projective curve over k of genus 1 with a fixed rational point $0 \in E(k)$.) Assume the characteristic of k is not 2 or 3. Then E can be made to be of the form (the projective closure of)

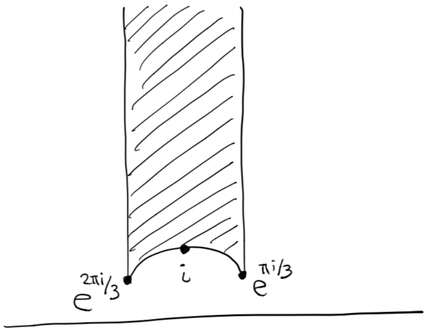
$$y^2 = x^3 + ax + b, \text{ with } 0 = (0 : 0 : 1) \text{ its point at infinity.}$$

Here smoothness translates into the fact that $x^3 + ax + b$ has no repeated roots, i.e. that $4a^3 - 27b^2 \neq 0$.

First assume we are working over $\mathbb{C}$. Then E is a compact Riemann surface of genus $g = 1$, so $E = \mathbb{C}/\Lambda$ for some lattice $\Lambda \simeq \mathbb{Z}^2 \hookrightarrow \mathbb{C}$. Hence

$$\left\{\begin{array}{c}\text{elliptic curves}\\ \text{over } \mathbb{C}\end{array}\right\}_{/\text{ iso}} \simeq \left\{\begin{array}{c}\text{lattices}\\ \Lambda \subset \mathbb{C}\end{array}\right\}_{/\text{ iso}} \xrightarrow{\text{“period ratio”}} {}_{SL_2(\mathbb{Z})}\backslash\mathbb{H},$$

where $\mathbb{H}$ is the upper half plane. The quotient ${}_{SL_2(\mathbb{Z})}\backslash\mathbb{H}$ can be identified (up to some ambiguity on the boundary) with its fundamental domain



so we can consider all complex elliptic curves as points in the region above.

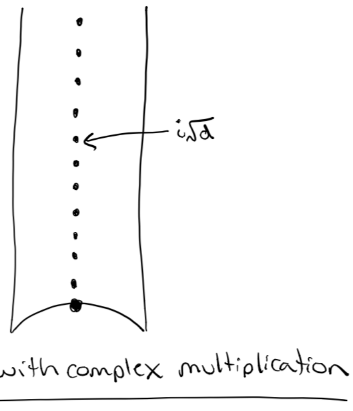
Certain elliptic curves have extra structure called complex multiplication. Let E be a complex elliptic curve. As a real Lie group, E is isomorphic to $S^1 \times S^1$, hence

$$\mathrm{End}_{\text{Lie gp}}(E) = \mathbb{Z}^2$$
$$(z, w) \mapsto (z^m, w^n) \leftrightarrow (m, n)$$

But E has additional structure - it is an elliptic curve ($E \simeq \mathbb{C}/\Lambda$), and a complex algebraic group. By a miracle of abelian varieties, the elliptic curve endomorphisms of E fixing 0 are the same as the complex algebraic group endomorphisms of E. Hence,

$$\mathrm{End}_{0\mapsto 0}(E) = \mathrm{End}_{\text{alg gp}}(E) = \{z \mid z\Lambda \subset \Lambda\} = \begin{cases}\mathbb{Z} & \text{if } \Lambda \cdot \Lambda \not\subset \Lambda \\ \Lambda & \text{if } \Lambda \cdot \Lambda \subset \Lambda\end{cases}.$$

In the second case, we say E has **complex multiplication**. In the fundamental domain, the elliptic curves with complex multiplication are of the form $i\sqrt{d}$:



Thus one can think of curves wuth complex multiplication as being very special.

Exercise 4.9. Show that if $\Lambda \cdot \Lambda \subset \Lambda$ (i.e. E has complex multiplication), $\Lambda \otimes \mathbb{Q}$ is an imaginary quadratic field. In particular, if E has complex multiplication then Λ is what is called an *order* in an imaginary quadratic field.

Next we work over $\mathbb{Q}$, and consider the elliptic curve E given by $y^2 = x^3 + ax + b$ for $a, b \in \mathbb{Z}$. To understand E, we reduce modulo p and study the number of points of $E(\mathbb{F}_p)$. If $E_{\mathbb{F}_p} = E \times \operatorname{Spec} \mathbb{F}_p$ is nonsingular, then p is a prime of **good reduction**. (This is the analogue for algebraic varieties of a prime being unramified.) We can bound $\#E(\mathbb{F}_p)$ by the **Hasse-Weil bound**:

Theorem 4.10. (Hasse-Weil)

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

where $|\alpha_p| \leq 2\sqrt{p}$.

The Hasse-Weil bound tells us that $1 + p$ is a "square root accurate" approximation for $\#E(\mathbb{F}_p)$. By our discussions last week, hopefully you are convinced that this is an analogue of the Riemann hypothesis for elliptic curves.

Big question: How do the α_p's behave?

We can start to answer this question using the **Grothendieck–Lefshetz trace formula.** Let $H^*(E)$ be the étale cohomology of E. For all p outside a finite set, we have an action of $\mathrm{Frob_p}$ on (étale, but don't worry if you don't know what this is) cohomology:

$$\begin{array}{cccc}
\dim: & 1 & 2 & 1 \\
 & H^0(E) & H^1(E) & H^2(E) \\
 & \circlearrowleft & \circlearrowleft & \circlearrowleft \\
 & \mathrm{Frob_p} = 1 & \mathrm{Frob_p} \sim \begin{pmatrix} \gamma_p & 0 \\ 0 & \overline{\gamma_p} \end{pmatrix} & \mathrm{Frob_p} = p
\end{array}$$

The Grothendieck-Lefshetz trace formula is

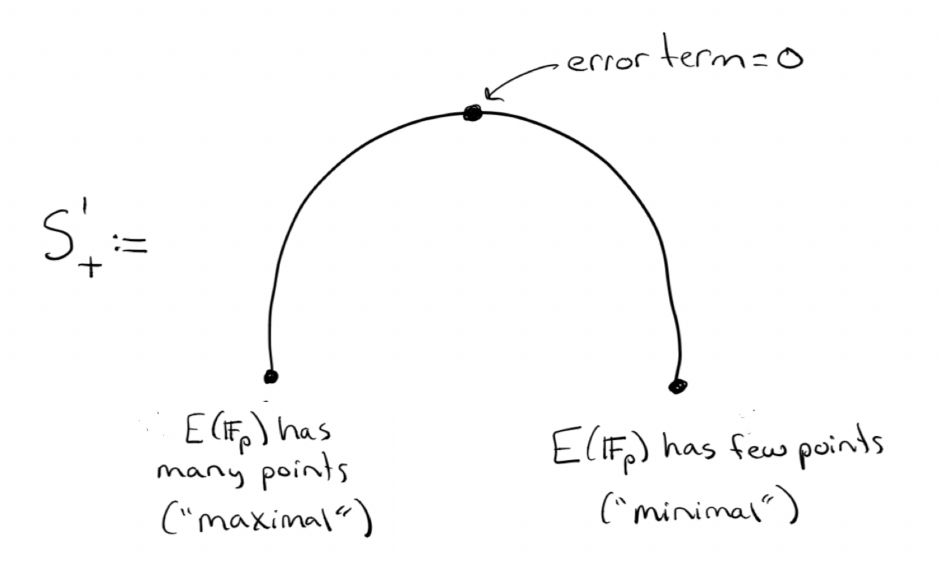
$$\#E(\mathbb{F}_p) = \sum (-1)^i \operatorname{Tr}(\mathrm{Frob_p} : H^i) = 1 + p - (\gamma_p + \overline{\gamma_p}),$$

where $\gamma_p, \overline{\gamma_p}$ are the eigenvalues of Frobenius on $H^1(E)$. Hence to determine the number of solutions of $E(\mathbb{F}_p)$, it is enough to examine γ_p, and it is true (but not so easy to see) that the Riemann hypothesis for E is equivalent to $|\gamma_p| = \frac{1}{2}$.

We can renormalize so that

$$\theta_p := \frac{1}{\sqrt{p}} \gamma_p \in S^1_+.$$

This leaves us with a sequence $\theta_2, \theta_3, \theta_5, \ldots$ of points on a semicircle S_1^+ controlling the number of points of E modulo p.

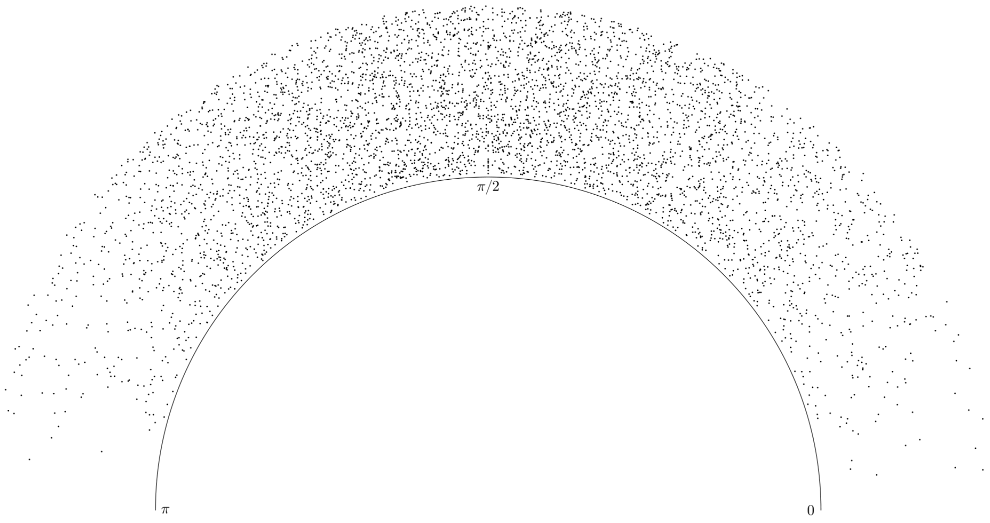

error term = 0
$S^1_+ :=$
$E(\mathbb{F}_p)$ has many points ("maximal")
$E(\mathbb{F}_p)$ has few points ("minimal")

Sato–Tate conjecture (1960): Suppose E does not have complex multiplication. If we identify $S^1_+ \xrightarrow{\simeq} [0, \pi]$, then

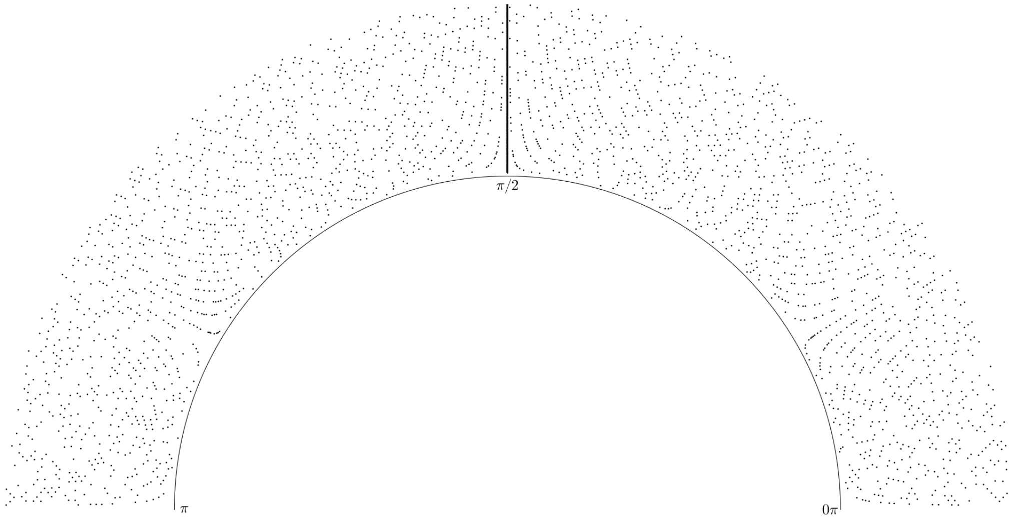
$$\lim_{n\to\infty} \frac{1}{\pi(n)} \sum_{p \leq n} \mu_{\theta_p} = \frac{2}{\pi} \sin^2 \theta d\theta.$$

Here μ_{θ_p} is the Dirac distribution.

In other words, the Sato–Tate conjecture is that the θ_p's look like eigenvalues of random matrices in $SU(2)$! Below is a very beautiful illustration of this phenomenon. For the elliptic curve $y^2 + y = x^3 + x + 3x + 5$ (which has no complex multiplication), the following is the plot of θ_p for the first $5,000$ primes. (The further out the dot, the bigger the prime.)



In contrast to this, consider the elliptic curve $y^2 = x^3 + 1$. Here complex multiplication is given by the Eisenstein integers. The plot below shows θ_p for the first $5,000$ primes. Norm is linear in the prime (so, again, the further the dot, the bigger the prime).



The difference between these two curves is striking!

Remark 4.11. The case of complex multiplication is well understood. The idea (Geordie thinks) is that the extra endomorphisms force the $\mathrm{Frob_p}$ to lie in a subgroup of $SU(2)$. (Geordie points out that he is "the exact opposite of an expert on this topic...")

Remark 4.12. One can think of Sato-Tate (roughly) as a higher-dimensional analogue of Chebotarev density: $\mathrm{Gal}(K/\mathbb{Q}) \leftrightarrow SU(2)$.

4.3 Equidistribution and L-functions

In the final part of this lecture, we will describe how the Sato–Tate conjecture follows from a simple part of the Langlands correspondence (which is still conjectural). The Sato–Tate conjecture has been proven using other methods, but the proof is very involved and heavily influenced by ideas from the Langlands program. This example is meant to showcase the power of the Langlands correspondence.

Let G be a compact group, X its space of conjugacy classes, and $x_p \in X$ a family of elements parameterized by primes p (perhaps outside some finite set of "bad" primes). For an irreducible character χ, we can define an L-function analogously to how we defined Artin L-functions for Galois groups:

$$L(\chi, s) = \prod_p \frac{1}{\det(1 - \rho(x_p)p^{-s})},$$

where ρ is the representation afforded by χ. This converges for $\Re(s) > 1$. Assume additionally that $L(\chi, s)$ extends to a meromorphic function on $\Re(s) \geq 1$ having neither zeros nor poles along $\Re(s) = 1$ except possibly at $s = 1$. Let $-c_\chi$ be the order of $L(\chi, s)$ at $s = 1$ (so $c_\chi > 0$ pole, $c_\chi < 0$ zero). With these assumptions, we have the following theorem.

Theorem 4.13.

$$\sum_{p \leq n} \chi(x_p) = c_\chi \cdot \frac{n}{\log(n)} + o\left(\frac{n}{\log(n)}\right).$$

The proof of this theorem involves some complex analysis and tricks with sums, but is not difficult. This theorem has an important corollary.

Corollary 4.14. If for all nontrivial χ, $L(\chi, s)$ is holomorphic and nonzero at $s = 1$, then the x_p are equidistributed in X.

So we can use L-functions to test whether a sequence in a compact group is equidistributed!

Exercise 4.15. (a) Show that $L(\chi, 1) \neq 0$ implies Dirichlet's theorem.

(b) Let K be a number field. It's known that $\zeta_K(s)/\zeta(s)$ is holomorphic and nonvanishing at $s = 1$. Using this, deduce Chebotarev's density theorem.

An important consequence of Corollary 4.14 is that it lets us reframe the Sato-Tate conjecture in terms of L-functions.

Example 4.16. (Serre) Assume that for all $m \geq 1$, the symmetric L-power function

$$L(S^m_\chi, s) := \prod_p \frac{1}{(1 - \theta_p^m p^{-s})(1 - \theta_p^{m-2} p^{-s}) \cdots (1 - \theta_p^{-m} p^{-s})}$$

satisfies the extra assumption above. (Here S^m_χ is the m^{th} symmetric power of the representation with character χ sending $\mathrm{Frob_p} \mapsto \begin{pmatrix} \theta_p & 0 \\ 0 & \theta_p^{-1} \end{pmatrix}$.) Then the Sato-Tate conjecture holds!

Recall our cartoon of the Langlands correspondence:

$$\begin{tikzcd}
\left\{\begin{array}{c}\text{“geometric” } n\text{-dimensional}\\ \text{rep'ns of } \mathrm{Gal}(K)=\mathrm{Gal}(\overline{K}/K)\end{array}\right\} \arrow[rr, leftrightarrow, "\text{finite-to-one}"] \arrow[dr] & & \left\{\begin{array}{c}\text{“automorphic” rep'ns}\\ \text{of } GL_n(\mathbb{A})\end{array}\right\} \arrow[dl] \\
& L\text{-functions} &
\end{tikzcd}$$

An extremely important part of this picture is **functoriality**. That is, the diagram should be compatible with

1. composition of representations of the Galois group with algebraic representations of GL_n (so $\rho : \mathrm{Gal}(K) \to GL_n \xrightarrow{\text{alg rep'n}} GL_m$ should correspond to some operation on automorphic representations), and

2. changing the field K.

A key piece of the Langlands correspondence is that L-functions coming from automorphic representations have many desirable properties, which are extremely difficult to establish for L-functions coming from geometric representations of $\mathrm{Gal}(K)$. For example, once we know that an L-function comes from an automorphic representation, we immediately know that it admits a meromorphic continuation and has a functional equation.

The Punchline: *In the simple example of the algebraic representation $GL_2 \to GL_m$ via symmetric powers, the prediction of functoriality implies the Sato-Tate conjecture!*

4.4 Solutions to exercises

Exercise 4.6. Check that the Haar measure on $SU(2)$ is indeed $\frac{2}{\pi}\sin^2\theta d\theta$ by showing that

$$\frac{2}{\pi}\int_0^\pi \sin^2\theta d\theta = 1$$

and

$$\int_0^\pi \chi_m \sin^2\theta d\theta = 0$$

for $m \neq 0$.

Exercise 4.7. Let $E = \mathbb{C}/\Lambda$ be a complex elliptic curve. Show that if $\Lambda \cdot \Lambda \subset \Lambda$ (i.e. E has complex multiplication), $\Lambda \otimes \mathbb{Q}$ is an imaginary quadratic field.

Exercise 4.12.

(a) Let $L(\chi, s)$ be an L function for a compact group G. Show that $L(\chi, 1) \neq 0$ implies Dirichlet's theorem.

(b) Let K be a number field. It's known that $\zeta_K(s)/\zeta(s)$ is holomorphic and nonvanishing at $s = 1$. Using this, deduce Chebotarev's density theorem.

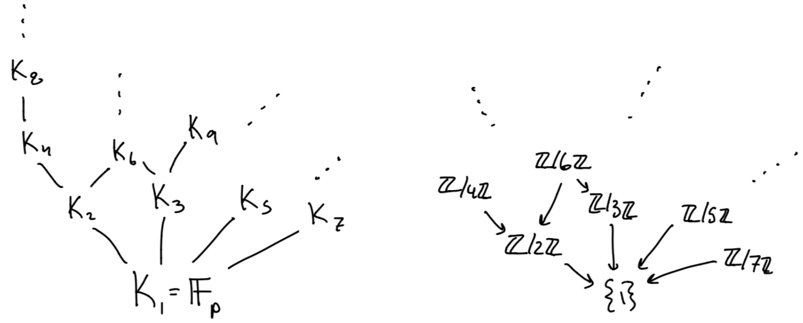
5 Lecture 5 (April 26, 2019): Infinite Galois theory and global class field theory

The topic of today's lecture is **class field theory**. But before diving in, we will start with a motivating question and a review of infinite Galois theory.

Basic Question: What are all finite extensions of a number field K (e.g. $\mathbb{Q}$)?

This is certainly a question of fundamental importance in number theory. One could also ask more specific questions, such as "How many number fields have a given Galois group and discriminant?" For almost every question of this sort, we have no idea what the answer is. Class field theory develops techniques for answering these questions in the abelian setting. We will say more precisely what this means later in the lecture, but for now, let's take a look at an example.

Example 5.1. Let $K = \mathbb{F}_p$, and $\overline{K}$ its algebraic closure. For all $n \geq 1$, there is a unique subfield $K_n \subset \overline{K}$ with p^n elements, and $\overline{K} = \bigcup_{n\geq 1} K_n$. We have the following picture of field extensions and corresponding Galois groups:



Let's calculate $\mathrm{Gal}(\overline{K}/K)$. Because $\overline{K} = \bigcup_{n\geq 1} K_n$, we have an injection

$$\mathrm{Gal}(\overline{K}/K) \hookrightarrow \prod_{n\geq 1} \mathrm{Gal}(K_n/K) = \prod_{n\geq 1} \mathbb{Z}/n\mathbb{Z}.$$

For $\varphi \in \mathrm{Gal}(\overline{K}/K)$, let the sequence (φ_n) be its image in $\prod_{n\geq 1} \mathrm{Gal}(K_n/K)$. A sequence $(\gamma_n) \in \prod_{n\geq 1} \mathrm{Gal}(K_n/K)$ is in the image if and only if $\gamma_n = \gamma_m \mod m$ whenever $m|n$. Hence,

$$\mathrm{Gal}(\overline{K}/K) = \varprojlim \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}$$

is the "profinite completion of $\mathbb{Z}$."

Exercise 5.2. (a) Show that $\widehat{Z} = \prod_{p \text{ prime}} \mathbb{Z}_p$.

(b) Show that $\widehat{\mathbb{Z}}$ has uncountably many subgroups. Hence a naive Galois correspondence cannot hold.

5.1 Infinite Galois theory

Let L/K be a Galois extension (algebraic, normal, separable, not necessarily finite). Then we have an injection

$$\mathrm{Gal}(L/K) \hookrightarrow \prod_{K \subset L' \subset L} \mathrm{Gal}(L'/K),$$

where the product is taken over all towers of field extensions $K \subset L' \subset L$, where the extension L'/K is finite Galois. For all towers of extensions $K \subset L' \subset L'' \subset L$, where the extensions L'/K and L''/K are finite Galois, there is a corresponding map $\mathrm{Gal}(L''/K) \to \mathrm{Gal}(L'/K)$. This determines the image of this injection; that is,

$$\mathrm{Gal}(L/K) = \varprojlim_{K \subset L' \subset L} \mathrm{Gal}(L'/K).$$

This is a topological group. Indeed, if we give $\prod_{K \subset L' \subset L} \mathrm{Gal}(L'/K)$ the product topology (which is compact, by Tychonov), then $\mathrm{Gal}(L/K)$ inherits the subspace topology.

Exercise 5.3. The group $\mathrm{Gal}(L/K)$ is closed (therefore compact) in $\prod_{K \subset L' \subset L} \mathrm{Gal}(L'/K)$.

Example 5.4. We see from Exercise 5.3 and Example 5.1 that the group $\widehat{\mathbb{Z}}$ is compact, which might look strange.

Exercise 5.5. (Important, can be used as a definition) A basis of open neighborhoods of $1 \in \mathrm{Gal}(L/K)$ is given by kernels of the maps

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(L'/L)$$

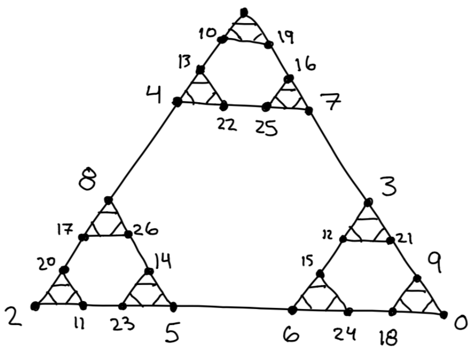
for L'/K finite Galois.

For a general group G, define

$$\widehat{G} = \varprojlim_{\substack{H \subseteq G \\ \text{normal} \\ \text{finite index}}} G/H.$$

The group G is **profinite** if $G \xrightarrow{\sim} \widehat{G}$, otherwise, say $\widehat{G}$ is the **profinite completion** of G. *So Galois groups are profinite groups!* The key example to keep in mind is the following.

Example 5.6. Consider the group $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. What does this group look like? Here's a picture for $p = 3$:



Exercise 5.7. Here are some fun thought experiments.

(a) Where is -1 in this picture?

(b) Think about $\mathbb{Q}_3$.

The motto: Galois groups are fractal-like objects!

Theorem 5.8. (Fundamental theorem of infinite Galois theory) Let L/K be a Galois extension. Then there exists a canonical bijection

$$\begin{aligned} \{K \subset L' \subset L\} &\leftrightarrow \left\{ \begin{array}{c} \text{closed subgroups} \\ \text{of } \mathrm{Gal}(L/K) \end{array} \right\} \\ L^H &\mapsfrom H \\ L' &\mapsto \mathrm{Gal}(L/L') \end{aligned}$$

Moreover, under this bijection,

$$\begin{aligned} \text{finite extensions} &\leftrightarrow \text{closed and open subgroups} \\ \text{Galois extensions} &\leftrightarrow \text{normal subgroups} \end{aligned}$$

Exercise 5.9. Show that the only closed subgroups of $\widehat{\mathbb{Z}}$ are $n\widehat{\mathbb{Z}}$ for $n \in \mathbb{Z}$. If $n \geq 1$, then the subgroup $n\widehat{\mathbb{Z}}$ corresponds to the extension K_n under the bijection above, and $n = 0$ corresponds to $\overline{K}$. (So $0\widehat{Z}$ is the only closed subgroup which isn't open.)

Now we return to the problem posed at the start of this lecture:

Describe all number fields over $\mathbb{Q}$

or, equivalently,

describe all closed subgroups of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$**.**

However, after some thought, one sees that this isn't really a well-defined question (from a philosophical point of view), because $\overline{\mathbb{Q}}$ involves a *choice* (or many choices), so there is no concrete canonical realisation of $\overline{\mathbb{Q}}$. Hence $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is only really a "group up to conjugacy," in the sense that any meaningful statements one can make about this group must be invariant under conjugation. (One cannot talk about individual elements.)

The Punchline:

1. Isomorphism classes of representations of "a group up to conjugacy" are canonical, so it makes sense to talk about representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *This is one reason why representations are so important in the Langlands program!*

2. The maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$ (which is the extension corresponding to $\overline{[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]}$) *is* canonical, and we can hope to describe it by studying the maximal abelian quotient $G^{ab} := G/\overline{[G,G]}$ of $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *This is class field theory!*

5.2 Global class field theory, first version

The key example to keep in mind is the maximal abelian extension of $\mathbb{Q}$.

Example 5.10. Let $K_m := \mathbb{Q}(\zeta_m)$ for $\zeta_m = e^{2\pi i/m}$. Define $\mathbb{Q}(\mu_\infty) := \bigcup_{m\geq 1} K_m$. The Galois group of $K_m/\mathbb{Q}$ is $(\mathbb{Z}/m\mathbb{Z})^\times$, hence

$$\mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) = \varprojlim (\mathbb{Z}/m\mathbb{Z})^\times = \prod_p \mathbb{Z}_p^\times.$$

Fact: ("Kronecker Jugendtraum") $\mathbb{Q}(\mu_\infty)$ is the maximal abelian extension of $\mathbb{Q}$.

This fact is not easy! (It will follow from global class field theory.) The hope of Kronecker was to predict this starting just from $\mathbb{Q}$, without calculating extensions.

Exercise 5.11. Use Kronecker Jugentraum to show that any continuous character $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times$ "is" a Dirichlet character. (Part of the exercise is to work out what "is" means in this context.)

Given a number field K, it is useful to consider all norms at once. Let $\mathbb{O} \subset K$ be the ring of integers. A **place** v is an equivalence class of nontrivial multiplicative norms

$$|\cdot|_v : K \to \mathbb{R}_{\geq 0}$$

on K.

Theorem 5.12. All places of a number field K are of the following form.

- **Finite places:** $|x|_v := (\#\mathbb{O}/\mathfrak{p})^{-\mathrm{val}_\mathfrak{p}(x)}$ for $\mathfrak{p} \subset \mathbb{O}$ prime.
- **Real places:** $|x|_v := |i(x)|$ for some real embedding $i : K \hookrightarrow \mathbb{R}$,
- **Complex places:** $|x|_v := |i(x)|^2$ for some pair of conjugate $i : K \hookrightarrow \mathbb{C}$ not landing in $\mathbb{R}$.

These are all possible notions of distance on a number field.

Exercise 5.13. Show that there are no nontrivial norms on a finite field.

Note that we could have chosen any scalar $\lambda > 1$ in place of $\#\mathbb{O}/\mathfrak{p}$ above. The reason for the the above normalization is the beautiful **product formula**: For $x \in K^\times$,

$$\prod_{\text{places } v} |x|_v = 1.$$

Note that this product makes sense because all but finitely many places are 1. The function field case of this formula is the statement that the number of poles and number of zeros (with multiplicity) agree.

5.3 Global class field theory á la Artin

Fix a finite abelian Galois extension L/K with abelian Galois group $\mathrm{Gal}(L/K)$. Let $\mathbb{O}_L \subset L$ and $\mathbb{O}_K \subset K$ be the rings of integers, and let $S_f \subset \mathbb{O}_K$ be the set of ramified primes. We have seen that for a prime $\mathfrak{p} \subset \mathbb{O}_K$ such that $\mathfrak{p} \notin S_f$, there is a corresponding conjugacy class $\mathrm{Frob}_{\mathrm{p}} \in \mathrm{Gal}(L/K)$. In general $\mathrm{Frob}_{\mathrm{p}}$ is only defined up to conjugacy, but since we are assuming that $\mathrm{Gal}(L/K)$ is abelian, $\mathrm{Frob}_{\mathrm{p}}$ is a single element. Hence we obtain a map (the **Artin map**):

$$\mathcal{J}^{S_f} = \bigoplus_{\mathfrak{p} \notin S_f} \mathbb{Z}\mathfrak{p} \to \mathrm{Gal}(L/K)$$
$$\sum m_{\mathfrak{p}}\mathfrak{p} \mapsto \prod {\mathrm{Frob}_{\mathrm{p}}}^{m_{\mathfrak{p}}}$$

Here $\mathcal{J}^{S_f} \subset \mathcal{J}$ is a subgroup of the group of nonzero fractional ideals $\mathcal{J} = \bigoplus_{\text{primes } \mathfrak{p}} \mathbb{Z}\mathfrak{p}$ discussed in Lecture 2. By Chebotarev's density theorem, the Artin map is surjective.

Question: What is the kernel of the Artin map?

The answer to this question is related to an observation we made in the very first lecture. Recall our motivating problem for the course of determining the number of solutions of a polynomial modulo p for various primes p. For quadratic polynomials, we used quadratic reciprocity to find some modulus $m \in \mathbb{Z}$ such that the number of solutions of the polynomial modulo p was given by the residue of p modulo m. At first, the modulus m seemed to be somewhat mysterious, but eventually we observed that it was obtained from the *ramified primes* (that is, the "weird primes" which we ignored). For example, for the polynomial $x^2 + 1$, which has 2 solutions modulo p if $p = 1 \mod 4$ and 0 solutions if $p = 3 \mod 4$, the modulus 4 is the square of 2, our only ramified prime.

Returning to the setting of the Artin map, we define a **modulus** m supported in a set of places S to be a formal $\mathbb{Z}$-linear combination of places $m = \sum m_i v_i$ such that $m_i \in \{0, 1\}$ for real places and $m_i = 0$ for all complex places and places $v_i \notin S$. Given a modulus m supported in a set of places S, we can define an associated group (the Ray class group) as follows. Consider the following two subsets of $K^\times$:

$$K^S = \{\lambda \in K^\times \mid \mathrm{val}_{\mathfrak{p}}(\lambda) = 0 \text{ for all } \mathfrak{p} \in S\}, \text{ and}$$

$$K^{m,1} = \{\lambda \in K^s \mid \mathrm{val}_{\mathfrak{p}}(\lambda - 1) \geq m_i \text{ for finite places, and } i(\lambda) \in \mathbb{R}^\times_{>0} \text{ for real places } m_i = 1\}.$$

The set $K^{m,1}$ is the set of λ which are "m close to 1." We have the following maps:

$$\begin{tikzcd}
K^\times \arrow[rr, "\mathrm{val}"] \arrow[dr, two heads] & & \mathcal{J} \arrow[r, two heads] & \mathcal{C}\ell_K \\
& \{\text{principal ideals}\} \arrow[ur, hook] & & \\
K^s \arrow[uu, hook] \arrow[rr, "\mathrm{val}"] & & \mathcal{J}^S \arrow[uu, hook] & \\
K^{m,1} \arrow[u, hook] \arrow[urr, "\mathrm{val}"] & & &
\end{tikzcd}$$

The **Ray class group** associated to the modulus m is the quotient

$$\mathcal{C}\ell_K^m := \mathcal{J}^S/\mathrm{val}(K^{m,1}).$$

Example 5.14. If $m = 0$, then $\mathcal{C}\ell_K^0 = \mathcal{C}\ell_K$ is the class group.

Example 5.15. Let $K = \mathbb{Q}$, and $m = n(p)$ for a prime $p \in \mathbb{Z}$. Then m is a modulus supported on $S = \{(p)\}$. We have

$$K^S = \left\{\frac{a}{b} \mid a, b \text{ are coprime to } p\right\} = \mathbb{Z}_{(p)}^\times, \text{ and}$$

$$K^{m,1} = \left\{\frac{a}{b} \mid a, b \text{ coprime to } p \text{ and } \mathrm{val}_p(\frac{a}{b} - 1) \geq n\right\} = \left\{\frac{a}{b} \mid \frac{a}{b} = 1 \mod p^n\right\}.$$

Hence

$$K^s/K^{m,1} = \mathbb{Z}_{(p)}^\times/K^{m,1} = (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathcal{C}\ell_{\mathbb{Q}}^m.$$

Theorem 5.16. For any modulus m, the Ray class group is finite and surjects onto the class group of K.

Theorem 5.17. (Artin) For any L/K as above, there exists a modulus m with $\mathrm{supp}(m) \cap \{\text{finite places}\} = S_f$ such that $\mathrm{val}(K^{m,1})$ is contained in the kernel of the Artin map. Moreover, for any modulus m and any quotient $q : \mathcal{C}\ell_K^m \twoheadrightarrow Q$, there exists an abelian extension L/K ramified only at primes in $\mathrm{supp}(m)$ such that

$$\begin{tikzcd}
\mathcal{C}\ell_K^m \arrow[r, "\text{Artin}"] \arrow[dr, two heads] & \mathrm{Gal}(L/K) \arrow[d, equal] \\
 & Q
\end{tikzcd}$$

commutes.

A weaker form of this theorem provides a more direct answer to our question from the beginning of this section.

Theorem 5.18. For any abelian Galois extension L/K, there exists an $\epsilon > 0$ such that if $\lambda \in K^{S_f}$ is ϵ close to 1 for all places $v \in S$, then $\mathrm{val}(\lambda)$ is in the kernel of the Artin map.

Example 5.19. Consider the extension $\mathbb{Q}(i)/Q$, which is the splitting field of the polynomial $x^2 + 1$. The ramified primes are 2 and ∞ (but we haven't discussed what it means for ∞ to be ramified, so we are sweeping this under the rug), so $S^f = \{(2)\}$. For any $p \neq 2$, $\mathrm{Frob_p}(i) = i^p$, hence in the Galois group, $\mathrm{Frob_p} \leftrightarrow p \mod 4 \in (\mathbb{Z}/4\mathbb{Z})^\times = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. We have

$$\mathcal{J}^{S_f} = \left\{\frac{a}{b} \mid a, b > 0 \text{ coprime to } 2\right\} = \mathbb{Z}_{(2),>0}^\times.$$

Hence the Artin map is the natural map

$$\mathbb{Z}_{(2),>0}^\times \to \big(\mathbb{Z}/4\mathbb{Z}\big)^\times.$$

Its kernel is the set of all elements satisfying a "congruence condition at 2:"

$$\Big\{\lambda \in \mathbb{Z}_{(2),>0}^\times \mid \mathrm{val}_2(\lambda - 1) \geq 2\Big\}.$$

We see from this example that the finitely many "weird" (ramified) primes from the first lecture are the primes determining our congruences.

Example 5.20. If $m = 0$, then $\mathcal{C}\ell_K^0 = \mathcal{C}\ell_K$. Hence the existence statement in Theorem 5.17 implies that there exists an unramified everywhere extension L/K with $\mathrm{Gal}(L/K) = \mathcal{C}\ell_K$. This extension is the **Hilbert class field**.

5.4 Solutions to exercises

Exercise 5.2.

(a) Show that $\widehat{Z} = \prod_{p \text{ prime}} \mathbb{Z}_p$.

(b) Show that $\widehat{\mathbb{Z}}$ has uncountably many subgroups. Hence a naive Galois correspondence cannot hold.

Exercise 5.3. Let L/K be a (not necessarily finite) Galois extensions. Show that the group $\mathrm{Gal}(L/K)$ is closed (therefore compact) in $\prod_{K \subset L' \subset L} \mathrm{Gal}(L'/K)$.

Exercise 5.4. Let L/K be a Galois extension. Show that a basis of open neighborhoods of $1 \in \mathrm{Gal}(L/K)$ is given by kernels of the maps

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(L'/L)$$

for L'/K finite Galois.

Exercise 5.10. Use Kronecker Jugentraum to show that any continuous character $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times$ "is" a Dirichlet character. (Part of the exercise is to work out what "is" means in this context.)

Exercise 5.12 Show that there are no nontrivial norms on a finite field.

6 Lecture 6 (May 3, 2019): Structure of local Galois groups, local class field theory

Sometimes if we find something difficult, it can be comforting to know that other people also found it difficult. Accordingly, we'll start today's lecture with a potted history of class field theory, following [Con01, Miy11].

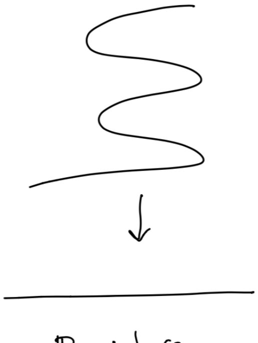
- **Kronecker, Weber (1850-1880)**: Kronecker's Jugentraum (that $\mathbb{Q}(\mu_\infty)$ is the maximal abelian extension of $\mathbb{Q}$), explicit class field theory (describing K^{ab} explicitly, not just its Galois group) for $\mathbb{Q}$ and $\mathbb{Q}(i)$, relevance of complex multiplication.
- **Dedekind, Frobenius (1880)**: defined $\mathrm{Frob}_{\mathrm{p}}$ (then everyone promptly forgot for 40 years).
- **Hilbert (189-1900)**: first correct proof of Jugentraum for $\mathbb{Q}$, emphasis on "places at ∞," introduction of Hilbert class field, 12^{th} problem on Hilbert's list was explicit class field theory for any K. (Still open! Even for $\mathbb{Q}(\sqrt{d}), d \geq 0$!)
- **Hensel (1897)**: introduction of p-adic numbers, took a while to catch on.
- **Takagi (1900)**: PhD student of Hilbert in Göttingen, thesis on $\mathbb{Q}(i)^{ab}$, proof of existence theorem during WWI (when there was no contact between Germany and Japan), result announced at the ICM in 1920.
- **Hasse (1922)**: local global principle, first time p-adics were taken seriously by the broader mathematics community.
- **Chebotarev (1927)**: density theorem.
- **E. Artin (1927)**: introduction of Artin map (the return of $\mathrm{Frob}_{\mathrm{p}}$!), reciprocity theorem.
- **Schmidt (1930)**: deduced local class field theory from global class field theory (proofs still analytic).
- **E. Noether (1930s)**: local theory should be simpler and come first
- **Chevalley (1940)**: algebraic proof of local class field theory

6.1 Motivating local class field theory: A trip across the bridge

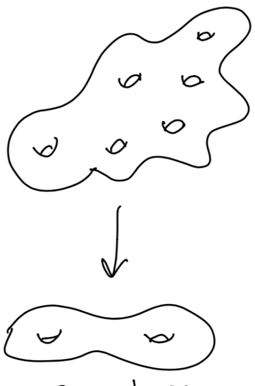
Recall that the "bridge" in this course is the motivating analogy between number fields and function fields.

Remark 6.1. This bridge was what motivated Hensel's advocation for the introduction of the p-adic numbers.

Let's look at local class field theory through this analogy. Let L/K be a finite Galois extension. Across the bridge, this should correspond to a surjective map (i.e. ramified cover) $f : X \to Y$ of algebraic curves/Riemann surfaces over $\mathbb{C}$. Recall that our $\mathbb{R}$-picture and $\mathbb{C}$-picture of such a map are the following:

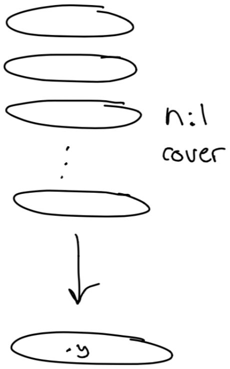


$\mathbb{R}$-picture

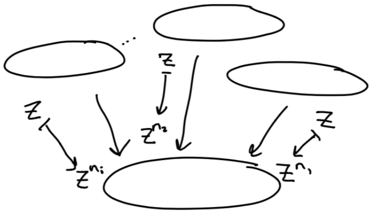


$\mathbb{C}$-picture

For all $y \in Y$ outside of a finite set, f is étale; that is, a smooth $n : 1$ cover in a neighborhood of y:



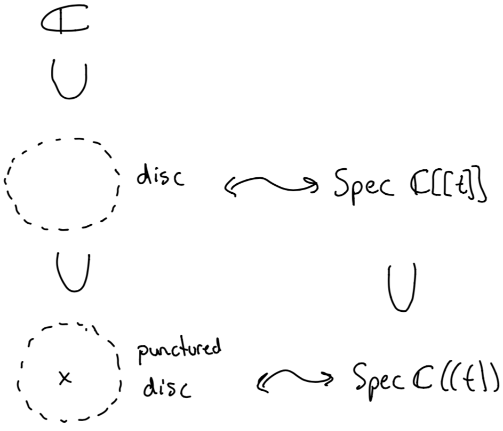
For a finite set of points $y \in Y$, f is not smooth, and locally sends $z \mapsto z^{n_i}$, such that $\sum n_i = n$:



If f is Galois, then all n_i are equal.

The Moral: The ramified cover f is determined by simple data ("local monodromies") at finitely many points ("ramified primes of Y").

Remark 6.2. We have



The algebraic closure of $\mathbb{C}((t))$ is $\mathbb{C}((t^{\mathbb{Q}})) := \bigcup\limits_{n\geq 1} \mathbb{C}((t^{1/n}))$. Hence,

$$\operatorname{Gal}\left(\overline{\mathbb{C}((t))}/\mathbb{C}((t))\right) = \lim_{\leftarrow} \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}.$$

This is "why" the local field information is so simple in function field/$\mathbb{C}$ case[1]. In language to come, every extension of $\mathbb{C}((t))$ is "tamely ramified."

The upshot is that on the function field side of the bridge, local information is easy, and can be patched together to form the global picture. On the number field side of the bridge, local information is much harder, but the philosophy we learn from our analogy is that it should still be easier than global information, so we should focus on it first. Because of this, essentially the rest of this course will be local.

Now we return to number fields. Let L/K be a finite Galois extension. Fix a place v of K. If v is finite (corresponding to some $\mathfrak{p} \subset \mathbb{O}_k$), then we know what it means for a place v' (corresponding to $\mathfrak{q} \subset \mathbb{O}_L$) of L to "lie over v:" v' lies over v precisely when $\mathfrak{q}$ is a prime above $\mathfrak{p}$ in the sense of lecture 2 (i.e. $\mathfrak{p}\mathbb{O}_L \subset \mathfrak{q}$).

If v is a real or complex place corresponding to $i : K \hookrightarrow \mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$, then a place v' of L **lies over** v if the corresponding injection i' fits into a commutative diagram

$$\begin{tikzcd}
L \arrow[r, hook, "i'"] \arrow[d, dash] & \mathbb{K}' \arrow[d, dash] \\
K \arrow[r, hook, "i"] & \mathbb{K}
\end{tikzcd}.$$

[1] Recall that we saw last lecture that $\operatorname{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \widehat{\mathbb{Z}}$ as well. This turns out to be a useful coincidence, but we won't comment on it further here.

Hence if v is real, then v' is either real or complex. A real place v is **ramified** if there exists a v' lying above v that is complex in L, and **unramified** if all v' above v are real. If v is complex, then all v' above v are complex, and we say the place v is **unramified**.

Fix a place v of K and a place v' of L over v. Let $L_{v'}$ (resp. K_v) be the completion of L (resp. K) with respect to the place v' (resp. v). Then we have the diagram

$$\begin{tikzcd}
L \arrow[r, hook] \arrow[d, dash] & L_{v'} \arrow[d, dash] \\
K \arrow[r, hook] & K_v
\end{tikzcd} .$$

Set

$$\begin{aligned} G_v &= \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma \text{ acts continuously on } L_v\} \\ &= \{\sigma \mid \sigma \text{ preserves } v'\} = \begin{cases} G_{\mathfrak{q}} & \text{if } v \text{ is finite} \\ \{1\} & \text{if } v \text{ is unramified infinite} \\ \mathbb{Z}/2\mathbb{Z} & \text{if } v \text{ is ramified infinite} \end{cases} . \end{aligned}$$

Here $G_{\mathfrak{q}} \subset \mathrm{Gal}(L/K)$ is the decomposition group corresponding to the prime $\mathfrak{q} \subset \mathbb{O}_L$ determining v'.

Remark 6.3. In the last case (when v is ramified infinite), we get a canonical element $c \in \mathrm{Gal}(L/K)$ corresponding to complex conjugation.

The point: $L_{v'}/K_v$ is a finite Galois extension of local fields with Galois group G_v. We will first try to understand such extensions for all places v, then piece together this information to understand L/K.

6.2 Local class field theory

Between the "easy" world of finite fields and the complicated world of global fields lies the world of local fields. Let K be a field equipped with discrete valuation val : $K \to \mathbb{Z} \cup \{\infty\}$. In K lies its ring of integers $\mathbb{O}_K$, with maximal idea $\mathfrak{m}$ generated by a "uniformizer" $\pi \in \mathfrak{m}$:

$$K \supset \mathbb{O}_K = \mathrm{val}^{-1}(\mathbb{Z}_{\geq 0} \cup \{\infty\}) \supset \mathfrak{m} = \mathrm{val}^{-1}(\mathbb{Z}_{>0} \cup \{\infty\}) = (\pi).$$

The field $k_K = \mathbb{O}_K/\mathfrak{m}$ is the residue field. Note that in this setup, K, $\mathbb{O}_K$ and $\mathfrak{m}$ are all canonical, but the uniformizer $\pi \in \mathfrak{m}$ isn't. For us, a **local field** will be a field K equipped with a discrete valuation as above such that

1. K is complete with respect to val (i.e. K has the topology coming from $\mathbb{O}_K = \varprojlim \mathbb{O}_K/\mathfrak{m}_K^n$), and

2. k_K is finite.

Exercise 6.4. Show that 1. and 2. are equivalent to K being locally compact.

Example 6.5. The field $\mathbb{Q}_p$ is locally compact because it is covered by dilates of $\mathbb{Z}_p$:

$$\mathbb{Q}_p = \bigcup_{n \geq 1} p^{-n}\mathbb{Z}_p.$$

Recall that $\mathbb{Z}_p$ are compact open sets in $\mathbb{Q}_p$.

Remark 6.6. In some terminology, $\mathbb{R}$ and $\mathbb{C}$ are also referred to as local fields.

Let L/K be a finite Galois extension of local fields. Then any element $\sigma \in \mathrm{Gal}(L/K)$ preserves $\mathbb{O}_L/\mathbb{O}_K$ and $\mathfrak{m}_L/\mathfrak{m}_K$, and thus acts on k_L/k_K. Hence we get maps

$$1 \to I_{L/k} \hookrightarrow \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(k_L/k_K) \to 1,$$

where $I_{L/K}$ is the inertia subgroup of lecture 2. The Galois group $\mathrm{Gal}(k_L/k_K) \simeq \mathbb{Z}/d\mathbb{Z}$ is generated by Frob_q. For $L = \overline{K}$, this short exact sequence becomes

$$1 \to I_{\overline{K}/K} \hookrightarrow \mathrm{Gal}(\overline{K}/K) \twoheadrightarrow \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \simeq \widehat{\mathbb{Z}} \to 1.$$

Local class field theory: There exists a canonical map[2] $r_K : K^\times \to \mathrm{Gal}(\overline{K}/K)^{ab}$ with dense image such that r_K induces an isomorphism $\widehat{K^\times} \xrightarrow{\sim} \mathrm{Gal}(\overline{K}/K)^{ab}$. Here $\widehat{K^\times}$ is the profinite completion of $K^\times$ (that is, the completion with respect to subgroups of finite index). Moreover,

1. the diagram

$$\begin{tikzcd}
1 \arrow[r] & I^{ab}_{\overline{K}/K} \arrow[r, hook] \arrow[d, equal] & \mathrm{Gal}(\overline{K}/K)^{ab} \arrow[r, two heads] & \mathrm{Gal}(\overline{k_K}/k_K) \simeq \widehat{\mathbb{Z}} \\
1 \arrow[r] & \mathbb{O}_K^\times \arrow[r, hook] & K^\times \arrow[r, "\mathrm{val}"] \arrow[u, "r_K"] & \mathbb{Z} \arrow[u]
\end{tikzcd}$$

   commutes, and

2. if L/K is finite Galois, then

$$\begin{tikzcd}
L^\times \arrow[r, "r_L"] \arrow[d, "\mathrm{Norm}_{L/K}"] & \mathrm{Gal}(\overline{L}/L)^{ab} \arrow[d, "\mathrm{res}"] \\
K^\times \arrow[r, "r_K"] & \mathrm{Gal}(\overline{L}/K)^{ab}
\end{tikzcd}$$

   commutes.

Remark 6.7. The analogous statements for the fields $\mathbb{R}$ and $\mathbb{C}((t))$ are the following:

[2] The canonical map r_K is sometimes called the "reciprocity map."

1. $K = \mathbb{R}$**:** In the diagram

$$\begin{tikzcd}
\mathbb{C}^\times \arrow[r, "r_{\mathbb{C}}"] \arrow[d, "\mathrm{Norm}_{\mathbb{C}/\mathbb{R}}"] & \mathrm{Gal}(\mathbb{C}/\mathbb{C}) = \{1\} \arrow[d] \\
\mathbb{R}^\times \arrow[r, "r_{\mathbb{R}}"] & \mathrm{Gal}(\mathbb{C}/\mathbb{R})
\end{tikzcd},$$

the map $r_{\mathbb{R}} : -1 \mapsto$ complex conjugation is continuous and surjective. The kernel of $r_{\mathbb{R}}$ is $\mathbb{R}^\times_{>0}$, the set of norms coming from $\mathbb{C}^\times$ (i.e. the image of $\mathrm{Norm}_{\mathbb{C}/\mathbb{R}}$).

2. $K = \mathbb{C}((t))$**:**[3] The map

$$r_{\mathbb{C}((t))} : \mathbb{C}((t))^\times \to \mathrm{Gal}\left(\overline{\mathbb{C}((t))}/\mathbb{C}((t))\right) = \widehat{\mathbb{Z}}$$

has dense image, so a reasonable choice is valuation $\mathrm{val} : \mathbb{C}((t))^\times \to \mathbb{Z}$.

It is useful to modify the Galois group $\mathrm{Gal}(\overline{K}/K)$ slightly. Define the **Weil group** of K to be the subgroup $W_K \subset \mathrm{Gal}(\overline{K}/K)$ of elements whose projection onto $\widehat{\mathbb{Z}}$ is an integral power of Frob_q; that is, W fits into the short exact sequence

$$\begin{tikzcd}
I_{\overline{K}/K} \arrow[r, hook] \arrow[d, equal] & W_K \arrow[r, two heads] \arrow[d, hook] & \mathbb{Z} \arrow[d, hook] \\
I_{\overline{K}/K} \arrow[r, hook] & \mathrm{Gal}(\overline{K}/K) \arrow[r, two heads] & \widehat{\mathbb{Z}}
\end{tikzcd}.$$

The purpose for this modification of the following fact: the reciprocity map r_K provides an isomorphism between $K^\times$ and the abelianization of the Weil group:

$$r_K : K^\times \xrightarrow{\simeq} W_K^{ab}.$$

With this, we can state the local Langlands correspondence for $GL_n(K)$.

Theorem 6.8. (**Local Langlands correspondence for** $GL_n(K)$) (Harris-Taylor) There is a bijection

$$\mathrm{Hom}_{cts}(W_K, GL_n(\mathbb{C}))/_{\mathrm{conj}} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{c} \text{irreps of } GL_n(K) \\ \text{in } \mathbb{C}\text{-vector spaces} \end{array} \right\}.$$

The continuous group homomorphisms on the left hand side of this bijection are referred to as the **Langlands parameters** of the corresponding $GL_n(K)$-representations on the right.

Remark 6.9. Actually, this is not quite correct. Instead we will consider should consider Weil-Deligne reps on the left, and smooth admissible reps on the right. These issues will be addressed in coming lectures.

[3] Note that K doesn't quite fit our assumptions so LCFT doesn't apply, but morally it fits into the same picture.

Example 6.10. The $n = 1$ case of this theorem is true by local class field theory:

$$\begin{aligned}\mathrm{Hom}_{cts}(W_K, GL_1(\mathbb{C}))/_{\mathrm{conj}} &= \mathrm{Hom}_{cts}(W_K, \mathbb{C}^\times)\\ &= \mathrm{Hom}_{cts}(W_K^{ab}, \mathbb{C}^\times)\\ &= \mathrm{Hom}_{cts}(K^\times, \mathbb{C}^\times)\\ &= \{\text{irreps of } GL_1(K)\}.\end{aligned}$$

Example 6.11. We can see explicitly that local class field theory is true for $\mathbb{Q}_p$. By a local version of the Jugentraum,

$$\mathbb{Q}_p^{ab} = \mathbb{Q}_p(\mu_\infty) = \bigcup \mathbb{Q}_p(\zeta_n),$$

where ζ_n is an n^{th} root of unity. Hence

$$\mathbb{Q}_p^{ab} = \mathbb{Q}_p(\mu_{p'}) \cdot \mathbb{Q}_p(\mu_{p^\infty}),$$

where $\mathbb{Q}_p(\mu_{p'}) := \bigcup_{p\nmid n} \mathbb{Q}_p(\zeta_n)$ and $\mathbb{Q}_p(\mu_{p^\infty}) := \bigcup_{n\geq 1} \mathbb{Q}_p(\zeta_{p^n})$. As before, $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) = (\mathbb{Z}/p^n\mathbb{Z})^\times$, so

$$\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) = \mathbb{Z}_p^\times.$$

If $p \nmid n$, note that $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ is unramified, so $\mathbb{Q}(\mu_{p'}) =: \mathbb{Q}_p^{ur}$ is the maximal unramified extension of $\mathbb{Q}_p$. Because $\overline{\mathbb{F}_p} = \bigcup_{p\nmid n} \mathbb{F}_p(\zeta_n)$, we have that

$$\mathrm{Gal}(\mathbb{Q}_p(\mu_{p'})/\mathbb{Q}_p) = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \widehat{\mathbb{Z}}.$$

We conclude that

$$\mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p) = \widehat{\mathbb{Z}} \times \mathbb{Z}_p^\times \simeq \widehat{\mathbb{Q}}_p^\times,$$

which is exactly what is predicted by local class field theory.

6.3 Structure of Galois groups of local fields

We'll finish this lecture with some remarks on the structure of local Galois groups. This section is hands-on and explicit. Morally, it should come before local class field theory.

Let L/K be a finite Galois extension of local fields, and $L \supset \mathbb{O}_L \supset \mathfrak{m}_L = (\pi_L)$, $K \supset \mathbb{O}_K \supset \mathfrak{m}_K = (\pi_K)$ the respective rings of integers, maximal ideals, and uniformizers. As before, there is a corresponding extension of residue fields k_L/k_K. We have a short exact sequence

$$1 \to I_{L/K} \to \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(k_L/k_K) \simeq \mathbb{Z}/n\mathbb{Z} \to 1,$$

where $I_{L/K} = \{\sigma \mid \sigma \text{ acts trivially on } k_L\}$, and $\mathrm{Gal}(k_L/k_K)$ is generated by the canonical generator Frob. Note that $\mathrm{Gal}(L/K)$ preserves $\mathbb{O}_K$, hence $\mathfrak{m}_K$, hence the valuation v_K, hence acts on $\mathbb{O}_K/\mathfrak{m}_K^j$, hence acts continuously on L.

Lemma 6.12. (Key lemma) Any $\sigma \in I_{K/L}$ is determined by its action on π_L.

Exercise 6.13. Prove Lemma 6.12. (Hint: use the fact that any $\sigma \in \mathrm{Gal}(L/K)$ is automatically continuous.)

Set $I := I_{L/K}$, $I_0 := I$, and $I_j := \{\sigma \in I \mid \sigma(\pi)\pi^{-1} \in 1 + \mathfrak{m}_L^j\}$ for $j \geq 1$.

Proposition 6.14. This defines a filtration

$$I = I_0 \supset I_1 \supset I_2 \supset \cdots$$

of I by normal subgroups. Moreover,

1. This is a finite filtration; i.e. $I_m = \{1\}$ for large enough m.

2. We have natural injections

$$\begin{aligned} I_0/I_1 &\xhookrightarrow{\sigma(\pi)\pi^{-1}} k_L^\times, \\ I_j/I_{j+1} &\xhookrightarrow{\qquad} (1 + \mathfrak{m}_L^j)/(1 + \mathfrak{m}_L^{j+1}) \simeq k_L \end{aligned}$$

   for $j \geq 1$. In particular, I is solvable, I_0/I_1 is of order prime to p, and I_1 is the Sylow p subgroup of I.

This filtration is called the **ramification filtration of** I. The proof is an easy exercise.

Definition 6.15. We say that L/K is **tamely ramified** if $I_1 = \{1\}$, and L/K is **unramified**[4] if $I_0 = \{1\}$.

Remark 6.16. This agrees with our earlier notion of unramified from Lecture 2.

6.4 Solutions to exercises

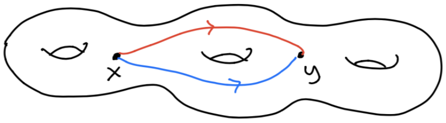
Exercise 6.4. Show that 1. and 2. are equivalent to K being locally compact.

Exercise 6.12. Prove Lemma 6.12. (Hint: use the fact that any $\sigma \in \mathrm{Gal}(L/K)$ is automatically continuous.)

[4] Note that a quirk of this terminology is that unramified is tamely ramified. It's strange, but we'll just have to get used to it.

7 Lecture 7 (May 14, 2019): Heuristic derivation of local Langlands for GL_2; basic representation theory of p-adic groups

We'll start today's lecture by tying up some lose ends from previous weeks. Recall that two lectures ago, we discussed how looking for a description of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is misguided because $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is only a "group up to conjugacy," since its definition requires a choice of $\overline{\mathbb{Q}}$. There's an analogy for this idea that Geordie learned from Kevin Buzzard which might be more familiar to us. Let X be a path-connected space. A choice of base point $x \in X$ yields the fundamental group $\pi_1(X, x)$. Another choice of base point $y \in X$ yields the isomorphic group $\pi_1(X, y)$.



An isomorphism $\pi_1(X, x) \simeq \pi(X, y)$ requires a choice of path from x to y in X. Such a choice of path is *not canonical.* Grothendieck taught us an analogue of this for extensions of fields.

$$\mathbb{Q} \leftrightarrow \text{“étale site” } \operatorname{Spec}\mathbb{Q} \text{ (something like a space)}$$
$$\text{choice of } \overline{\mathbb{Q}} \leftrightarrow \text{choice of “base point” of } \operatorname{Spec}\mathbb{Q}$$

Then the étale fundamental group $\pi_1^{\acute{e}t}(\operatorname{Spec}\mathbb{Q}, \mathbb{Q}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

The punchline: The fundamental group $\pi_1(X, x)$ depends on base point x, but $\operatorname{Rep}\pi_1(X, x) \simeq \{\text{local systems on } X\}$ is canonical! Transporting this statement via Grothendieck's analogy we see that, although the absolute Galois group is not defined canonically, its category of (continuous) representations is. It is this category that the Langlands correspondence tries to understand.

Last lecture we stated the **local Langlands correspondence for GL_n**: Fix a local field K (i.e. K is a finite extension of $\mathbb{Q}_p$ or $K \simeq \mathbb{F}_q((t))$). There is a canonical bijection

$$\left\{ \begin{array}{c} \text{cts reps of } W_K \\ \text{in } GL_n(\mathbb{C}) \end{array} \right\}_{/\text{iso}} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{c} \text{irred blah} \\ \text{reps of } GL_n(K) \end{array} \right\}_{/\text{iso}}.$$

Here W_K is the **Weil group** of the field K. Last week we showed why this follows from local class field theory for $n = 1$. However, this statement is not quite precise. On the left hand side we need to consider **Weil-Deligne representations** of W_K, and on the right hand side we need to establish exactly what conditions are captured by "blah." We'll keep stating versions of this theorem every lecture until we converge on something correct.

Our final piece of housekeeping is the **no small subgroups argument**. This is a very useful fact that hasn't fit in naturally to our story so far, so we'll slot it in here.

Definition 7.1. A topological group G has **no small subgroups** if there exists a neighborhood U of the identity in G such that any subgroup contained in U is trivial.

Example 7.2. Here are some examples of groups with no small subgroups.

1. The circle group S^1.

2. Discrete groups (e.g. finite groups). We can take $U = \{id\}$.

3. The real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$. (Powers of any non-identity element move far away from the identity.)

4. Any Lie group G. (Use that $\exp : \operatorname{Lie} G \to G$ is a local diffeomorphism and $\exp(mg) = \exp(g)^m$.)

5. Any topological subgroup of a group with no small subgroups has no small subgroups (e.g. $\mathbb{Q}/\mathbb{Z} \hookrightarrow S^1$ has no small subgroups).

Remark 7.3. In contrast, profinite groups have "many small subgroups," because because a basis of neighbourhoods of the identity consists of subgroups of finite index.

Lemma 7.4. Let Γ be a profinite group and G a topological group with no small subgroups. Then any continuous group homomorphism $\varphi : \Gamma \to G$ has finite image.

Proof. Let $U \subset G$ be an open neighborhood of the identity containing no nontrivial subgroups, and let $\varphi : \Gamma \to G$ be a continuous group homomorphism. Then $\varphi^{-1}(U) \subset \Gamma$ is open. Since Γ is profinite, there exists a normal subgroup $N \subset \varphi^{-1}(U)$ such that G/N is finite. The image $\varphi(N) \subset U$ is a subgroup, so $\varphi(N) = \{1\}$ since G has no small subgroups. Hence Γ factors through a finite group, $\varphi : \Gamma \to \Gamma/N \to G$. □

The Moral:

$$\left\{ \begin{array}{c} \text{Fractal-like objects} \\ (p\text{-adic groups, Galois groups}) \end{array} \right\} \cap \left\{ \begin{array}{c} \text{Euclidean-type objects} \\ \text{(Lie groups)} \end{array} \right\} = \{\text{finite groups}\}$$

A consequence of this is that we cannot draw any good pictures of $\mathbb{Z}_p$ in $\mathbb{C}$ (or for that matter in any Lie group)which respect the addition or multiplication structure.

This moral gives us a new perspective of the local Langlands correspondence. The "no small subgroups" lemma implies that the left hand side of the LLC consists (roughly) of a collection of finite subgroups of $GL_n(\mathbb{C})$, along with surjections from a Galois-group-type object to the subgroups. So very roughly, the LLC provides a classification of irreducible admissible representations of a Lie group over a local field by certain finite subgroups of $GL_n(\mathbb{C})$.

7.1 You could have guessed the LLC for GL_2!

The goal is this section is to give a heuristic explanation for the LLC. Warning: this is not precise! Everything we say here will have to be tweaked later. Geordie learned this perspecive from a series of lectures by Dipendra Prasad in Russia.

Starting place: Say we wanted to guess the representation theory of $GL_n(\mathbb{Q}_p)$. What would we do?

Step 1: We might start by figuring out the representation theory of finite reductive groups. For example, let $G = SL_2(\mathbb{F}_q)$. There are two maximal tori in G, up to conjugacy:

$$T_s = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_q^\times \right\} \simeq \mathbb{Z}/(q-1)\mathbb{Z}, \text{ the “split torus,” and}$$

$$T_a = \{\lambda \in \mathbb{F}_{q^2}^\times \subset GL_2(\mathbb{F}_q) \mid \mathrm{Norm}(\lambda) = 1\} \simeq \mathbb{Z}/(q+1)\mathbb{Z}, \text{ the “anisotropic torus.”}$$

In the definition of T_a above, we are using the fact that $GL_2(\mathbb{F}_q)$ is the group of invertible linear transformations of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^2$, so

$$\mathbb{F}_{q^2}^\times \subset GL_{\mathbb{F}_q}(\mathbb{F}_q^2) = GL_2(\mathbb{F}_q).$$

Roughly,

$$\left\{ \begin{matrix} \text{irred reps of} \\ SL_2(\mathbb{F}_q) \text{ over } \mathbb{C} \end{matrix} \right\} \overset{1:1}{\longleftrightarrow} \underset{\text{“principal series”}}{\{\chi : T_s \to \mathbb{C}^\times\}_{/\chi \sim \chi^{-1}}} \bigsqcup \underset{\text{“discrete series”}}{\{\theta : T_a \to \mathbb{C}^\times\}_{/\theta \sim \theta^{-1}}}$$

Let us check that we're not too far off by doing a count. Irreducible representations of a finite group are in bijection with conjugacy classes, and conjucagy classes are roughly in bijection with characteristic polynomials, so the sizes of the sets above are roughly

$$\begin{matrix} \# \text{ characteristic polynomials} \\ \text{of elements in } SL_2(\mathbb{F}_q) \end{matrix} = |\{x^2 + ax + 1 \mid a \in \mathbb{F}_q\}| = q = \frac{q-1}{2} + \frac{q+1}{2}.$$

For more details and a careful construction of the irreducible representation of $SL_2(\mathbb{F}_q)$, see the notes from Joe Baine's talks on the Informal Friday Seminar webpage. The upshot is that we obtain almost all irreducible representations of $SL_2(\mathbb{F}_q)$ through some “induction” from characters of the two conjugacy classes of tori. (Note that the details are much more complicated as there is no actual induction functor. In the setting of finite reductive groups we use Deligne-Lusztig induction.)

Step 2: Once we had a good idea of the representation theory of finite reductive groups, a next natural step might be to understand the representation theory of real reductive groups. For example, let $G = SL_2(\mathbb{R})$. Again, there are two conjugacy classes of maximal tori: the “split torus”

$$T_s = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{R}^\times \right\} \simeq \mathbb{R}^\times,$$

and the "anisotropic torus"

$$T_a = \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \right\} \simeq SO_2.$$

Something similar happens in this setting to what we saw with the finite reductive groups. Roughly,

$$\left\{ \begin{matrix} \text{irred admissible} \\ \text{reps of } SL_2(\mathbb{R}) \end{matrix} \right\} \overset{1:1}{\longleftrightarrow} \underset{\text{"principal series"}}{\left\{ \begin{matrix} \text{cts characters} \\ \text{of } T_s \simeq \mathbb{R} \times \mathbb{Z}/2\mathbb{Z} \end{matrix} \right\}} \bigsqcup \underset{\text{"discrete series"}}{\left\{ \begin{matrix} \text{cts characters} \\ \text{of } T_a \simeq SO_2 \simeq S^1 \end{matrix} \right\}}$$

So again we see that roughly, irreducible representations are all obtained by "inducing" characters of conjugacy classes of tori.

Step 3: We dream that something similar might be true for representations of p-adic groups. Let $G = GL_2(K)$ for a local field K. By descent, we have the following relationship:

$$\left\{ \begin{matrix} \text{conjugacy classes of} \\ \text{max'l tori in } GL_2(K) \end{matrix} \right\} \leftrightarrow \left\{ \begin{matrix} \text{semisimple } K\text{-algebras} \\ L \text{ s.t. } \dim_K L = 2 \end{matrix} \right\}$$
$$L^\times \leftrightarrow L$$

There are two cases:

1. Split torus: $L \simeq K \times K$, so maximal torus is of the form $L^\times \simeq K^\times \times K^\times$.
2. Anisotropic torus: L/K degree 2 extension, so maximal torus is of the form $L^\times$.

Applying our analogy from earlier, we might expect

$$\left\{ \begin{matrix} \text{irred blah} \\ \text{reps of } GL_2(K) \end{matrix} \right\} \xleftrightarrow{\text{roughly 1:1}} \left\{ \begin{matrix} \text{pairs of characters} \\ \chi_1, \chi_2 : K^\times \to \mathbb{C}^\times \end{matrix} \right\} \bigsqcup \left\{ \begin{matrix} \text{characters } \theta : L^\times \to \mathbb{C}^\times \\ \text{where } L/K \text{ is degree 2} \end{matrix} \right\}.$$

Now, local class field theory tells us that $W_K^{ab} \simeq K^\times$ and $W_L^{ab} \simeq L^\times$. Moreover, $W_L \subset W_K$ is an index 2 subgroup, so

$$\left\{ \begin{matrix} \text{irred blah} \\ \text{reps of } GL_2(K) \end{matrix} \right\} \xleftrightarrow{\text{roughly 1:1}} \{\chi_1 \otimes \chi_2 : W_K \to GL_2(\mathbb{C})\} \sqcup \left\{\operatorname{Ind}_{W_L}^{W_K}(\theta) : W_L \to GL_2(\mathbb{C})\right\}.$$

It turns out that our dream is a reality:

Fact: If $p \neq 2$, all continuous representations of W_K are either of the form $\chi_1 \otimes \chi_2$ or $\operatorname{Ind}_{W_L}^{W_K}(\theta)$ as above.

So we guessed LLC for $GL_2(K)$! Though again, let us emphasize that this is not actually the correct version of the correspondence (it is for example not compatible with taking duals). However it won't take too much effort to make this into a correct statement next lecture.

Remark 7.5. For $p = 2$, the matching still works, but there are more objects on both sides.

7.2 Basic representation theory of p-adic groups

Let K be a local field. Then $GL_n(K)$ is a topological group, with a basis of open neighborhoods of id given by

$$K_j = \{g \in GL_n(\mathbb{O}_K) \mid g = id \mod \mathfrak{m}_K^j\}.$$

Note that $GL_n(\mathbb{O}_K)/K_j \simeq GL_n(\mathbb{O}_K/\mathfrak{m}_K^j)$ is a finite group.

For example, if $K = \mathbb{Q}_p$, we have a natural surjective map

$$GL_n(\mathbb{Q}_p) \supset GL_n(\mathbb{Z}_p) \xrightarrow{\varphi_j} GL_n(\mathbb{Z}/p^j\mathbb{Z})$$

for all $j \in \mathbb{Z}_{:} \geq 0$, and $K_j = \varphi_j^{-1}(id)$.

Remark 7.6.
1. $K_j \subset K_0$ is normal.
2. K_0 is a maximal compact subgroup.

Exercise 7.7. Let $\pi \in \mathbb{O}_K \subset K$ be a uniformizer.

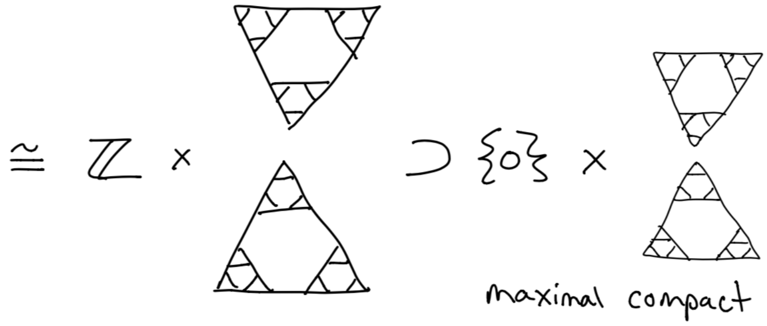
1. Establish the Bruhat decomposition:

$$GL_n(K) = \bigsqcup_{\substack{\lambda_1 \geq \lambda_2 \ldots \geq \lambda_n \\ \lambda_i \in \mathbb{Z}}} GL_n(\mathbb{O}_K) \begin{pmatrix} \pi^{\lambda_1} & & & & \\ & \pi^{\lambda_2} & & & \\ & & \pi^{\lambda_3} & & \\ & & & \cdots & \\ & & & & \pi^{\lambda_n} \end{pmatrix} GL_n(\mathbb{O}_K) \quad (*)$$

(*Hint: Gaussian elimination.*)

2. Use $(*)$ to classify the subgroups $GL_n(\mathbb{O}_K) \subset H \subset GL_n(K)$.
3. Hence or otherwise, show that $GL_n(\mathbb{O}_K)$ is a maximal compact subgroup of $GL_n(K)$.

Example 7.8. Consider $GL_1(\mathbb{Q}_3) = \mathbb{Q}_3^\times = \mathbb{Z} \times \mathbb{Z}_3^\times$. Recall our picture of the 3-adics from Example 5.6. A picture of the maximal compact subgroup K_0 of this group is:



A space is **totally disconnected** if every point admits a family of compact open neighborhoods; e.g. $GL_n(K)$ is totally disconnected because each K_j is compact open. Let G be a totally disconnected topological group and V a vector space over a field $\mathbb{K}$ of characteristic 0. We give V the discrete topology.

Definition 7.9. A representation $\rho : G \to GL(V)$ is

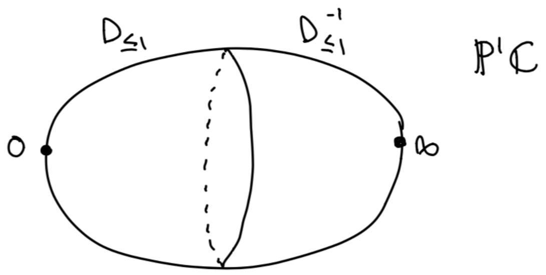
1. **smooth** if for all $v \in V$, $\operatorname{stab}_G v$ is open, and
2. **admissible** if for all open $K \subset G$, V^K is finite dimensional.

Example 7.10.

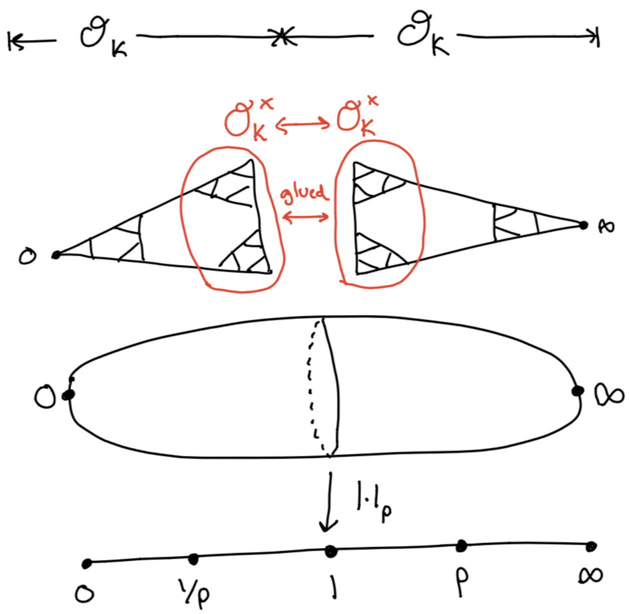
1. The trivial representation $\mathbb{K}$ is smooth and admissible, $\mathbb{K}^\infty$ is smooth but not admissible.
2. The standard representation of $GL_n(K)$ on K^n is not smooth, as $\operatorname{stab}_{GL_n(K)} v$ is not open for $v \neq 0$.
3. The group $G = (\mathbb{Z}_p, +)$ acts on the vector space $\mathcal{F} = \{\varphi : \mathbb{Z}_p \to \mathbb{C} \mid \varphi \text{ is locally constant}\}$ in the natural way, forming the "smooth regular representation." (This is the p-adic analogue of $L^2(G)$.) We claim that this representation is smooth and admissible.
    - **Smooth:** Let $\varphi \in \mathcal{F}$. Then for all $x \in \mathbb{Z}_p$, there is a neighborhood U_x such that $\varphi|_{U_x}$ is constant. This forms a covering of $\mathbb{Z}_p$ by open neighborhoods of the form $U_x = x + p^{n_x}\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is compact, there exists a finite subcovering $U_{x_1}, \ldots, U_{x_m}$. Then φ is fixed by $p^n\mathbb{Z}_p$, where $n = \operatorname{Max}\{n_i\}$, so the the stablizer of φ is open, hence the representation is smooth.
    - **Admissible:** A basis of open neighborhoods of 0 is given by $p^m\mathbb{Z}_p$, $m \geq 0$. Then

    $$\begin{aligned} \mathcal{F}^{p^m\mathbb{Z}_p} &= \{\varphi \mid \varphi \text{ is constant on } p^m\mathbb{Z}_p\text{-orbits}\} \\ &= \{\varphi : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{C}\} \end{aligned}$$

    is finite dimensional, so the representation is admissible.
4. (The most important example!) Recall that $\mathbb{P}^1\mathbb{C}$ is covered by the compact sets $D_{\leq 1} = \{z \mid |z| \leq 1\}$ and $D_{\leq 1}^{-1}$, so $\mathbb{P}^1\mathbb{C}$ is compact:



Similarly, $\mathbb{P}^1K = K \cup \{\infty\}$ is covered by the compact sets $D_{\leq 1} = \{z \in K \mid |z|_p \leq 1\} = \mathbb{O}_K$ and $D^{-1}_{\leq 1}$, so $\mathbb{P}^1K$ is compact:



$\mathcal{O}_K$
$\mathcal{O}_K$
$\mathcal{O}_K^\times \longleftrightarrow \mathcal{O}_K^\times$
glued
0
∞
0
∞
$|\cdot|_p$
0
1/p
1
p
∞

The vector space

$$I = \{f : \mathbb{P}^1K \to \mathbb{C} \mid f \text{ is locally constant}\}$$

admits a natural $GL_2(K)$-action, and the same argument as in the previous example (using compactness) shows that I is a smooth, admissible representation of $GL_2(K)$. In fact,

$$\text{constant functions} \hookrightarrow I \twoheadrightarrow St$$

Where $St := I/\{\text{constant functions}\}$ is the **Steinberg module**. The module St is irreducible (exercise, might be hard with current technology!).

Exercise 7.11. Show that any smooth finite dimensional representation of $GL_n(K)$ factors over $\det : GL_n(K) \to K^\times$. (*Hint: the kernel of a smooth finite dimensional representation is a finite intersection of stabilizers of a basis, so it must be open and normal, hence contains* $SL_n(K)$).

Exercise 7.12. The representation $\mathcal{F}' = \{\varphi : \mathbb{Q}_p \to \mathbb{C} \mid \varphi \text{ is locally constant}\}$ of $\mathbb{Z}_p$ is *not* admissible or smooth.

7.3 Solutions to exercises

Exercise 7.7. Let $\pi \in \mathbb{O}_K \subset K$ be a uniformizer.

1. Establish the Bruhat decomposition:

$$GL_n(K) = \bigsqcup_{\substack{\lambda_1 \geq \lambda_2 \ldots \geq \lambda_n \\ \lambda_i \in \mathbb{Z}}} GL_n(\mathbb{O}_K) \begin{pmatrix} \pi^{\lambda_1} & & & & \\ & \pi^{\lambda_2} & & & \\ & & \pi^{\lambda_3} & & \\ & & & \cdots & \\ & & & & \pi^{\lambda_n} \end{pmatrix} GL_n(\mathbb{O}_K) \quad (*)$$

   (*Hint: Gaussian elimination.*)

2. Use $(*)$ to classify the subgroups $GL_n(\mathbb{O}_K) \subset H \subset GL_n(K)$.

3. Hence or otherwise, show that $GL_n(\mathbb{O}_K)$ is a maximal compact subgroup of $GL_n(K)$.

Exercise 7.11. Show that any smooth finite dimensional representation of $GL_n(K)$ factors over $\det : GL_n(K) \to K^\times$. (*Hint: the kernel of a smooth finite dimensional representation is a finite intersection of stabilizers of a basis, so it must be open and normal, hence contains* $SL_n(K)$).

Exercise 7.12. The representation $\mathcal{F}' = \{\varphi : \mathbb{Q}_p \to \mathbb{C} \mid \varphi \text{ is locally constant}\}$ of $\mathbb{Z}_p$ is *not* admissible or smooth.

8 Lecture 8 (May 17, 2019): Precise statement of local Langlands for GL_2, $p \neq 2$

We pick up where we left off in the previous lecture. Let

$$\mathfrak{m}_K \subset \mathbb{O}_K \subset K$$

be the maximal ideal in the ring of integers of a local field. We are interested in the representation theory of the group $GL_n(K)$. (Or, more generally, the representation theory of any totally disconnected group G, but for concreteness we will work with GL_n.)

Recall that the sets

$$K_j = \{g \in GL_n(\mathbb{O}_K) \mid g = id \mod \mathfrak{m}_K^j\}$$

form a basis of open neighborhoods of $id \in GL_n(K)$. In addition to being open neighborhoods of the identity, the K_i are *subgroups* of $GL_n(K)$. (Note the existence of such subgroups which form a basis for open neighborhoods of the identity is only possible because $GL_n(K)$ is a totally disconnected group; a Lie group could not have such a family of subgroups because Lie groups have no small subgroups.)

Last week we saw that K_0 is a maximal compact subgroup of $GL_n(K)$. Let V be a representation of $GL_n(K)$. Because $K_0 \supset K_1 \supset K_2 \supset \cdots$, we have a chain

$$V^{K_0} \subset V^{K_1} \subset V^{K_2} \cdots$$

If V is smooth, each vector lies in V^U for some open $U \subset G$, hence lies in some V^{K_i}. So the filtration is exhaustive. If V is admissible, each V^{K_i} is finite dimensional.

Because $K_i \subset K_0$ is normal, the subspace V^{K_i} is stable under action by K_0. The subgroup $K_i \subset K_0$ acts trivially on V^{K_i}, so the K_0-action factors through the finite group $K_0/K_i \simeq GL_n(\mathbb{O}_K/\mathfrak{m}_K^i)$; e.g. for $K = \mathbb{Q}_p$, the K_0 action on V^{K_i} factors through $GL_n(\mathbb{Z}/p^i\mathbb{Z})$. (The key point here is that $K_i \subset K_0$ is *normal*, so the quotient K_0/K_i is a *group*.) Since representations of finite groups are completely reducible, we have a decomposition

$$V^{K_i} = \bigoplus_{\rho \in \widehat{K_0/K_i}} V^{K_i}(\rho),$$

where $V^{K_i}(\rho)$ is the ρ-isotypic component of V^{K_i}; that is, $V^{K_i}(\rho)$ is the direct sum of all irreducible subrepresentations of V^{K_i} which are isomorphic to ρ. Passing to the limit, we obtain a decomposition

$$V = \bigoplus_{\rho \in \widehat{K_0}} V(\rho).$$

Here $\widehat{K_0}$ denotes all representations of K_0 which factor over some quotient K_0/K_i.

Lemma 8.1. The representation V is admissible if and only if each isotypic component $V(\rho)$ in the decomposition above is finite-dimensional.

Proof. Assume that $V(\rho)$ is infinite dimensional for some $\rho \in \widehat{K_0}$. By definition, ρ factors through K_0/K_i for some i. Hence, $V(\rho) \subset V^{K_i}$ is an infinite dimensional subspace and V is not admissible.

To prove the opposite implication, assume that each $V(\rho)$ is finite-dimensional. For each i, we have a decomposition

$$V^{K_i} = \bigoplus_{\rho \in \widehat{K_0}} V(\rho)^{K_i}.$$

But since $V(\rho)$ is the direct sum of irreducible representations which are isomorphic to ρ, we have

$$V(\rho)^{K_i} = \begin{cases} 0 & \text{if } \rho|_{K_i} \neq \text{triv}, \\ V(\rho) & \text{otherwise.} \end{cases}$$

Hence

$$V^{K_i} = \bigoplus_{\substack{\rho \in \widehat{K_0} \\ \rho|_{K_i} = \text{triv}}} V(\rho).$$

Since K_0/K_i is a finite group, there are only finitely many representations $\rho \in \widehat{K_0}$ which factor through K_0/K_i for any fixed i, so decomposition above is a finite direct sum of finite-dimensional representations, hence V is admissible. □

Remark 8.2. This is like the theory of K-finite vectors in representation theory of real Lie groups. A big difference is that the representation theory of, for example $GL_m(\mathbb{Z}/p^n\mathbb{Z})$ for large m and n is extremely complicated, whereas we know the representation theory of compact Lie groups rather well.

Example 8.3.

1. Consider the $\mathbb{Z}_p$-representation $\mathcal{F} = \{\varphi : \mathbb{Z}_p \to \mathbb{C} \mid \varphi \text{ is locally constant}\}$ from Example 7.10.3. For an open neighborhood $p^m\mathbb{Z}_p$ of the identity, the invariants are

$$\begin{aligned} \mathcal{F}^{p^m\mathbb{Z}_p} &= \{\varphi \mid \varphi \text{ constant on } p^m\mathbb{Z}_p \text{ orbits}\} \\ &= \text{ regular representation of } \mathbb{Z}_p/p^m\mathbb{Z}_p. \end{aligned}$$

   Hence,

$$\mathcal{F} = \bigoplus_{\substack{\text{continuous} \\ \chi:\mathbb{Z}_p \to \mathbb{C}^\times}} \mathbb{C}_\chi.$$

2. Consider the $GL_2(K)$-representation

$$I = \{f : \mathbb{P}^1 K \to \mathbb{C} \mid f \text{ is locally constant}\}$$

   from example 7.10.4. Here

$$I^{K_n} = \{\varphi : \mathbb{P}^1(\mathcal{O}_K/\mathfrak{m}_K^n) \to \mathbb{C}\},$$

   so

$$I = \lim_{\to} \mathbb{C}[\mathbb{P}^1(\mathcal{O}_K/\mathfrak{m}_K^n)].$$

Let V be a representation of $GL_n(K)$. A map $\xi : V \to \mathbb{C}$ is **smooth** if $\operatorname{stab}_{GL_n(K)} \xi$ is open. Define the **smooth dual**

$$\widehat{V} = \{\text{smooth vectors } \xi : V \to \mathbb{C}\}.$$

Lemma 8.4. Assume V is a smooth representation of $GL_n(K)$. If $V = \bigoplus_{\rho \in \widehat{K_0}} V(\rho)$, then $\widehat{V} = \bigoplus_{\rho \in \widehat{K_0}} V(\rho)^*$.

In particular, if V is smooth and admissible, then so is $\widehat{V}$, and $V \xrightarrow{\sim} \widehat{\widehat{V}}$.

Proof. The map $\xi : V \to \mathbb{C}$ is smooth if and only if ξ vanishes on all but finitely many $V(\rho)$. The lemma follows. □

The goal for the remainder of this lecture will be to give a birds-eye view on the smooth admissible representations of $GL_1(K)$ and $GL_2(K)$. But first, we need a digression on norms.

8.1 Canonical norms

Recall that to make the product formula of Section 5.2 hold, we define three types of equivalence classes of multiplicative norms ("places," denoted by v) on a local field K:

- **finite places:** $|x|_v := (\#\mathbb{O}_K/\mathfrak{p})^{-\operatorname{val}_\mathfrak{p}(x)}$ for some prime $\mathfrak{p} \subset \mathbb{O}_K$,
- **real places:** $|x|_v := |i(x)|$ for some real embedding $i : K \hookrightarrow \mathbb{R}$, and
- **complex places:** $|x|_v := |i(x)|^2$ for some pair of conjugate embeddings $i : K \hookrightarrow \mathbb{C}$ not landing in $\mathbb{R}$.

Different normalizations would also yield multiplicative norms, but we chose the ones above to make the product formula

$$\prod_{\text{places } v} |x|_v = 1$$

for $x \in K^\times$ hold. For example, if $K = \mathbb{Q}_p$, $|p| = \epsilon$ gives a norm for any $0 < \epsilon < 1$, so why do we choose $|p| = 1/p$? In some sense, this choice is justified by the product formula, but it is still a little mysterious.

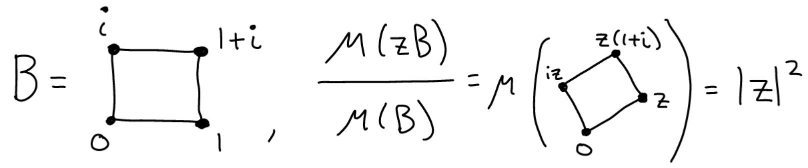
Tate made the following observation which further justifies this choice. For a place v, the completion K_v is is locally compact. Let μ be the additive Haar measure on K_v. The measure μ is unique up to a scalar. Define

$$|x|_v = \text{ factor by which } x\cdot \text{ scales the Haar measure;}$$

i.e., $|x|_v = \frac{\mu(x \cdot A)}{\mu(A)}$ for $A \subset K_v$ measurable and $0 < \mu(A) < \infty$.

Example 8.5. 1. $K_v = \mathbb{R}$: For $x \in \mathbb{R}$, $|x|_v = \frac{\mu(x[0,1])}{\mu([0,1])} = \mu([0,x]) = |x|$.

2. $K_v = \mathbb{C}$: For $z \in \mathbb{C}$, and



3. $K = \mathbb{Q}_p$: Recall that $\mathbb{Z}_p = \bigsqcup_{0 \leq m < p} m + p\mathbb{Z}_p$, so $p\mu(p\mathbb{Z}_p) = \mu(\mathbb{Z}_p)$. Hence,

$$|x|_v = \frac{\mu(p\mathbb{Z}_p)}{\mu(\mathbb{Z}_p)} = \frac{1}{p}.$$

From now on, whenever we consider a norm on a locally compact field, we will always consider this canonical norm, denoted $|\cdot|$.

8.2 Smooth admissible representations of $GL_1(K)$

Let V be a smooth admissible representation of $GL_1(K) = K^\times$. Since V is smooth admissible,

$$V = \bigcup V^{K_i}$$

and each V^{K_i} is finite-dimensional. Furthermore, since $K^\times$ is abelian, each of the subgroups $K_j := 1 + \mathfrak{m}_K^j \subset \mathbb{O}_K^\times$ is normal in $K^\times$, and the group

$$K^\times / K^j \simeq \mathbb{Z} \times (\mathbb{O}_K / \mathfrak{m}_K^j)^\times$$

acts on V^{K_j}. Hence if V is irreducible, V is one-dimensional and determined by a character of the form $|\cdot|^c \chi : K^\times \to \mathbb{C}$, where $c \in \mathbb{C}$ and $\chi : \mathbb{O}_K^\times \to \mathbb{C}$ is a continuous character.

Remark 8.6. The category of smooth admissible representations of $GL_1(K)$ is not semisimple. For example, the representation

$$x \mapsto \begin{pmatrix} 1 & \log|x| \\ 0 & 1 \end{pmatrix}$$

is a smooth, two-dimensional admissible representation which is not semisimple.

8.3 Smooth admissible representations of $GL_2(K)$

Recall from our heuristic description of last lecture that we expect roughly two types of representations of $GL_2(K)$: "principal series" representations coming from a split torus, and "cuspidal" representations coming from an anisotropic torus.

Let $B \subset GL_2(K)$ be the subgroup of upper triangular matrices. Given continuous characters $\chi_1, \chi_2 : K^\times \to \mathbb{C}$, define

$$I(\chi_1, \chi_2) := \{\varphi : GL_2(K) \to \mathbb{C} \,|\varphi \text{ loc. const., and } \varphi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot g\right) = \chi_1(a)\chi_2(d)|\frac{a}{d}|^{1/2}\varphi(g)$$
$$\text{for all } \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B\}.$$

Example 8.7.

$$\begin{aligned} I(|\cdot|^{-1/2}, |\cdot|^{1/2}) &= \{\varphi : GL_2(K) \to \mathbb{C} \mid \varphi \text{ loc. const. and } \varphi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot g\right) = \varphi(g)\} \\ &= \{\varphi : \mathbb{P}^1 K \simeq G/B \to \mathbb{C} \mid \varphi \text{ locally constant}\} \end{aligned}$$

We saw last time that $I(|\cdot|^{-1/2}, |\cdot|^{1/2})$ is smooth and admissible.

The representations $I(\chi_1, \chi_2)$ formed in this way are called **principal series representations**.

Theorem 8.8.

1. For all χ_1, χ_2, $I(\chi_1, \chi_2)$ is smooth and admissible.
2. $\widehat{I(\chi_1, \chi_2)} \simeq I(\chi_1^{-1}, \chi_2^{-1})$.
3. If $\chi_1/\chi_2 = |\cdot|^{-1}$, then we have an exact sequence of representations
$$0 \to C(\chi_1, \chi_2) \to I(\chi_1, \chi_2) \to S(\chi_1, \chi_2) \to 0$$
with $\dim C(\chi_1, \chi_2) = 1$ and $S(\chi_1, \chi_2)$ irreducible.
4. If $\chi_1/\chi_2 = |\cdot|$, then we have an exact sequence of representations
$$0 \to S(\chi_1, \chi_2) \to I(\chi_2, \chi_2) \to C(\chi_1, \chi_2) \to 0$$
with $\dim C(\chi_1, \chi_2) = 1$ and $S(\chi_1, \chi_2)$ irreducible.
5. Otherwise, $I(\chi_1, \chi_2)$ is irreducible.
6. If $\chi_1/\chi_2 \simeq |\cdot|^{-1}$, then $S(\chi_1, \chi_2) \simeq S(\chi_2, \chi_1)$ and $C(\chi_1, \chi_2) \simeq C(\chi_2, \chi_1)$, and if $\chi_1/\chi_2 \not\simeq |\cdot|^{\pm 1}$, then $I(\chi_1, \chi_2) \simeq I(\chi_2, \chi_1)$.

Remark 8.9. Some remarks on the theorem:

(a) The representation $I(\chi_1, \chi_2)$ is an example of an induced representation for a totally disconnected group.

(b) Why the strange $|\frac{a}{b}|^{1/2}$ factor? It's necessary to make 2. hold! So why does 2. hold? Consider
$$I(|\cdot|^{1/2}, |\cdot|^{-1/2}) = \{\varphi \mid \varphi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot g\right) = |\frac{a}{d}|\varphi(g)\}.$$

We can define a function
$$\begin{aligned} \Phi : I(|\cdot|^{1/2}, |\cdot|^{-1/2}) &\to \mathbb{C} \\ \varphi &\mapsto \int_{K_0} \varphi d\mu. \end{aligned}$$

(One can think of $I(|\cdot|^{1/2}, |\cdot|^{-1/2})$ as being some "functions" on $\mathbb{P}^1 K$ and we are integrating over $\mathbb{P}^1(K)$ to get a number. More precisely, these are "densities", but to explain why would take us too far afield.) Here's a minor miracle: the function Φ is $GL_2(K)$-invariant, hence

$$C(|\cdot|^{1/2}, |\cdot|^{-1/2}) = \mathbb{C}$$

is the trivial representation. Now, given $\varphi \in I(\chi_1, \chi_2)$ and $\varphi' \in I(\chi_1^{-1}, \chi_2^{-1})$, $\varphi\varphi' \in I(|\cdot|^{1/2}, |\cdot|^{-1/2})$. By composing with Φ, we get a $GL_2(K)$-invariant pairing:

$$I(\chi_1, \chi_2) \times I(\chi_1^{-1}, \chi_2^{-1}) \to \mathbb{C},$$

which turns out to be non-degenerate, establishing 2.

(c) Part 6. is the most complicated to prove. It uses an intertwiner $I(\chi_1, \chi_2) \to I(\chi_2, \chi_1)$ via analytic continuation (there are connections to the Jantzen filtration).

(d) Finally, note that $\operatorname{Rep} GL_2(K)$ is not semisimple, so we cannot just compute homs as in the finite group case.

The other class of representations of $GL_2(K)$ are cuspidal representations.

Theorem 8.10. For every degree 2 extension L/K and continuous character $\theta : L^\times \to \mathbb{C}$ which does not factor through the norm, there exists an irreducible representation $BC_{L/K}(\theta)$. We have that $BC_{L/K}(\theta) \simeq BC_{L/K}(\theta')$ if and only if $\theta^\sigma \simeq \theta'$ for $\sigma \in \operatorname{Gal}(L/K)$.

The construction of $BC_{L/K}(\theta)$ is complicated, via the Weil representation. What is going on metaphorically?

- Consider $SL_2(\mathbb{F}_q)$. We've seen in Joe's Informal Friday Seminar talks that a character $\theta : T_a \to \mathbb{C}^\times$ gives rise to a local system L_θ on $\mathbb{P}^1_{\mathbb{F}_q} \backslash \mathbb{P}^1(\mathbb{F}_q)$. Taking the first cohomology yields a cuspidal representation $R^G_{T_a}(\theta)$.
- Consider $SL_2(\mathbb{R})$. A character $\theta : SO(2) \to \mathbb{C}^\times$ (such characters are classified by $\mathbb{Z}$) gives rise to a local system $\mathcal{O}(n)$ on the upper half plane, taking global sections yields a discrete series representation $\Gamma(\mathbb{H}, \mathcal{O}(n))$.
- Now take $GL_2(K)$. A character $\theta : L^\times \to \mathbb{C}$ gives rise to a local system $\mathcal{L}_\theta$ on "Drinfeld space" $\mathbb{P}^1(\overline{K})/\mathbb{P}^1(K)$. Taking first cohomology yields the representation $BC_{L/K}(\theta)$. Note that this is very technical, and is an active area of research.

This can also be viewed through the lens of Langlands functoriality. Let L/K be a degree n extension, so $W_L \subset W_K$ is an index n subgroup. We have the following diagram:

$$\begin{tikzcd}
\left\{\begin{array}{c}\text{1-dim'l reps}\\ \text{of } L^\times\end{array}\right\} \arrow[r, leftrightarrow] \arrow[d, "\mathrm{Ind}_{W_L}^{W_K}"] & \left\{\begin{array}{c}\text{irred. smooth ad.}\\ \text{reps of } GL_1(L)\end{array}\right\} \arrow[d, "BC=\text{“base change”}"] \\
\left\{\begin{array}{c}n\text{-dim'l reps}\\ \text{of } K^\times\end{array}\right\} \arrow[r, leftrightarrow] & \left\{\begin{array}{c}\text{irred smooth}\\ \text{reps of } GL_n(K)\end{array}\right\}
\end{tikzcd}$$

Thus an innocuous induction functor on the left hand side predicts a highly non-trivial correspondence between irreducible representation on the right hand side!

8.4 Weil-Deligne representations

We are almost ready to make a precise statement of the local Langlands correspondence for $GL_2(K)$! Recall local class field theory: there is a map

$$r_K : W_K \to K^\times.$$

Composing with $|\cdot|$ gives us the **norm character**

$$|\cdot| : W_K \to \mathbb{Q}^\times.$$

An n-dimensional **Weil-Deligne representation** is a triple (ρ, V, N), where

- V is an n-dimensional complex vector space,
- $\rho : W_K \to GL(V)$ is a continuous representation, and
- $N \in \mathrm{End}(V)$ is nilpotent such that
$$\rho(x)N\rho(x)^{-1} = |x|N \tag{$*$}$$
for all $x \in W_K$. (In fact, $(*)$ forces N to be nilpotent.)

Example 8.11.

1. Any n-dimensional continuous representation of W_K with $N = 0$ is a Weil-Deligne representation.
2. The representation $\rho = \begin{pmatrix} |\cdot|\chi & 0 \\ 0 & \chi \end{pmatrix}$ for any character $\chi : W_K \to \mathbb{C}^\times$ and $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ form a Weil-Deligne representation. Indeed, for $x \in W_K$,
$$\begin{aligned} \rho(x)N\rho(x)^{-1} &= \begin{pmatrix} |x|\chi(x) & 0 \\ 0 & \chi(x) \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} |x|^{-1}\chi(x)^{-1} & 0 \\ 0 & \chi(x)^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 0 & |x| \\ 0 & 0 \end{pmatrix} \\ &= |x| \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$
We denote this Weil-Deligne representation $St(\chi, |\cdot|\chi)$.

A Weil-Deligne representation is ***F*-semisimple** if V is semisimple as a representation of W_K.

Exercise 8.12. Let $\widetilde{\mathrm{Frob}} \in W_K$ be any lift of Frobenius. Show that a Weil-Deligne representation is F-semisimple if and only if $\widetilde{\mathrm{Frob}}$ is semisimple.

Theorem 8.13. (*Local Langlands correspondence for GL_2, $p \neq 2$*) Fix a local field K of residue characteristic $p \neq 2$. There is a canonical bijection

$$\left\{ \begin{array}{c} F\text{-semisimple} \\ 2\text{-dimensional} \\ \text{Weil-Deligne reps} \end{array} \right\}_{/\simeq} \leftrightarrow \left\{ \begin{array}{c} \text{irred. smooth admiss.} \\ \text{reps of } GL_2(K) \end{array} \right\}_{/\simeq}$$

Moreover, this bijection is given as follows.

$$\begin{aligned}
\chi_1/\chi_2 = |\cdot|^{\pm 1} : &\left(\begin{pmatrix}\chi_1 & 0\\ 0 & \chi_2\end{pmatrix}, N = 0\right) \leftrightarrow C(\chi_1, \chi_2)\\
\chi_1/\chi_2 = |\cdot|^{\pm 1} : &\left(\begin{pmatrix}\chi|\cdot| & 0\\ 0 & \chi\end{pmatrix}, N = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\right) \leftrightarrow S(\chi, |\cdot|\chi)\\
\chi_1/\chi_2 \neq |\cdot|^{\pm 1} : &\left(\begin{pmatrix}\chi_1 & 0\\ 0 & \chi_2\end{pmatrix}, N = 0\right) \leftrightarrow I(\chi_1, \chi_2)\\
L/K, \theta : L^\times \to \mathbb{C}^\times : &\left(\mathrm{Ind}_{W_K}^{W_L}(\theta), N = 0\right) \leftrightarrow BC_{L/K}(\theta)
\end{aligned}$$

Where the character $\theta : L^\times \to \mathbb{C}^\times$ does not factor through the norm.

8.5 Solutions to Exercises

Exercise 8.12. Let $\widetilde{\mathrm{Frob}} \in W_K$ be any lift of Frobenius. Show that a Weil-Deligne representation is F-semisimple if and only if $\widetilde{\mathrm{Frob}}$ is semisimple.

9 Lecuture 9 (May 24, 2019): Why is $p = 2$ special? Spherical representations and Satake isomorphism

Today's lecture has two objectives: to explore what the LLC looks like when $p = 2$, and to examine how a simple special case of the LLC for GL_n leads to the Satake isomorphism.

9.1 Ramification filtration revisited

To begin, we revisit the ramification filtration of Section 6.3. Let L/K be a finite Galois extension where K and L are both local fields. We have the following inclusions:

$$\begin{tikzcd}
L \arrow[d, dash] & \mathbb{O}_L \arrow[l, hook] \arrow[d, dash] & \mathfrak{m}_L \arrow[l, hook] \arrow[r, equal] \arrow[d, dash] & (\pi_L) \arrow[d, dash] \\
K & \mathbb{O}_K \arrow[l, hook] & \mathfrak{m}_K \arrow[l, hook] \arrow[r, equal] & (\pi_L)
\end{tikzcd}$$

Here the uniformizers π_K, π_L are the only non-canonical objects in the diagram above. We denote by $k_K = \mathbb{O}_L/\mathfrak{m}_L$ (resp. $k_L = \mathbb{O}_L/\mathfrak{m}_L$) the residue fields. There is a short exact sequence

$$I_{L/K} \hookrightarrow \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(k_L/k_K) = \langle \mathrm{Frob} \rangle \simeq \mathbb{Z}/f\mathbb{Z}.$$

Lemma 9.1. An element $\sigma \in I_{L/K}$ in the inertia subgroup is determined by $\sigma(\pi_L)$.

This leads to the **ramification filtration** of the Galois group. Define

$$I_0 := I_{L/K}, \quad I_j := \left\{ \sigma \in I_{L/K} \mid \frac{\sigma(\pi_L)}{\pi_L} = 1 \mod \mathfrak{m}_L^j \right\}.$$

Then

$$\mathrm{Gal}(L/K) \supset I_0 \supset I_1 \supset I_2 \supset \cdots \supset \{1\}$$

is a filtration of $\mathrm{Gal}(L/K)$.

Key Facts:

1. The ramification filtration is a finite exhaustive filtration.

2. There is an injection $I_0/I_1 \hookrightarrow \mathbb{O}_L^\times/(1+\mathbb{O}_L^\times) \simeq k_L^\times : \sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L}$. Hence I_0/I_1 is cyclic of order prime to p.

3. For $j \geq 1$, there is an injection $I_j/I_{j+1} \hookrightarrow (1+\mathfrak{m}_L^j)/(1+\mathfrak{m}_L^{j+1}) \simeq (k_L, +) : \sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L}$. Hence I_j/I_{j+1} is an abelian p-group, and I_1 is a Sylow p-subgroup of $I_{L/K}$.

This filtration leads to some nomenclature: The first subquotient $\mathrm{Gal}(L/K)/I_{L/K}$ is canonically isomorphic to $\mathbb{Z}/f\mathbb{Z}$, and is referred to as the **unramified** part of the Galois group. The second subquotient $I_{L/K}/I_1$ is cyclic of order prime to p, and is referred to as the **tamely ramified** part of the Galois group. The remaining subquotients of the ramification filtration are abelian p-groups (and hence I_1 is a solvable p-group), and are referred to as the **wildly ramified** part of the Galois group.

The upshot is that there are significant constraints on which groups can appear as Galois groups of extensions of local fields. (For example, they must be solvable.) This is in sharp contrast to the number field setting, where many types of groups can appear as Galois groups of extensions of $\mathbb{Q}$. (Though exactly which groups appear as Galois groups of number fields is still very much an open problem, the *inverse Galois problem.*)

Example 9.2. 1. Consider the extension $L = \mathbb{Q}_p(\sqrt[p-1]{p})$ of $K = \mathbb{Q}_p$. Here $\pi_L = \sqrt[p-1]{p}$ and $\pi_K = p$ are uniformizers.

Exercise 9.3. Show that the set μ_{p-1} of all $(p-1)^{st}$ roots of unity is contained in $\mathbb{Q}_p$.

The Galois group of this extension is

$$\mathrm{Gal}(L/K) = \{\sigma_\zeta : \sqrt[p-1]{p} \mapsto \zeta \sqrt[p-1]{p} \text{ for } \zeta \in \mu_{p-1}\} \simeq k_K^\times \hookrightarrow k_L^\times.$$

One can check that $\mathrm{Gal}(L/K)$ is totally ramified; that is, $I_{L/K} = \mathrm{Gal}(L/K)$. (This follows from the observation that we are adjoining roots of p, whose image is zero in the residue field.) Furthermore, if $\sigma_\zeta \in I_{L/K} = \mathrm{Gal}(L/K)$, then $\frac{\sigma_\zeta(\pi_L)}{\pi_L} = \zeta \in k_L^\times$, hence $I_1 = \{1\}$ and $\mathrm{Gal}(L/K)$ is tamely ramified.

2. Examples of wild ramification are almost always hard! We really should spend a lecture on such examples, but we are quickly running out of time, so sadly we will not.

Next we'll examine the structure of the absolute Galois group of a local field. For a local field K, we have an exact sequence

$$I_{\overline{K}/K} \hookrightarrow \mathrm{Gal}(\overline{K}/K) \twoheadrightarrow \widehat{\mathbb{Z}}.$$

We would like to pass to the limit to obtain a ramification filtration of the inertia subgroup $I_{\overline{K}/K}$ from the ramification filtrations of the inertia subgroups of finite extensions. However, there is a problem: if $L'/L/K$ is a tower of finite extensions, then the ramification filtration of $I_{L'/K}$ is related to multiples of the ramification filtration of $I_{L/K}$.

This can be fixed through an "upper numbering" procedure which replaces I_j with $I_{L/K}^\lambda$ for $\lambda \in \mathbb{Q}_{\geq 0}$ in a way that is compatible with extensions. (Exactly how one does this appears pretty crazy at first sight. It is explained in Serre's Local Fields [Ser79].) This leads to a ramification filtration $I_{\overline{K}/K}^\lambda$ of the inertia subgroup of the absolute Galois group indexed by rational numbers:

$$\mathrm{Gal}(\overline{K}/K) \supset I_{\overline{K}/K} \supset I_{\overline{K}/K}^{>0} \supset \cdots \supset I_{\overline{K}/K}^{463/5} \supset \cdots.$$

This filtration has the property that $\mathrm{Gal}(\overline{K}/K)/I_{\overline{K}/K} = \widehat{\mathbb{Z}}$ canonically, $I_{\overline{K}/K}/I_{\overline{K}/K}^{>0} \simeq \prod_{\substack{l \neq p \\ \text{prime}}} \mathbb{Z}_l$ non-canonically, and other subquotients are pro-p groups.

Important points:

1. The first two steps depend only on the residue characteristic of the field.

2. Via class field theory, the image of this filtration in $W_K^{ab} \simeq K^\times$ corresponds to the filtration by $1 + \mathfrak{m}_K^j \subset \mathbb{O}_K$. The fact that the only jumps in this filtration are at integers (as opposed to other elements of $\mathbb{Q}$) is the **Hasse–Arf Theorem**.

9.2 More details on Weil–Deligne representations

Next we would like to show two things: (1) why any Weil–Deligne representation is "close" to a continuous representation of $\mathrm{Gal}(\overline{K}/K)$ and (2) why $p = 2$ is special in the local Langlands correspondence.

Proposition 9.4. Any indecomposible F-semisimple Weil–Deligne representation is isomorphic to $St_n \otimes \rho$, where ρ is an irreducible representation of W_K.

Here St_n is the Steinberg representation from the previous lecture; e.g.

$$St_4 = \left(\begin{pmatrix} |\cdot|^3 & 0 & 0 & 0 \\ 0 & |\cdot|^2 & 0 & 0 \\ 0 & 0 & |\cdot| & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, N = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \right)$$

The proof of this proposition is left as a somewhat tricky exercise. It becomes easier if you know what the weight filtration associated to a nilpotent operator is.

Proposition 9.5. 1. Let $\rho : W_K \to GL(v)$ be an irreducible representation. Then there exists a continuous character $\chi : W_K \to \mathbb{C}^\times$ such that $\rho \otimes \chi$ has finite image and hence defines a representation $\rho \otimes \chi : \mathrm{Gal}(\overline{K}/K) \to GL(V)$.

2. Suppose that $\rho : W_K \to GL(V)$ is irreducible and not induced from any proper subgroup of W_K. Then the restriction to wild intertia is irreducible. In particular, $\dim V$ is a power of p (since any irreducible module over a p-group has dimension divisible by p).

Remark 9.6. Proofs of these two statements can be found in [Tat79].

Propositions 9.4 and 9.5.1 show that every Weil–Deligne representation is "close" to a representation of the absolute Galois group, in the sense that every Weil-Deligne representation can be obtained from the Steinberg representation and an irreducible representation of W_K, and every irreducible representation of W_K can be upgraded to a representation of $\mathrm{Gal}(\overline{K}/K)$ by tensoring with a character.

The two statements of Proposition 9.5 are reasonably easy consequences of the following lemma.

Lemma 9.7. Suppose a group G has the form

$$\Gamma \hookrightarrow G \twoheadrightarrow \mathbb{Z}$$

for some finite group Γ. Then any irreducible G-module is either irreducible over Γ or induced from a subgroup of the form $\Gamma \rtimes m\mathbb{Z}$.

The proof of this lemma is a worthwhile exercise!

9.3 Why is LLC for $p = 2$ special?

Proposition 9.5 shows that for $p \neq 2$, all irreducible 2-dimensional representations of W_K are induced from a finite index subgroup. However, for $p = 2$, it's possible that there are irreducible representations of W_K which are not induced. So do such representations exist? Yes!

Consider a continuous two-dimensional representation $\rho : \mathrm{Gal}(\overline{K}/K) \to GL_2(\mathbb{C})$. By the no small subgroups lemma, the image of ρ must lie in a finite subgroup of $GL_2(\mathbb{C})$, so in the composition of ρ with the projection

$$GL_2(\mathbb{C}) \to PGL_2(\mathbb{C}),$$

the image must be conjugate to a subgroup of the maximal compact subgroup $SO_3 \subset PGL_2(\mathbb{C})$. The finite subgroups of SO_3 were classified[5]! They are of the following types:

- cyclic (symmetries of the product of an m-gon and an interval, fixing one end)
- dihedral (symmetries of the product of an m-gon and an interval)
- A_4 (symmetries of the tetrahedron)
- symmetries of the cube
- A_5 (symmetries of the icosahedron)

Reducible representations have images in cyclic subgroups of SO_3, and induced representations have images which are dihedral groups. What about the other three? Are there any representations of $\mathrm{Gal}(\overline{K}/K)$ whose image lies in any of the final three finite subgroups? Since $\mathrm{Gal}(\overline{K}/K)$ is solvable, we can eliminate the non-solvable group A_5 from our list. Let's consider the composition series of A_4:

$$K_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \hookrightarrow A_4 \twoheadrightarrow \mathbb{Z}/3\mathbb{Z}$$

By the structure of the ramification filtration, this subgroup structure is only possible for a local Galois group if $p = 2$. It turns out that it does indeed occur for some local fields!

The upshot is that for $p = 2$, there are more representations on each side of the LLC, and the extra representations on the Weil group side are this special class of irreducible non-induced representations whose image lies in A_4. (Geordie isn't sure if representations corresponding to the symmetries of the cube exist.)

A mystery to ponder: Let G be a compact Lie group (e.g. a finite group), and let $R(G)_{\mathbb{C}}$ be its representation ring. What is a character

$$\theta : R(G)_{\mathbb{C}} \to \mathbb{C}?$$

[5] by Klein in 1884, [Kle93]

9.4 Unramified representations

One way to convince yourself that the LLC is amazing is to see that simple special cases already have deep consequences. The first example of this that we've seen is local class field theory. The second example we will see now!

The local Langlands correspondence for $GL_n(K)$ says that there is a canonical bijection:

$$\left\{ \begin{array}{c} F\text{-semisimple} \\ n\text{-dimensional} \\ \text{Weil-Deligne reps} \end{array} \right\}_{/\simeq} \xleftrightarrow{1:1} \left\{ \begin{array}{c} \text{irred smooth} \\ \text{admissible} \\ \text{reps of } GL_n(K) \end{array} \right\}_{/\simeq}$$

On the left hand side of this bijection, we can consider a special class of **unramified Weil-Deligne representations** consisting of those representations of W_K which are trivial on the inertia subgroup. The corresponding representations on the right hand side are the **spherical representations** of $GL_n(K)$:

$$\left\{ \begin{array}{c} \text{Weil-Deligne reps} \\ \text{s.t. } N = 0 \text{ and } \rho \\ \text{factors through } \mathbb{Z}\text{:} \\ W_k \twoheadrightarrow \mathbb{Z} \hookrightarrow GL_n(\mathbb{C}) \end{array} \right\}_{/\simeq} \xleftrightarrow{1:1} \left\{ \begin{array}{c} \text{reps of } GL_n(K) \\ \text{admitting a} \\ GL_n(\mathbb{O}_K)\text{-fixed vector} \end{array} \right\}_{/\simeq}$$

Semisimple representations of W_K which factor through $\mathbb{Z}$ are in bijection with semisimple elements of $GL_n(\mathbb{C})$, and irreducible representations of $GL_n(K)$ admitting a $GL_n(\mathbb{O}_K)$-fixed vector are in bijection with irreducible representations of the "spherical Hecke algebra" (which you are not expected to be familiar with and we will soon define). Thus, the restriction of the local Langlands correspondence to this special case results in a bijection

$$\left\{ \begin{array}{c} \text{semisimple elements} \\ \text{in } GL_n(\mathbb{C}) \end{array} \right\}_{/\text{conj}} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{c} \text{irreducible reps of} \\ \mathcal{H}_{sph} := \mathcal{H}(GL_n(\mathbb{O}_K), GL_n(K)) \end{array} \right\}_{/\simeq}$$

This is the **Satake isomorphism**! We will spend the rest of the lecture explaining this bijection (particularly the right hand side) in more detail.

Remark 9.8. The left-hand-side of the bijection above is independent of K, and even of the residue characteristic p!

9.5 Hecke algebras

Suppose G is a finite group.

Case 1: Consider $N \subset G$ a normal subgroup. If V is a G-representation, then G acts on V^N (because for $n \in N, g \in G$, and $v \in V^N$, $n \cdot gv = g \cdot g^{-1}ng \cdot v = gv$), and the action factors over G/N. Moreover, one can checek that $\mathrm{End}(\mathrm{Ind}_N^G \mathbb{C}) \simeq \mathbb{C}[G/N]$. Hence we have a bijection

$$\left\{ \begin{array}{c} \text{irred } G\text{-modules} \\ \text{with an } N\text{-fixed vector} \end{array} \right\}_{/\simeq} \leftrightarrow \{ \text{ irred } G/N\text{-modules}\}_{/\simeq}.$$

Case 2: Consider $H \subset G$ not necessarily normal. Given a G-representation V, what acts on V^H? The Hecke algebra! The operator

$$\begin{aligned} \pi_H : V &\to V^H \\ v &\mapsto \frac{1}{|H|} \sum_{h \in H} h \cdot v \end{aligned}$$

projects onto H-invariants. This can be used to define a "Hecke operator" $[HgH]$ for every $g \in G$ which makes the following diagram commute:

$$\begin{tikzcd} V^H \arrow[r, "{[HgH]}"] \arrow[d, hook] & V^H \\ V \arrow[r, "\cdot g"] & V \arrow[u, "\pi_H"'] \end{tikzcd}$$

Note that all g in the same double coset yield the same Hecke operator. Alternatively, this operator is the sum

$$[HgH] = \frac{1}{|H|} \sum_{g' \in HgH} g'.$$

The **Hecke algebra** $\mathcal{H}(H, G)$ of the pair (H, G) is the vector space ${}^H\mathbb{C}[G]^H$ with multiplication

$$(f * f')(g) := \frac{1}{|H|} \sum_{g = hh'} f(h) f'(h).$$

This is an associative unital algebra with unit

$$1_H = \frac{1}{|H|} \sum_{h \in H} h.$$

Example 9.9.

1. If N is normal, $\mathcal{H}(N, G) = \mathbb{C}[G/N]$.
2. If $G = GL_n(\mathbb{F}_q)$ and $B = \left\{ \begin{pmatrix} * & \cdots & * \\ 0 & \ddots & \vdots \\ 0 & 0 & * \end{pmatrix} \right\}$, then $\mathcal{H}(B, G)$ is the "Hecke algebra of S_n at $q = |\mathbb{F}_q|$." This algebra is almost independent of q.

Exercise 9.10. (Do it!) Show that

$$\operatorname{End}(\operatorname{Ind}_H^G \mathbb{C}) \simeq \mathcal{H}(H, G).$$

Hence

$$\langle \operatorname{Ind}_H^G \mathbb{C} \rangle \xrightarrow{\sim} \mathcal{H}(H, G)\text{-mod}.$$

(Here the angle brackets mean the smallest abelian category generated by kernels, cokernels, extensions, and direct sums.) Deduce that

$$\left\{ \begin{matrix} \text{irred. } G\text{-modules} \\ \text{with } H\text{-fixed vector} \end{matrix} \right\} \overset{1:1}{\longleftrightarrow} \{\text{irred } \mathcal{H}(H, G)\text{-modules}\}.$$

Remark 9.11. There is a tendency in the literature to consider one subgroup H at a time, but one can also consider all subgroups (or a particularly nice family of subgroups) at the same time, resulting in a "Hecke algebroid."

We can also define Hecke algebras of p-adic groups. Let $G = GL_n(K)$ for a local field K, and $K_0 = GL_n(\mathbb{O}_K)$ the maximal compact subgroup. Then the "big" Hecke algebra of G is

$$\mathcal{H}^{big} = \left\{ \varphi : G \to \mathbb{C} \mid \begin{matrix} \varphi \text{ locally constant} \\ \text{compact support} \end{matrix} \right\}.$$

An alternate description is

$$\mathcal{H}^{big} = \bigcup_i \left\{ \varphi : G \to \mathbb{C} \mid \begin{matrix} \varphi \text{ locally constant on } K_i\text{-double} \\ \text{cosets, non-zero on finitely many} \end{matrix} \right\}.$$

Exercise 9.12. Prove that the two formulations of $\mathcal{H}^{big}$ are equivalent.

The algebra structure on $\mathcal{H}^{big}$ is given by

$$(f * f')(g) = \int_{h \in G} f(h) f'(h^{-1}g) d\mu,$$

where μ is the Haar measure.

Example 9.13. Let 1_{K_i} be the indicator function on K_i. Then

$$1_{K_i} * 1_{K_i}(g) = \int_{h \in G} 1_{K_i}(h) 1_{K_i}(h^{-1}g) d\mu = \begin{cases} 0 & \text{if } g \notin K_i, \\ \int_{K_i} 1 d\mu & \text{if } g \in K_i. \end{cases}$$

In other words,

$$1_{K_i} * 1_{K_i} = \mu(K_i) 1_{K_i},$$

so 1_{K_i} is a quasi-idempotent.

Remark 9.14. Because any irreducible G-module has $V^{K_i} \neq 0$ for some i, $\mathcal{H}^{big}$ can be used to understand all smooth admissible representations of G. However, it is very complicated.

Assume $\mu(K_0) = 1$ so 1_{K_0} is idempotent. The **spherical Hecke algebra** is

$$\mathcal{H}^{sph} = \mathcal{H}(K_0, G) := 1_{K_0} \mathcal{H}^{big} 1_{K_0}.$$

Exercise 9.15. (Do it!) Prove the Cartan decomposition of G:

$$G = \bigsqcup_{\substack{\underline{\lambda} \\ \lambda_1 \geq \lambda_2 \ldots \geq \lambda_n \\ \lambda_i \in \mathbb{Z}}} K_0 \begin{pmatrix} \pi^{\lambda_1} & & & & \\ & \pi^{\lambda_2} & & & \\ & & \pi^{\lambda_3} & & \\ & & & \ddots & \\ & & & & \pi^{\lambda_n} \end{pmatrix} K_0$$

Hence

$$\mathcal{H}^{sph} = \bigoplus_{\underline{\lambda}} \mathbb{C} 1_{\underline{\lambda}}.$$

There are two miracles.

Theorem 9.16. 1. The spherical Hecke algebra $\mathcal{H}^{sph}$ is commutative.

2. (**The Satake isomorphism**) There exists a canonical bijection

$$\mathcal{H}^{sph} \overset{\sim}{\leftrightarrow} R({}^LGL_n(\mathbb{C})).$$

Remark 9.17. The Langlands dual group ${}^LGL_n(\mathbb{C}) \simeq GL_n(\mathbb{C})$ so we could have replaced the right hand side of the Satake isomorphism with the representation ring of $GL_n(\mathbb{C})$; however, the theorem also holds for general reductive groups and there the dual group is important.

Recall our mystery from earlier in the lecture: For a compact Lie group G, what is a character $\theta : R(G)_{\mathbb{C}} \to \mathbb{C}$ of its representation ring? By the Chevalley restriction theorem, $R(G)_{\mathbb{C}} \simeq R(T)^W_{\mathbb{C}}$, where $T \subset G$ is a maximal torus and W is the Weyl group of G. So a character of $R(G)_{\mathbb{C}}$ is just a choice of a semisimple conjugacy class in G!

Theorem 9.16 can be used to establish unramified LLC:

$$\begin{tikzcd}
\left\{\begin{array}{c}\text{“spherical representations;”}\\ \text{i.e. smooth admissible}\\ \text{irred reps of } G \text{ with}\\ \text{a } K_0\text{-fixed vector}\end{array}\right\}_{/\simeq} \arrow[r, leftrightarrow, "1:1", "\text{Hecke algebra magic}"'] & \left\{\begin{array}{c}\text{irreducible}\\ \mathcal{H}(K_0,G)=\mathcal{H}^{sph}-\\ \text{modules}\end{array}\right\}_{/\simeq} \\
{} \arrow[r, leftrightarrow, "1:1", "\text{commutativity of } \mathcal{H}^{sph}"'] & \left\{\begin{array}{c}\text{characters}\\ \chi : \mathcal{H}^{sph} \to \mathbb{C}\end{array}\right\} \\
{} \arrow[r, leftrightarrow, "1:1", "\text{Satake isomorphism}"'] & \left\{\begin{array}{c}\text{characters}\\ \theta : R({}^LGL_n(\mathbb{C})) \to \mathbb{C}\end{array}\right\} \\
{} \arrow[r, leftrightarrow, "1:1", "\text{the mystery from earlier}"'] & \left\{\begin{array}{c}\text{conjugacy classes}\\ \text{of semisimple}\\ \text{elts in } {}^LGL_n(\mathbb{C})\end{array}\right\} \\
{} \arrow[r, leftrightarrow, "1:1", "\text{definition}"'] & \left\{\begin{array}{c}\text{unramified}\\ n\text{-dimensional}\\ \text{Weil–Deligne}\\ \text{representations}\end{array}\right\}_{/\simeq}
\end{tikzcd}$$

9.6 Solutions to exercises

Exercise 9.3. Show that the set μ_{p-1} of all $(p-1)^{st}$ roots of unity is contained in $\mathbb{Q}_p$.

Solution: Recall the following theorems.

Fermat's Little Theorem: For an integer $a \in \mathbb{Z}$ which is not divisible by p, $a^{p-1} = 1 \mod p$.

Hensel's Lemma: Let $f(x) \in \mathbb{Z}_p[x]$. If the reduction $\overline{f}(x) \in \mathbb{F}_p[x]$ has a simple root x_0, then there exists a unique $a \in \mathbb{Z}_p$ such that $f(a) = 0$ and the reduction $\overline{a} = x_0 \in \mathbb{F}_p$.

Consider the polynomial $f(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x]$. By Fermat's little theorem, $f(x)$ has $p-1$ roots mod p. Hensel's implies that there exist $p-1$ distinct elements $a_1, \ldots, a_{p-1} \in \mathbb{Z}_p$ such that $f(a_i) = a^{p-1} - 1 = 0$. Hence the $(p-1)^{st}$ roots of unity $\mu_{p-1} = \{a_1, \ldots, a_{p-1}\} \subset \mathbb{Q}_p$.

Exercise 9.4. Prove Proposition 9.4

Exercise 9.6. Prove Lemma 9.7

Exercise 9.9. (Do it!) Show that

$$\mathrm{End}(\mathrm{Ind}_H^G \mathbb{C}) \simeq \mathcal{H}(H, G).$$

Hence

$$\langle \mathrm{Ind}_H^G \mathbb{C} \rangle \xrightarrow{\sim} \mathcal{H}(H, G)\text{-mod}.$$

(Here the angle brackets mean the smallest abelian category generated by kernels, cokernels, extensions, and direct sums.) Deduce that

$$\left\{ \begin{array}{c} \text{irred. } G\text{-modules} \\ \text{with } H\text{-fixed vector} \end{array} \right\} \overset{1:1}{\longleftrightarrow} \{\text{irred } \mathcal{H}(H, G)\text{-modules}\}$$

Solution: By Frobenius reciprocity,

$$\mathrm{Hom}_G(\mathrm{Ind}_H^G \mathbb{C}, \mathrm{Ind}_H^G \mathbb{C}) \simeq \mathrm{Hom}_H(\mathbb{C}, \mathrm{Res}_H^G \mathrm{Ind}_H^G \mathbb{C}).$$

As a vector space, $\mathrm{Res}_H^G \mathrm{Ind}_H^G \mathbb{C} \simeq \mathbb{C}[G/H]$ with H-action given by $h \cdot f(gH) = f(h^{-1}gH)$ for $h \in H$, $g \in G$. An H-module homomorphism

$$\varphi : \mathbb{C} \to \mathbb{C}[G/H]$$

is a linear map with the property that $\varphi(z)(gH) = \varphi(z)(hgH)$ for all $z \in \mathbb{C}$, $h \in H$, $g \in G$. Such an H-module morphism is completely determined by $\varphi(1) \in \mathbb{C}[H \backslash G/H]$. Thus,

$$\mathrm{End}(\mathrm{Ind}_H^G \mathbb{C}) \simeq \mathcal{H}(H, G).$$

Exercise 9.11. Prove that the two formulations of $\mathcal{H}^{big}$ are equivalent.

Exercise 9.14. (Do it!) Prove the Cartan decomposition of G:

$$G = \bigsqcup_{\substack{\underline{\lambda} \\ \lambda_1 \geq \lambda_2 \ldots \geq \lambda_n \\ \lambda_i \in \mathbb{Z}}} K_0 \begin{pmatrix} \pi^{\lambda_1} & & & & \\ & \pi^{\lambda_2} & & & \\ & & \pi^{\lambda_3} & & \\ & & & \ddots & \\ & & & & \pi^{\lambda_n} \end{pmatrix} K_0$$

Hence

$$\mathcal{H}^{sph} = \bigoplus_{\underline{\lambda}} \mathbb{C}1_{\underline{\lambda}}.$$

10 Lecture 10 (May 31, 2019): The final lecture

Today is about the big picture. We start with the very big picture, and finish with the moderately big picture. This is also the final lecture of the first term of this course!

10.1 The big picture

10.1.1 Dimension 0

Let's go back to the beginning. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial; e.g. $f(x) = x^2 + 1$. Back in March, we wondered: How many solutions does $f(x)$ have modulo a prime p? We constructed tables:

p	2	3	5	7	11	13	17	19	23	
# of sol's mod p	1	0	2	0	0	2	2	0	0	...
p mod 4	2	3	1	3	3	1	1	3	3	

Then we studied this via representation theory. The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the roots $\{\sigma_1, \ldots, \sigma_n\} \subset \overline{\mathbb{Q}}$ of $f(x)$, so we have a permutation representation

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL(H),$$

where $H := \bigoplus_{i=1}^n = \mathbb{C}\sigma_i$. Then for unramified primes,

$$\#\text{ solutions of } f(x) \text{ mod } p \ = \mathrm{Tr}(\mathrm{Frob_p}, H).$$

Even in this innocent ("dimension 0") case, H is enormously complicated. To simplify things, we instead considered a collection of *local* representations $H_{\mathbb{Q}_p}$, defined as follows. For each p, consider roots $\sigma_1', \ldots, \sigma_n'$ of $f(x)$ in $\overline{\mathbb{Q}}_p$. Then for each p we have "local Galois representations"

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to GL(H_{\mathbb{Q}_p}),$$

where $H_{\mathbb{Q}_p} = \bigoplus \mathbb{C}\sigma_i'$. This gives us a "categorification" of the table above:

p	2	3	5	7	11	13	17	19	23	
	$\mathrm{H}_{\mathbb{Q}_2}$	$\mathrm{H}_{\mathbb{Q}_3}$	$\mathrm{H}_{\mathbb{Q}_5}$	$\mathrm{H}_{\mathbb{Q}_7}$	$\mathrm{H}_{\mathbb{Q}_{11}}$	$\mathrm{H}_{\mathbb{Q}_{13}}$	$\mathrm{H}_{\mathbb{Q}_{17}}$	$\mathrm{H}_{\mathbb{Q}_{19}}$	$\mathrm{H}_{\mathbb{Q}_{23}}$	...

If p is unramified, then the inertia subgroup $I \subset \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ acts trivially on $H_{\mathbb{Q}_p}$, so the local Galois representation is unramified. By the Satake isomorphism (Theorem 9.16), this implies that $H_{\mathbb{Q}_p}$ is determined by a semisimple conjugacy class $[x] \in GL_n(\mathbb{C})$, and

$$\#\text{ solutions of } f(x) \text{ mod } p \ = \mathrm{Tr}([x]).$$

For unramified primes, the representation $H_{\mathbb{Q}_p}$ is rather simple. However, for ramified primes, the representation $H_{\mathbb{Q}_p}$ can be quite complicated:

1. The study of $H_{\mathbb{Q}_p}$ lets us define local factors in the Artin L-function.

2. We can hope to understand $H_{\mathbb{Q}_p}$ through the local Langlands correspondence.

Remember our slogan: There is a lot of substance at ramified primes/points!

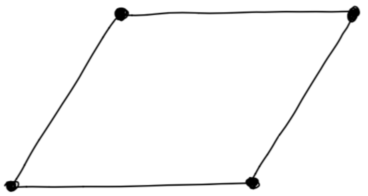
10.1.2 Dimension ≥ 1

The classic example is that of an elliptic curve E; e.g. the projective completion of the curve $y^2+y=x^3+x^2+3x+5$ that we studied in the lecture on the Sato-Tate conjecture, Lecture 4. What is the analogue of the Galois representation H in this setting?

Recall that E is a group, and the complex points of E are

$$E(\mathbb{C}) = \text{ solutions over } \mathbb{C} \ = \mathbb{C}/\Lambda,$$

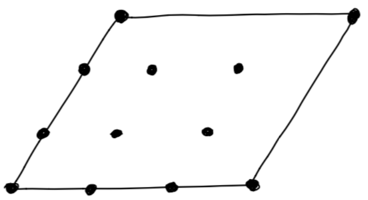
where $\Lambda \subset \mathbb{C}$ is a lattice That is, we obtain $E(\mathbb{C})$ by identifying opposite edges in this picture, where the dots represent elements of Λ:



The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ does not act in any meaningful way on $E(\mathbb{C})$. It does act on $E(\overline{\mathbb{Q}})$, but this is an enormously complicated set, a little too complicated for us! However, for any prime ℓ, we can consider the "ℓ^m-torsion points":

$$E[\ell^m] := \{x \in E(\overline{\mathbb{Q}}) \mid \ell^m \cdot x = 0\} \simeq (\mathbb{Z}/\ell^m\mathbb{Z})^2\,;$$

e.g., for $\ell = 3, m = 1$:



There is a natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[\ell^m]$. The **Tate module** is formed by taking the direct limit of the $E[\ell^m]$:

$$T_\ell(E) := \lim_{\leftarrow} E[\ell^m] \simeq \mathbb{Z}_\ell^2.$$

The Tate module has a continuous action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Moreover, if $E_{\mathbb{F}_p}$ is smooth, then

$$\#E(\mathbb{F}_p) = 1 + p - \mathrm{Tr}(\mathrm{Frob_p}, T_\ell(E)).$$

So in this classic example of an elliptic curve, the Tate modules play the role of the representation H which appeared in the dimension 0 setting. Notice that in the previous section we constructed a single representation H, but there is one Tate module for each prime ℓ. This is an embarassment of riches!

The Tate module $T_\ell(E)$ is an example of "ℓ-adic cohomology:"

$$T_\ell(E) = H^1_{\acute{e}t}(E, \mathbb{Z}_\ell)^*.$$

In general, given a variety X over a field k and a prime ℓ such that multiplication by ℓ is non-zero in k, there is a continuous action of $\mathrm{Gal}(\overline{k}/k)$ on the ℓ-adic cohomology groups $H^*_{\acute{e}t}(X_{\overline{k}}, \mathbb{Q}_\ell)$. Again, it is useful to study these representations via their restriction to local Galois groups $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. We can always calculate these after base change to $\operatorname{Spec}\mathbb{Q}_p$ and at primes of good reduction after base change to $\operatorname{Spec}\mathbb{F}_p$. (**Exercise:** Think about what this statement means for $f(x) \in \mathbb{Z}[x]$.)

In addition to étale cohomology, one has several other methods for associating cohomology groups to the variety X:

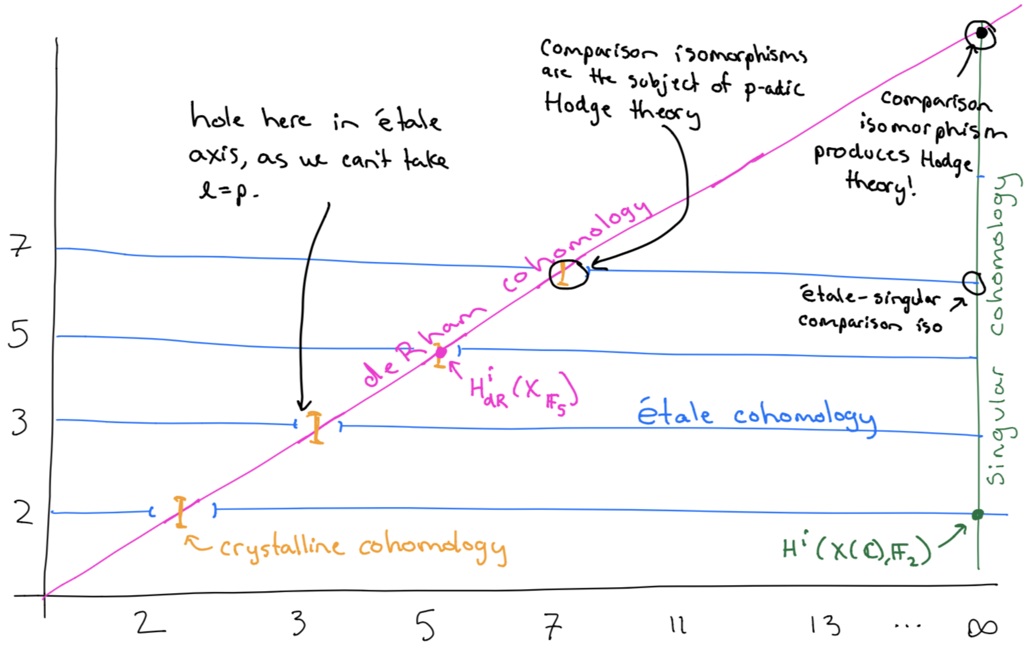
1. **singular cohomology:** $H^i(X(\mathbb{C}), \mathbb{Z})$, $H^i(X(\mathbb{C}), \mathbb{F}_p)$ (related via universal coefficient theorem)

2. **deRham cohomology:** $H^i_{dR}(X)$, $H^i_{dR}(X_{\mathbb{F}_p})$ (cohomology of differential forms)

3. **crystalline cohomology:** $H^i_{crys}(X_{\mathbb{F}_p}/\mathbb{Z}_p)$ (a fancy theory that produces $\mathbb{Z}_p$-vector spaces for $\mathbb{F}_p$-schemes)

Grothendieck's philosophy: All of these cohomology groups should be shadows of a unique object, the "motive" of X.

Scholze: Perhaps the "motive" is more like a sheaf/local system on $\operatorname{Spec}\mathbb{Z} \times \operatorname{Spec}\mathbb{Z}$. **Scholze's ICM picture:**


hole here in étale axis, as we can't take ℓ=p.
Comparison isomorphisms are the subject of p-adic Hodge theory
comparison isomorphism produces Hodge theory!
de Rham cohomology
étale-singular comparison iso
Singular cohomology
$H^i_{dR}(X_{\mathbb{F}_5})$
étale cohomology
crystalline cohomology
$H^i(X(\mathbb{C}),\mathbb{F}_2)$
7
5
3
2
2
3
5
7
11
13
...
∞

when axes meet: comparison isomorphisms (the "glue" of the "sheaf")

Scholze also predicts an archimidean theory for varieties in characteristic p which has been missing since the beginning of this subject!

Recommendation/Exercise: Read section 10 of Scholze's ICM paper.

How does one compare columns in Scholze's picture? In other words, if $G_{\mathbb{Q}_p} = \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q}_p)$, how can we compare

$$\rho : G_{\mathbb{Q}_p} \to GL_n(\mathbb{Q}_\ell) \text{ and } \rho' : G_{\mathbb{Q}_p} \to GL_n(\mathbb{Q}_{\ell'})?$$

The problem is the topology. The solution is given by Weil–Deligne representations.

A topological group Γ is **pro-p** if it is profinite and for all open normal subgroups $N \subset \Gamma$, Γ/N is a p-group.

Example 10.1. Two examples of pro-p-groups are:

1. wild inertia $\subset G_{\mathbb{Q}_p}$, and
2. $1 + p\mathrm{Mat}_n\mathbb{Z}_p = K_1 \subset GL_n(\mathbb{Q}_p)$.

Lemma 10.2. Any continuous group homomorphism

$$\rho : \Gamma \to G$$

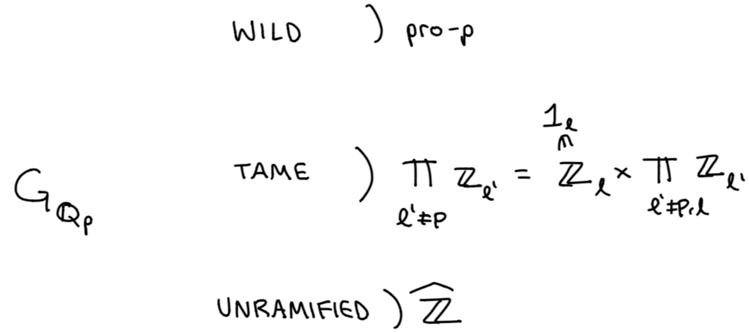
from a pro-p group Γ to a pro-ℓ group G is trivial.

Corollary 10.3. For a pro-p group Γ, any continuous group homomorphism

$$\rho : \Gamma \to GL_n(\mathbb{Q}_p)$$

has finite image.

We have seen (via the ramification filtration) the $G_{\mathbb{Q}_p}$ has the following structure:



WILD
pro-p
$G_{\mathbb{Q}_p}$
TAME
$\prod_{\ell' \neq p} \mathbb{Z}_{\ell'} = \mathbb{Z}_\ell \times \prod_{\ell' \neq p, \ell} \mathbb{Z}_{\ell'}$
1_ℓ
UNRAMIFIED
$\widehat{\mathbb{Z}}$

Grothendieck showed us that the pro-ℓ' group $\prod_{\ell' \neq p, \ell} \mathbb{Z}_{\ell'} \subset I$ must have finite image. Moreover, $\rho(1_\ell) \in GL_n(\mathbb{Q}_\ell)$ is almost unipotent. So what Grothendieck has shown us is that we can "take logs to get Weil–Deligne representations."

Theorem 10.4. (Grothendieck) After identifying $\overline{\mathbb{Q}}_\ell$ with $\mathbb{C}$, one has a canonical injection

$$\left\{ \begin{array}{c} \text{cts. reps.} \\ \rho : G_{\mathbb{Q}_p} \to GL_n(\mathbb{Q}_\ell) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} \text{Weil–Deligne reps} \\ \text{of } G_{\mathbb{Q}_p} \text{ over } \mathbb{C} \end{array} \right\}.$$

Notice that the set on the right is independent of ℓ!

Remark 10.5. We are being a bit lazy, but one can identify the image of this injection.

10.2 Local Langlands correspondence for split groups

Let G be a split reductive algebraic group over $\mathbb{Z}$ determined by the root datum $(X^* \supset R, X_* \supset R^\vee)$, and $\widehat{G}$ its dual group, determined by the opposite root datum $(X_* \supset R^\vee, X^* \supset R)$. Fix a local field K and set $q = |\mathbb{O}_K/\mathfrak{m}_K|$.

A **Weil–Deligne representation in** $\widehat{G}$ is a pair (ρ, e), where

- $\rho : W_K \to \widehat{G}(\mathbb{C})$ is a continuous group homomorphism, and
- $e \in \operatorname{Lie} \widehat{G}(\mathbb{C})$ is a nilpotent element

such that $\rho(g)e\rho(g)^{-1} = |g|e$ for all $g \in W_K$. A Weil–Deligne representation in $\widehat{G}$ is **F-semisimple** if ρ is semisimple.

Example 10.6. A Weil–Deligne representation in GL_n is just an n-dimensional Weil–Deligne representation, as in Section 8.4.

Given a Weil–Deligne representation (ρ, e), consider

$$Z_{\widehat{G}}(\rho, e) = \{g \in \widehat{G} \mid g \cdot (\rho, e) = (\rho, e)\}.$$

Theorem 10.7. (**Local Langlands correspondence**) There is a canonical correspondence

$$\left\{ \begin{array}{c} F\text{-semisimple} \\ \text{WD reps in } \widehat{G} \end{array} \right\}_{/\widehat{G}\text{-conj}} \xleftrightarrow{\text{1:finite}} \left\{ \begin{array}{c} \text{irred smooth} \\ \text{admissible reps} \\ \text{of } G(K) \end{array} \right\}_{/\simeq}$$

Fibres of this map should be indexed by irreducible representations of $Z_{\widehat{G}}(\rho, e)/Z_{\widehat{G}}(\rho, e)^\circ$ and are called "L-packets."

10.3 The Deligne–Langlands conjecture

Last week we examined (for $G = GL_n$) a simple special case of the local Langlands correspondence, the case of unramified WD representations, and found that it followed from the Satake isomorphism. Another slightly less simple special case of the LLC is given by **tamely ramified WD representations with unipotent monodromy** (TRUM). By restricting the correspondence in Theorem 10.7 to TRUM, we hope to obtain a correspondence:

$$\left\{ \begin{array}{c} \text{TRUM; i.e. } (\rho, e) \\ \text{s.t. } \rho \text{ factors} \\ W_K \twoheadrightarrow \mathbb{Z},\ e \text{ arbitrary} \end{array} \right\} \xleftrightarrow{\text{1:finite}} \left\{ \begin{array}{c} \text{reps with an} \\ \text{Iwahori fixed} \\ \text{vector} \end{array} \right\}$$

By analogous arguments to the ones we made last week for GL_n, the set of ρ which factor through $W_K \twoheadrightarrow \mathbb{Z}$ is in bijection with the set of conjugacy classes of semisimple elements in $\widehat{G}$. Hence the left hand side of the correspondence above is in bijection with the set

$$\{(s, e) \mid s \in \widehat{G} \text{ semisimple }, e \in \operatorname{Lie} \widehat{G} \text{ nilpotent s.t. } ses^{-1} = qe\}_{/\widehat{G}\text{-conj}}.$$

The right hand side of the corrspondence above is in bijection with the set

$$\{\text{irred reps of the "Iwahori-Hecke algebra" } \mathcal{H}_{\text{aff}} := \mathcal{H}(I, G(K))\}.$$

This motivates the following conjecture of Deligne–Langlands.

The Deligne–Langlands conjecture: As in the set-up above, let $q = |\mathbb{O}_K/\mathfrak{m}_K|$ be the residue characteristic of the local field K. There is a bijection:

$$\left\{ (s, e, \chi) \;\middle|\; \begin{array}{c} s \in \widehat{G}(\mathbb{C}) \text{ semisimple,} \\ e \in \operatorname{Lie} \widehat{G} \text{ nilpotent, and} \\ \chi \text{ irred rep of } \pi_0(Z_{\widehat{G}}(\rho, e)) \\ \text{s.t. } ses^{-1} = qe \end{array} \right\}_{/\widehat{G}\text{-conj}} \xleftrightarrow{\simeq} \{\text{irred } \mathcal{H}_{\text{aff}}\text{-modules}\}_{/\simeq}$$

Remark 10.8. The affine Hecke algebra $\mathcal{H}(I, G(K))$ has a presentation in which q becomes a variable. The above conjecture can either be understood with fixed $q = \#|\mathbb{O}_K/\mathfrak{m}_K|$ or with q as a variable, in which case q is also a variable on the left hand side.

Recall that the unramified LLC followed from the Satake isomorphism:

$$\underset{\text{“constructible”}}{\mathcal{H}_{\text{sph}} = \mathcal{H}(G(\mathbb{O}_K), G(K))} \xleftrightarrow{\simeq} R(\widehat{G}) = \mathcal{O}\left(\substack{\text{semisimple conj.}\\ \text{classes in } \widehat{G}}\right) \xleftrightarrow{\simeq} \underset{\text{“coherent”}}{K^0(\text{pt}/\widehat{G}) = K^{\widehat{G}}(\text{pt})}$$

Similarly, the TRUM case of the LLC (which reduces to the Deligne–Langlands conjecture) follows from the Kazhdan–Lusztig isomorphism:

$$\underset{\text{“constructible”}}{\mathcal{H}_{\text{aff}}} \xleftrightarrow{\simeq} \underset{\text{“coherent”}}{K^{\widehat{G}\times\mathbb{C}^\times}(St)}$$

Indeed, if $\pi : \widetilde{\mathcal{N}} = T^*\mathcal{B} \to \mathcal{N}$ is the Springer resolution, $\mathcal{B}_e = \pi^{-1}(e)$ is the Springer fibre of a nilpotent element $e \in \mathcal{N}$, and St is the Steinberg variety, the Kazhdan–Lusztig isomorphism (which is not easy to establish!) implies that there is an action of the affine Hecke algebra $\mathcal{H}_{\text{aff}}$ on $K^{Z_{\widehat{G}\times\mathbb{C}^\times}(e)}(\mathcal{B}_e)$. Here we can see that

$$Z_{\widehat{G}\times\mathbb{C}^\times}(e) = \{(g, c) \mid c \cdot geg^{-1} = e\} = \{(g, c) \mid geg^{-1} = c^{-1} \cdot e\}$$

looks very close to the parameters in the Deligne–Langlands conjecture. This action shows us that the K-theory of Springer fibres provides all simple $\mathcal{H}_{\text{aff}}$-modules, thus proving the Deligne–Langlands conjecture.

10.4 Geometric Satake equivalence

There is a geometric upgrade of the Satake isomorphism which has proven to be a major tool in geometric representation theory. Set $K = k((t))$, so $\mathbb{O}_K = k[[t]]$, where $k = \mathbb{C}$ or $\mathbb{F}_q$. Then

$$\mathcal{H}(G(\mathbb{O}_K), G(K)) = \frac{G(\mathbb{O}_K)\text{-invariant functions on the}}{\text{“affine Grassmanian” } \mathcal{G}r_G := G(K)/G(\mathbb{O}_K)}.$$

The **geometric Satake equivalence** is the equivalence of categories:

$$\underset{\text{“constructible”}}{(\text{Perv}_{G(\mathbb{O}_K)}(\mathcal{G}r, \mathbb{C}), *)} \xrightarrow{\simeq} \underset{\text{“coherent”}}{(\text{Rep}\, \widehat{G}_{\mathbb{C}}, \otimes)}$$

This equivalence was key in recent work by V. Laffourgés giving an “automorphic to Galois” correspondence for global function fields.

10.5 Bezrukavnikov’s equivalence

There is also a geometric upgrade of the Kazhdan–Lusztig isomorphism. With $K = k((t))$ as above, the affine Hecke algebra is

$$\mathcal{H}_{\text{aff}} = \text{ Iwahori-invariant functions on } G(K)/I.$$

Here $G(K)/I$ is the set of k-points of the "affine flag variety" $\mathcal{F}l_G$. Roughly, Bezrukavnikov's equivalence is an equivalence of categories

$$\begin{array}{ccc} (D^b_{I\times I}(\mathcal{F}l_G),*) & \xrightarrow{\simeq} & (D^b\mathrm{Coh}^{G\times\mathbb{C}^\times}(St),*) \\ \text{"constructible"} & & \text{"coherent"} \end{array}.$$

Remark 10.9. This is a bit of a lie! It would take several more lecture to precisely describe the categories on each side of this equivalence.

This equivalence has many applications in geometric representation theory. For example, a mod p version of this equivalence would imply everything that we know about modular representations of algebraic groups!

References

[Art24] Emil Artin. Über eine neue art von l-reihen. In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, volume 3, pages 89–108. Springer, 1924.

[Bum98] Daniel Bump. *Automorphic Forms and Representations*, volume 55. Cambridge University Press, 1998.

[Buz17] Kevin Buzzard. Automorphic forms and the Langlands program, MSRI summer school. *Available at `https://www.youtube.com/playlist?list=PLhsb6tmzSpiysoRR0bZozub-MM0k3mdFR`*, 2017.

[CF67] JWS Cassels and A Fröhlich. *Algebraic Number Theory.* Thompson Book Company, Inc., 1967.

[Clo06] L Clozel. The Sato-Tate conjecture. *Current Developments in Mathematics*, 2006(1):1–34, 2006.

[Con01] Keith Conrad. History of class field theory. *This unpublished essay is available online as a PDF file at `www.math.uconn.edu/~kconrad/blurbs/gradnumthy/cfthistory.pdf`*, 2001.

[Gro11] Benedict Gross. Representation Theory and Number Theory, Eilenberg lectures at Columbia University. *Available at `https://www.youtube.com/playlist?list=PL5E0D6DC4BCD8309D`*, 2011.

[KL87] David Kazhdan and George Lusztig. Proof of the Deligne-Langlands conjecture for Hecke algebras. *Inventiones mathematicae*, 87(1):153–215, 1987.

[Kle93] Felix Klein. *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade.* Birkhäuser Verlag, Basel; B. G. Teubner, Stuttgart, 1993. Reprint of the 1884 original, Edited, with an introduction and commentary by Peter Slodowy.

[Kri05] Martin H. Krieger. A 1940 letter of André Weil on analogy in mathematics. *Notices Amer. Math. Soc.*, 52(3):334–341, 2005. Excerpted from ıt Doing mathematics [World Scientific Publishing Co., Inc., River Edge, NJ, 2003; MR1961400].

[Lan90] R. P. Langlands. Representation theory: its rise and its role in number theory. In *Proceedings of the Gibbs Symposium (New Haven, CT, 1989)*, pages 181–210. Amer. Math. Soc., Providence, RI, 1990.

[Mil97] James S Milne. Class Field Theory. *Lecture notes available at* ***https://www.jmilne.org/math/CourseNotes/cft.html***, 1997.

[Miy11] Katsuya Miyake. Takagi's class field theory: From where? and to where? *RIMS Kôkyûroku Bessatsu*, B25:125–160, 2011.

[MS16] Barry Mazur and William Stein. *Prime Numbers and the Riemann Hypothesis.* Cambridge University Press, 2016.

[Sch17] Peter Scholze. p-adic geometry. *ICM Lecture, arXiv:1712.03708*, 2017.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Tat79] J. Tate. Number theoretic background. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pages 3–26. Amer. Math. Soc., Providence, R.I., 1979.

[Wey16] Hermann Weyl. Über die gleichverteilung von zahlen mod. eins. *Mathematische Annalen*, 77(3):313–352, 1916.

[You16] Alexander Youcis. Weil-Deligne representations and p-adic Hodge theory: motivation. *Available at:* ***https://ayoucis.files.wordpress.com/2016/11/weil-deligne-representations-2.pdf***, 2016.