Langlands Correspondence and Bezrukavnikov’s Equivalence

Anna Romanov

April 20, 2020

This document contains notes from a course taught by Geordie Williamson at the University of Sydney in 2019-2020. The primary goal of these lectures was 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.
# Contents

1 Lecture 1 (March 8, 2019): Reciprocity Laws .................................................. 6  
1.1 Reciprocity Laws ......................................................................................... 6  
1.2 Higher dimensional varieties ...................................................................... 8  
1.3 What is going on here? What does this have to do with representation theory? 8  
1.4 Schematic picture of the Langlands correspondence ................................. 9  
1.5 Chebotarev density theorem ....................................................................... 10  
1.6 Solutions to Exercises .................................................................................. 12  

2 Lecture 2 (March 15, 2019): Review of some algebraic number theory .......... 14  
2.1 Number fields ............................................................................................. 14  
2.2 An analogy ................................................................................................... 15  
2.3 The fundamental exact sequence ................................................................ 16  
2.4 Ramification ................................................................................................ 17  
2.5 The case of Galois extensions .................................................................... 19  
2.6 Solutions to exercises .................................................................................. 20  

3 Lecture 3 (March 21, 2019): $L$-functions ..................................................... 23  
3.1 The Riemann $\zeta$-function ....................................................................... 23  
3.2 Why do we care? ......................................................................................... 24  
3.3 Dirichlet $L$-functions ............................................................................... 25  
3.4 Dedekind $\zeta$-functions ........................................................................... 26  
3.5 Walking across the bridge .......................................................................... 27  
3.6 Artin $L$-functions ..................................................................................... 28  
3.7 Solutions to exercises .................................................................................. 30  

4 Lecture 4 (April 12, 2019): The Sato-Tate conjecture .................................... 32  
4.1 Equidistribution in representation theory .................................................. 32  
4.2 Elliptic curves and the Sato-Tate conjecture ............................................. 35  
4.3 Equidistribution and $L$-functions ................................................................ 39  
4.4 Solutions to exercises .................................................................................. 40  

5 Lecture 5 (April 26, 2019): Infinite Galois theory and global class field theory .................................................. 41  
5.1 Infinite Galois theory ............................................................................... 42  
5.2 Global class field theory, first version ...................................................... 44  
5.3 Global class field theory à la Artin ............................................................ 45  
5.4 Solutions to exercises .................................................................................. 47  

6 Lecture 6 (May 3, 2019): Structure of local Galois groups, local class field theory .................................................. 48  
6.1 Motivating local class field theory: A trip across the bridge ..................... 48  
6.2 Local class field theory .............................................................................. 51  
6.3 Structure of Galois groups of local fields ................................................ 54  
6.4 Solutions to exercises .................................................................................. 55
<table>
<thead>
<tr>
<th>Lecture 13 (September 13, 2019): Springer resolution, conormal space, Steinberg variety</th>
<th>104</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.1 Many examples of Springer fibres</td>
<td>105</td>
</tr>
<tr>
<td>13.2 The conormal space</td>
<td>109</td>
</tr>
<tr>
<td>13.3 The Steinberg variety</td>
<td>111</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lecture 14 (October 11, 2019): Springer correspondence, Borel-Moore homology, convolution algebras</th>
<th>113</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1 Borel-Moore homology</td>
<td>115</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lecture 15 (October 18, 2019): More convolution algebras, Kazhdan–Lusztig isomorphism, Bezrukavnikov’s equivalence (rough statement)</th>
<th>119</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1 Equivariant $K$-theory</td>
<td>120</td>
</tr>
<tr>
<td>15.2 Kazhdan–Lusztig isomorphism</td>
<td>122</td>
</tr>
<tr>
<td>15.3 Bezrukavnikov’s equivalence: rough outline</td>
<td>124</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lecture 16 (November 1, 2019): Motivating the constructible side of Bezrukavnikov’s equivalence</th>
<th>126</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1 Weil conjectures</td>
<td>126</td>
</tr>
<tr>
<td>16.2 The Hecke algebra, revisited</td>
<td>129</td>
</tr>
<tr>
<td>16.3 Perverse sheaves on $\mathbb{P}^1_{\mathbb{C}}$</td>
<td>131</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lecture 17 (March 6, 2020): Constructible and perverse sheaves on curves</th>
<th>133</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.1 Perverse sheaves</td>
<td>134</td>
</tr>
<tr>
<td>17.2 Nearby and vanishing cycles, Beilinson glueing</td>
<td>139</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lecture 18 (March 13, 2020): Nearby cycles, vanishing cycles, and Beilinson glueing on curves</th>
<th>141</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.1 Glueing</td>
<td>148</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lecture 19 (March 27, 2020): Overview of proof that the derived category of perverse sheaves agrees with constructible derived category</th>
<th>150</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.1 Yoneda extensions</td>
<td>153</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lecture 20 (April 3, 2020): Highest weight categories, perverse sheaves for affine stratifications, back to Kazhdan–Lusztig isomorphism</th>
<th>160</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.1 Highest weight categories</td>
<td>161</td>
</tr>
<tr>
<td>20.2 Where are we going for the next few weeks?</td>
<td>167</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lecture 21 (April 10, 2020): Equivariant $K$-theory of the Steinberg variety and the antishperical module</th>
<th>169</th>
</tr>
</thead>
<tbody>
<tr>
<td>21.1 Equivariant $K$-theory</td>
<td>169</td>
</tr>
<tr>
<td>21.2 Equivariant $K$-theory of the Steinberg variety</td>
<td>172</td>
</tr>
<tr>
<td>21.3 The spherical and anti-spherical modules</td>
<td>174</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>22.1</td>
<td>Notation and set-up</td>
</tr>
<tr>
<td>22.2</td>
<td>The case of $SL_3$</td>
</tr>
<tr>
<td>22.3</td>
<td>The general case</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>( p )</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td># of sol’s mod ( p )</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>...</td>
</tr>
<tr>
<td>( p ) mod 4</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

\[ 1 \rightarrow (\mathbb{F}_p^\times)^2 \rightarrow \mathbb{F}_p^\times \rightarrow \{\pm 1\} \rightarrow 1, \]

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

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

Let’s do another example. Consider the equation

\[ x^2 - 3 = 0. \]

We ask the same question and compute:

<table>
<thead>
<tr>
<th>( p )</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td># of sol’s mod ( p )</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>...</td>
</tr>
<tr>
<td>( p ) mod 12</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>5</td>
<td>7</td>
<td>11</td>
<td>5</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>
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

\[
x^2 - 3 \text{ has 2 solutions mod } p \iff \left( \frac{3}{p} \right) = 1
\]

\[
\iff \left( \frac{p}{3} \right) (-1)^{\epsilon(p)\epsilon(3)} = 1
\]

\[
\iff \left( \frac{p}{3} \right) (-1)^{\epsilon(p)} = 1
\]

\[
\iff \begin{cases} 
p = 1 \mod 3 \text{ and } p = 1 \mod 4 \\
p = 2 \mod 3 \text{ and } p = 3 \mod 4
\end{cases}
\]

\[
\iff p = 1 \text{ or } -1 \mod 12.
\]

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

<table>
<thead>
<tr>
<th>( p )</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
<th>43</th>
<th>47</th>
<th>53</th>
</tr>
</thead>
<tbody>
<tr>
<td># of sol’s mod ( p )</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>( y ) ( \backslash ) ( x )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>( \times )</td>
<td>( \times )</td>
<td>( \times )</td>
<td>( \times )</td>
<td>( \checkmark )</td>
</tr>
<tr>
<td>1</td>
<td>( \checkmark )</td>
<td>( \times )</td>
<td>( \times )</td>
<td>( \times )</td>
<td>( \times )</td>
</tr>
<tr>
<td>2</td>
<td>( \times )</td>
<td>( \times )</td>
<td>( \checkmark )</td>
<td>( \times )</td>
<td>( \times )</td>
</tr>
<tr>
<td>3</td>
<td>( \times )</td>
<td>( \times )</td>
<td>( \checkmark )</td>
<td>( \times )</td>
<td>( \times )</td>
</tr>
<tr>
<td>4</td>
<td>( \checkmark )</td>
<td>( \times )</td>
<td>( \times )</td>
<td>( \times )</td>
<td>( \times )</td>
</tr>
</tbody>
</table>

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 \( \text{approximately} \ p \) 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.

<table>
<thead>
<tr>
<th>( p )</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
<th>43</th>
<th>47</th>
<th>53</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td># ( ST(p) )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-4</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>-4</td>
<td>-10</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>...</td>
</tr>
</tbody>
</table>

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

\[ \Gamma = \text{Gal}(K/\mathbb{Q}), \]

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

\[ \Gamma \circ H = \bigoplus_{i=1}^{n} \mathbb{C} \alpha_i. \]
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, $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{p^n}$. Recall that the Galois group $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z}$ is generated by the Frobenius map

$$\text{Frob}_p : x \mapsto x^p.$$  

Then $\mathbb{F}_p = (\mathbb{F}_{p^n})^{\text{Frob}_p}$, and the number of solutions of $\bar{f}$ is the number of fixed points of $\text{Frob}_p$ on $\{\alpha_1, \ldots, \alpha_n\}$. For such a $p$ (“unramified”) and after a choice (“prime in $\mathcal{O}$ above $p$”), we get a bijection

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

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

**Remark 1.2.** Different choices of “prime in $\mathcal{O}$ over $p$” result in conjugate $\text{Frob}_p$’s. Hence, it is best to think of $\text{Frob}_p$ as a conjugacy class instead of an individual element.

The upshot of the discussion above is that

$$\# \text{ solutions modulo } p = \# \text{ fixed points of } \text{Frob}_p \text{ on } \{\bar{\alpha}_1, \ldots, \bar{\alpha}_n\} = \# \text{ of fixed points of } \text{Frob}_p \text{ on } \{\alpha_1, \ldots, \alpha_n\} = \text{Tr}(\text{Frob}_p, H),$$

where $H$ is the permutation representation introduced at the beginning of this section. The number $\text{Tr}(\text{Frob}_p, H)$ 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 $p \nmid \Delta(f)$,

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

### 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.

```
"geometric" reps $V$ of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ↦ "character" $\text{Tr}(\text{Frob}_p, V)$ ↦ automorphic forms

↓

$L$-functions (analytic)
```

From any “geometric” representation of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, 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 $\text{Tr}(\text{Frob}_p, V)$, we can attach the associated “$L$-function,” which is an analytic object. (For example, when we start with
the trivial representation of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the resulting $L$-function is the Riemann $\zeta$-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 $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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 $\text{Tr}(\text{Frob}_p, H)$ as a “character,” we would like to know at least that the set $\{\text{Frob}_p\}$ for all $p$ unramified cover the set of all conjugacy classes of $\Gamma$. This is a deep theorem.

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

$$\{p \text{ unramified } | \text{Frob}_p = C\}$$

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 $\text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} = \{\text{id}, s\}$. In this example, all $p \neq 2$ are unramified. Then for such an unramified $p$,

$$\text{Frob}_p : i \mapsto i^p.$$

Hence,

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

**Exercise 1.5.** (Mandatory) Check that $\text{Frob}_p$ 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 \( \text{Gal}(\mathbb{Q}(\phi)/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} = \langle s \rangle \).

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 \( p \),

\[
\text{Frob}_p : \zeta \mapsto \zeta^p.
\]

Hence,

\[
\text{Frob}_p : \begin{cases} 
\phi \mapsto \phi & \text{if } p = 1 \text{ or } 9 \mod 10 \\
\phi \mapsto s(\phi) & \text{if } p = 3 \text{ or } 7 \mod 10
\end{cases}
\]

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,

\[
\# \text{ solutions modulo } p = 5 \iff \text{ all solutions in } \mathbb{F}_{p^n} \text{ are defined over } \mathbb{F}_p \\
\iff \text{ all solutions are fixed by } \overline{\text{Frob}}_p \\
\iff \text{Frob}_p = \text{id}.
\]

Since \( \text{id} \) is in its own conjugacy class, we expect \( f(x) \) to have 5 solutions modulo \( p \) about \( 1/60\text{th} \) 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 Frob_p : i ↦→ 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 \( k \in \mathbb{Z}_+ \)), \( \mathbb{F}_{p^k} \cong \mathbb{F}_p[x]/(g(x)) \), 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 \( \text{Frob}_3 : x ↦→ x^3 \) acts on the set of roots by sending \( i ↦→ 2i \) and \( 2i ↦→ i \). Therefore, \( \text{Frob}_3 \) must act on the set \( \{i, -i\} \) by sending \( i ↦→ -i \) and \(-i ↦→ i \). Since \( i^3 = -i \), we see that indeed \( \text{Frob}_3 : i ↦→ i^3 \).

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, \( \text{Frob}_5 : x ↦→ x^5 \) sends \( 2 ↦→ 2 \) and \( 3 ↦→ 3 \). Therefore, \( \text{Frob}_5 \) must send \( i ↦→ i = i^5 \) and \(-i ↦→ (-i)^5 \), so again, \( \text{Frob}_5 : i ↦→ i^5 \).

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

\[
\text{Frob}_p = \bar{id} \iff x^p = x \text{ for all roots } x \text{ of } \bar{f} \iff x \in \mathbb{F}_p \iff p = 1 \mod 4,
\]
and

\[
\text{Frob}_p = \bar{s} \iff x^{p^2} = x \text{ but } x^p \neq x \text{ for all roots } x \text{ of } \bar{f} \iff x \not\in \mathbb{F}_p \iff p = 3 \mod 4.
\]

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

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

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

Note that \( \Phi_m(x)x^m - 1 \), so for any root \( \alpha \) of \( \Phi_m \) or \( \bar{\Phi}_m \) for any prime \( p \), \( \alpha^m = 1 \). The Galois group of this extension is \( \Gamma = (\mathbb{Z}/m\mathbb{Z})^\times \). Since \( \Gamma \) is abelian, conjugacy classes are singletons. The order of \( \Gamma \) 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 \( \{p| \text{Frob}_p = x\} \) 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
then \( \overline{\text{Frob}}_p = \overline{\text{Frob}}_q \), since for any root \( \alpha \) of \( \Phi_m \), \( \alpha^p = \alpha^q = \alpha^a \). Since \( \text{Frob}_p \) acts on the set of roots of \( \Phi_m \), as \( \overline{\text{Frob}}_p \) acts on the set of roots of \( \Phi_m \), this implies that \( \text{Frob}_p = \text{Frob}_q \).

Similarly, if \( \text{Frob}_p = \text{Frob}_q \) for two primes \( p \neq q \), then \( \alpha^p = \alpha^q \) for any root \( \alpha \) of \( \Phi_m \), and \( p = q \mod m \). Hence,

\[ p = q \mod m \iff \text{Frob}_p = \text{Frob}_q \]

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. \( \square \)
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 \( \mathcal{O} \subset K \) consisting of all elements of \( K \) which satisfy a monic polynomial with coefficients in \( \mathbb{Z} \). The ring of integers \( \mathcal{O} \) 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. \( K = \mathbb{Q}(i) \), \( \mathcal{O} = \mathbb{Z}[i] \).
2. \( K = \mathbb{Z}(\sqrt{2}) \), \( \mathcal{O} = \mathbb{Z}[\sqrt{2}] \).
3. \( K = \mathbb{Q}(\sqrt{5}) \), \( \mathcal{O} = \mathbb{Z}[\phi] \), where \( \phi = \frac{1+\sqrt{5}}{2} \).

Generally, for a complicated extension, it is not easy to find \( \mathcal{O} \).

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

\[
\text{Tr} : K \to \mathbb{Q} \\
\text{Nm} : K^\times \to \mathbb{Q}^\times
\]

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

\[
K \times K \to \mathbb{Q} \\
(x, y) := \text{Tr}(xy).
\]

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

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

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 $\mathcal{O} = \mathbb{Z}[i]$ has basis $\{\alpha_1, \alpha_2\} = \{1, i\}$. We can compute

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

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

**Exercise 2.5.**

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

$$\mathcal{O} = \begin{cases} \mathbb{Z}[\sqrt{\alpha}] & \text{if } \alpha \not\equiv 1 \pmod{4} \\ \mathbb{Z}[\frac{1+i\sqrt{\alpha}}{2}] & \text{if } \alpha \equiv 1 \pmod{4} \end{cases}.$$

Hence, calculate

$$\text{Disc}(K) = \begin{cases} 4\alpha & \text{if } \alpha \not\equiv 1 \pmod{4} \\ \alpha & \text{if } \alpha \equiv 1 \pmod{4} \end{cases}.$$

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 $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, 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.

\[
\begin{align*}
\{ \text{finite extensions of } \mathbb{C}(x) = \text{Frac} \mathbb{C}[x] \text{ (called function fields)} \} & \hookleftarrow \{ \text{smooth complex projective curves } C \text{ over } \mathbb{P}^1 \mathbb{C} \} \\
& \hookrightarrow \{ \text{compact Riemann surfaces with a map to } \mathbb{P}^1 \mathbb{C} \}
\end{align*}
\]
The first arrow going left is given by taking the function field of the curve. We can also go in the other direction. Given 

\[
K \leftrightarrow \mathbb{O} \\
\downarrow \quad \downarrow \\
\mathbb{C}(x) \leftrightarrow \mathbb{C}[x]
\]

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

Similarly, there is a bijection

\[
\left\{ \text{finite extensions } K \text{ of } \mathbb{F}_p(x) \right\} \leftrightarrow \left\{ \text{smooth projective curves } C \text{ over } \mathbb{P}^1_{\mathbb{F}_p} \right\}.
\]

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:

function fields over \(\mathbb{C}\) \(<<\) function fields over \(\mathbb{F}_p\) \(<<\) 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 \(p \neq 0\) is maximal, and
- every fractional ideal has a unique factorization \(I = \prod p_i^{e_i}\), where \(p_i\) are prime ideals.

Denote by \(J = \bigoplus_{p \neq 0} \mathbb{Z}_p\) the group of nonzero fractional ideals under this product. We have the following fundamental exact sequence:

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

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 \( \mathcal{O}^\times \) is finitely generated of rank \( r_1 + r_2 - 1 \).

**Exercise 2.9.** Compute \( \mathcal{O}^\times \) 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,

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

and we have the following exact sequence:

\[ \{1\} \to \mathbb{C}^\times \to K^\times \to \mathcal{P} \hookrightarrow \bigoplus_{x \in C} \mathbb{Z}x \to \text{Pic}(C) \to 0. \]

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

**Remark 2.10.** The group \( \text{Pic}(C) = \text{Jac}(C) \times \mathbb{Z} \) 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 \( \mathcal{O}^\times \) 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 \( K_0(\mathcal{O}) = \mathbb{Z} \oplus \mathcal{C} \ell(K) \).

### 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 $C = \text{Spec} \mathbb{F}_p[x, y]/(y^2 = x^3 + 1) \to \text{Spec} \mathbb{F}_p[x]$. Fibres of this map over a point $x = \lambda$ are singular if $\lambda$ 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 $\mathcal{O}$ its ring of integers. For each prime $p \in \mathbb{Z}$, the corresponding ideal in $\mathcal{O}$ decomposes into the product of prime ideals in $\mathcal{O}$:

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

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 $\mathcal{O}/\mathfrak{p}_i$ is a finite extension of $\mathbb{F}_p$ (so $\mathcal{O}/\mathfrak{p}_i = \mathbb{F}_{p^{f_i}}$ 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 \( \mathcal{O} \) if and only if \( p \nmid \text{Disc}(K) \).

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 \( \mathcal{O} = \mathbb{Z}[i] \) and \( \text{Disc}(K) = -4 \). (See Exercise 2.4.) Since \((1 + i)^2 = 1 + 2i - 1 = 2i\), we see that the ideal \((2) \subset \mathcal{O}\) 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) \( \theta \) of \( K \). We can assume without loss of generality that \( \theta \in \mathcal{O} \). Then \( \theta \) satisfies a monic polynomial \( f(x) \in \mathbb{Z}[x] \) of degree \( n \), so \( \mathbb{Z}[\theta] \subset \mathcal{O} \) is of finite index \( m \). Then for \( p \) such the \( p \nmid m \) and \( p \nmid \text{Disc}(K) \)

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

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

\[
\text{(p) splits completely } \iff f \text{ is reducible modulo } p \\
\text{(p) is inert } \iff f \text{ is irreducible modulo } p.
\]

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 \( \text{Gal}(K/\mathbb{Q}) = G \). Then \( G \) acts on \( \mathcal{O} \), and Frobenius proved the following result.

Theorem 2.18. If \((p) = \prod p_i^{e_i}\), then \( G \) acts transitively on the primes \( p_i \).
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 \(n = ef g_p\). Fix a prime \(p_i = p\) lying over \((p)\). Denote by \(G_p\) the stabilizer of \(p\) in \(G\) (the “decomposition group”). Then

\[ |G/G_p| = \# \text{ primes over } p = g_p. \]

so \(|G_p| = ef\). Let \(I_p\) be the subgroup of \(G_p\) which acts trivially on \(\mathcal{O}_p\) (the “inertia group”). This group has order \(e\). We have the following exact sequence

\[ 1 \to I_p \to G_p \to \text{Aut}(\mathcal{O}/p) \to \mathbb{Z}/f\mathbb{Z}. \]

Since \(\mathcal{O}/p \cong \mathbb{F}_{p^f}\), the group \(\text{Aut}(\mathcal{O}/p)\) is generated by \(\text{Frob}_p : x \mapsto x^p\). If \(p\) is unramified (i.e. \(p \nmid \text{Disc}(K)\)), then \(e = 1\), so \(I_p\) is trivial and \(G_p \cong \mathbb{Z}/f\mathbb{Z}\). In this case, \(\text{Frob}_p \in G_p\) is defined to be the element that maps to \(\text{Frob}_p \in \text{Aut}(\mathcal{O}/p)\). A different choice of \(p\) lying over \(p\) results in conjugate \(G_p\) and conjugate \(\text{Frob}_p\). This explains rigorously the \(\text{Frob}_p\) 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 \(\text{Frob}_p\) must fix all roots of \(\bar{f}(x)\) in \(\mathbb{F}_p\), so \(\text{Frob}_p = \text{id}\) 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 \(\text{Frob}_p\) will lie in a conjugacy class \(C\) about \(|C|/|\Gamma|\) of the time. We see that in our computation,

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

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

**Solution:** See Exercise 2.5.

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

\[
\mathcal{O} = \begin{cases} 
\mathbb{Z}[\sqrt{\alpha}] & \text{if } \alpha \not\equiv 1 \pmod{4} \\
\mathbb{Z}\left[\frac{1+\sqrt{\alpha}}{2}\right] & \text{if } \alpha \equiv 1 \pmod{4}
\end{cases}
\]

Hence, calculate

\[
\text{Disc}(K) = \begin{cases} 
4\alpha & \text{if } \alpha \not\equiv 1 \pmod{4} \\
\alpha & \text{if } \alpha \equiv 1 \pmod{4}
\end{cases}
\]

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

\textit{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,

\[
a + b\sqrt{\alpha} \in \mathcal{O} \iff p_{a,b}(x) \in \mathbb{Z}[x] \\
\iff 2a \in \mathbb{Z} \text{ and } a^2 - \alpha b^2 \in \mathbb{Z}.
\]

If \( a + b\sqrt{\alpha} \in \mathcal{O} \) and \( a \not\in \mathbb{Z} \), 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 \( 2b \not\in \mathbb{Z} \), then \( a^2 - \alpha b^2 \) if not an integer. (Or else \((2b)^2 \) would be expressible as \( \frac{\gamma}{\alpha} \) for some integer \( \gamma \equiv 1 \pmod{4} \), which is impossible since \( \alpha \) 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 \( \alpha = 1 \pmod{4} \). We conclude that there exists an algebraic integer \( a + b\sqrt{\alpha} \in \mathcal{O} \) with \( a, b \not\in \mathbb{Z} \) if and only if \( \alpha = 1 \pmod{4} \). In this case, \( \frac{1+\sqrt{\alpha}}{2} \in \mathcal{O} \), since this is a root of the monic polynomial \( x^2 - x + \frac{1-\alpha}{4} \in \mathbb{Z}[x] \), and \( \mathbb{Z}\left[\frac{1+\sqrt{\alpha}}{2}\right] = \mathcal{O} \). If \( \alpha \not\equiv 1 \pmod{4} \), then \( p_{a,b} \in \mathbb{Z}[x] \) if and only if \( a, b \in \mathbb{Z} \), so \( \mathbb{Z}[\sqrt{\alpha}] = \mathcal{O} \).

Once we know this, it is easy to calculate the discriminant of \( K \). If \( \alpha \not\equiv 1 \pmod{4} \), the set \( \{1, \sqrt{\alpha}\} \) is a basis for \( \mathcal{O} = \mathbb{Z}[\sqrt{\alpha}] \). With this choice of basis, the three matrices corresponding to multiplication by \( 1, \sqrt{\alpha} \), and \( \alpha \) 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

\[
\text{Disc}(K) = \det \begin{pmatrix} 2 & 0 \\ 0 & 2\alpha \end{pmatrix} = 4\alpha.
\]
If $\alpha = 1 \mod 4$, then $\left\{1, \frac{1+\sqrt{\alpha}}{2}\right\}$ is a basis for $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{\alpha}}{2}\right]$. 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

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

From this, we calculate that the discriminant of $K$ is

$$\text{Disc}(K) = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{\alpha+1}{4} \end{pmatrix} = \alpha.$$

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

$K$ is totally real $\iff r_2 = 0 \iff (\cdot, \cdot)$ 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 $\mathcal{O}^\times$ 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 $\mathcal{C}(K)$ and $\mathcal{O}^\times$ are finite if $C$ is an affine curve.

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

**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 $(p) \subset \mathcal{O}$. Show that $n = \sum_{i=1}^{g_p} e_if_i$, 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 $\zeta$-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. $\zeta(2) = \frac{\pi^2}{6}$), and noticed that the $\zeta$-function may also be given as the Euler product:

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

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 $\zeta(2) = \frac{\pi^2}{6}$, the irrationality of $\pi^2$ also implies that the right hand product must be infinite.

Riemann showed that $\zeta$ 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 $\zeta(s) - \frac{1}{s} \zeta(1) = -\log(1-s)$ converges for $\Re(s) > 0$), and “trivial zeros” at $-2, -4, \ldots$. Furthermore, he established the functional equation: $\Lambda(s) := \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$ satisfies

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

Here $\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}dx$ 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
\[
\psi(n) = \sum_{m \leq n} \Lambda_{vm}(m).
\]

**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 \( \rho \) of the Riemann \( \zeta \)-function.

In other words,
\[
x - \psi(x) = \log(2\pi) + \sum_{\rho} \frac{x^\rho}{\rho},
\]
so the zeros of the Riemann \( \zeta \)-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 \( \frac{x^{2n} - 1}{2n} = -\frac{1}{2n\pi} \) decays very quickly, so for large \( x \), trivial zeros have almost no effect on the formula.
• A pair \( \rho, \bar{\rho} \) of non-trivial conjugate zeros: Each such pair contributes

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

where \( \lambda \) and \( \gamma \) depend in a simple way on \( \rho \) and \( \bar{\rho} \). So \( \Re(\rho) \) is crucial in the contribution of \( \rho \) 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, \( \lambda \) 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 \( \zeta(s) \) 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

\[
\{ p \text{ prime} \mid p = a \mod m \}.
\]

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: \( x \mapsto e^{2\pi ij/\phi(m)} \) 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 $\chi$ induces a character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$.

Such a function $\chi$ 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 $\chi$ is trivial, we recover the Riemann $\zeta$-function. If $\chi$ is not trivial, then $L(\chi, s)$ is entire.

Dirichlet’s theorem (that $\{p | p = a \mod m\}$ is infinite, with distribution $\frac{1}{\phi(m) \log x}$) is an easy consequence of the fact that $L(\chi, 1) \neq 0$ if $\chi$ 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 $\zeta$-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 $\zeta$-function.

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

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

This sum admits an Euler product because of the uniqueness of factorization of ideals in $\mathcal{O}$. 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 $K = \mathbb{Q}(i) \supset \mathcal{O} = \mathbb{Z}[i]$. Then

$$
\zeta_K(s) = \prod_{p \subseteq \mathcal{O} \text{ prime}} \frac{1}{1 - \mathcal{N}p^{-s}}
$$

$$
= \left( \frac{1}{1 - 2^{-s}} \right) \prod_{(p) \text{ s.t. } (p) \text{ splits}} \left( \frac{1}{1 - \mathcal{N}p^{-s}} \right) \left( \frac{1}{1 - \mathcal{N}p^{-s}} \right) \prod_{(p) \text{ s.t. } (p) \text{ is inert}} \left( \frac{1}{1 - \mathcal{N}p^{-2s}} \right)
$$

$$
= \prod_{p=1 \mod 4} \left( \frac{1}{1 - p^{-s}} \right) \prod_{p=3 \mod 4} \left( \frac{1}{1 - p^{-s}} \right)^2 \prod_{p \equiv 3 \mod 4} \left( \frac{1}{1 - p^{-s}} \right) \left( \frac{1}{1 + p^{-s}} \right)
$$

$$
= \zeta(s) L(\chi, s),
$$

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 witnessing 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 $\mathcal{O}$ 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,

$$
\zeta_{\mathbb{A}^1_{\mathbb{F}_p}}(s) = \sum_{\mathcal{N}I \neq 0 \in \mathbb{F}_p[x]} (\mathcal{N}I)^{-s}
$$

$$
= \sum_{f \text{ monic}} (\mathcal{N}(f))^{-s}
$$

$$
= \sum_{d \geq 1} \left( \sum_{f \text{ monic degree } d} (p^d)^{-s} \right)
$$

$$
= \sum_{d \geq 0} p^d (p^d)^{-s}
$$

$$
= \sum_{d \geq 0} (p^{-s+1})^d
$$

$$
= \frac{1}{1 - p^{-s+1}}.
$$
So $\zeta_{\mathbb{A}_1 F_p}(s)$ is a rational function with a unique pole at $s = 1$ and no zeros. Since $\zeta_{\mathbb{A}_1 F_p}(s)$ 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 $\mu$ 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 $G = \text{Gal}(K/\mathbb{Q})$, and $d_K = \text{Disc}(K)$. Recall from previous lectures that:

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

Fix a finite dimensional complex representation

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

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

$$L_{ur}(V, s) = \prod_{p \nmid d_K} \frac{1}{\det(1 - p^{-s} \text{Frob}_p|_V)}.$$
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 $\zeta$-function as a special case.

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

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

Therefore, by quadratic reciprocity,

$$L_{ur}(\rho, s) = \prod_{p} \left(1 - \left(\frac{p}{\alpha}\right)p^{-s}\right)^{-1}$$

$$= \prod_{p} (1 - \chi(p)p^{-s})^{-1}$$

$$= L(\chi, s) \text{ up to finitely many factors}$$

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 $\zeta$-function.)

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

\[
\begin{align*}
\psi(2) &= \log 2 \\
\psi(3) &= \log 2 + \log 3 \\
\psi(4) &= \log 3 + \log 4 \\
\psi(5) &= \log 3 + \log 4 + \log 5 \\
\psi(6) &= \log 3 + \log 4 + \log 5 \\
\psi(7) &= \log 3 + \log 4 + \log 5 + \log 7 \\
\psi(8) &= \log 3 + \log 5 + \log 7 + \log 8 \\
\psi(9) &= \log 3 + \log 5 + \log 7 + \log 8 + \log 9
\end{align*}
\]

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

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

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 $\text{Res} > 1$. 
(c) For a Galois extension $K/\mathbb{Q}$, let $V_{\text{reg}}$ be the regular representation of $G$. Show that $L_{\text{ur}}(V_{\text{reg}}, s) = \zeta_K(s)$ up to finitely many factors.

**Solution (to part (c)):** Assume $p \in \mathbb{Z}$ is unramified. Recall that for any prime $p \subset \mathcal{O}$ above $p$, we have a bijection $G_p \rightarrow \text{Aut}(\mathcal{O}/p)$, and Frob$_p \in G$ is defined to be the element that maps to $\overline{\text{Frob}}_p : x \mapsto x^p \in \text{Aut}(\mathcal{O}/p)$ under this bijection. Furthermore, $\mathcal{O}/p \cong \mathbb{F}_{p^f}$, so Frob$_p$ has order $f$, and $Np = \# \mathcal{O}/p = p^f$.

The regular representation of $G$ is the representation $\rho : G \rightarrow GL(V_{\text{reg}})$, where the vector space $V_{\text{reg}} = \mathbb{C}[G]$ is the group algebra of $G$, and $\rho(g)$ is given by left multiplication by $g$. For any vector $v_1 \in V_{\text{reg}}$, repeated action by $\phi = \rho(\text{Frob}_p)$ generates an $f$-dimensional subspace $V_1 \subset V_{\text{reg}}$ with basis $\{v_1, \phi v_1, \ldots, \phi^{f-1} v_1\}$. We can choose any vector $v_2 \not\in V_1$, and again repeated action by $\phi$ generates a $f$-dimensional subspace $V_2$ with basis $\{v_2, \phi v_2, \ldots, \phi^{f-1} v_2\}$.

Continuing this process, we obtain a basis for $V_{\text{reg}}$ of the form

$$\{v_1, \phi v_1, \ldots, \phi^{f-1} v_1, v_2, \phi v_2, \ldots, \phi^{f-1} v_2, \ldots, v_g, \phi v_g, \ldots, \phi^{f-1} v_g\},$$

where $g_p$ is the number of primes over $p$. (Recall that the degree of the extension $K/\mathbb{Q}$ is $n = fg_p$.) With this choice of basis, $\phi$ acts on the subspace $V_i \subset V_{\text{reg}}$ 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 $L_{\text{ur}}(V_{\text{reg}}, s)$. We conclude that

$$L_{\text{ur}}(V_{\text{reg}}, s) = \prod_{p \notin dK} \frac{1}{\det(I - p^{-s} \phi)} = \prod_{p \notin dK} \left(\frac{1}{1 - p^{-fs}}\right)^{g_p} = \prod_{p \subset \mathcal{O} \text{ prime}} \frac{1}{1 - Np^{-s}} = \zeta_K(s),$$

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 its relationship to the global Langlands picture. We will see that seemingly innocuous statements in the Langlands correspondence can have very powerful repercussions.

4.1 Equidistribution in representation theory

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

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

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 $e(x) = \exp(2\pi ix)$. 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

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

**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 $f(x) \in \mathbb{R}[x]$ 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 \( \chi \) 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 \( \mu \), 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 \( \chi, \chi' \) 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 \( \chi \).

**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

<table>
<thead>
<tr>
<th>Haar measure</th>
<th>#( C_i )</th>
<th>conj. class</th>
<th>triv</th>
<th>nat</th>
<th>sgn</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/6</td>
<td>1</td>
<td>( C_1 )</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>1/2</td>
<td>3</td>
<td>( C_2 )</td>
<td>1</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>1/3</td>
<td>2</td>
<td>( C_3 )</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
</tbody>
</table>

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 $\Lambda \cong \mathbb{Z}^2 \hookrightarrow \mathbb{C}$. Hence

$$\left\{ \text{elliptic curves over } \mathbb{C} \right\} / \text{iso} \cong \left\{ \text{lattices } \Lambda \subset \mathbb{C} \right\} / \text{iso} \rightarrow \text{period ratio} \rightarrow \frac{SL_2(\mathbb{Z})}{H},$$

where $H$ is the upper half plane. The quotient $\frac{SL_2(\mathbb{Z})}{H}$ 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

$$\text{End}_{\text{Lie gp}}(E) = \mathbb{Z}^2$$

$$(z, w) \mapsto (z^m, w^n) \leftrightarrow (m, n)$$

But $E$ has additional structure - it is an elliptic curve ($E \cong \mathbb{C}/\Lambda$), 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,

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

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 with 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 $\Lambda$ 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 $E_{\overline{\mathbb{F}}_p} = E \times \text{Spec} \mathbb{F}_p$ 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 $\alpha_p$’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 $\text{Frob}_p$ on (étale, but don’t worry if you don’t know what this is) cohomology:

$$\text{dim} : \begin{array}{ccc} 1 & 2 & 1 \\ H^0(E) & H^1(E) & H^2(E) \\ \circ & \circ & \circ \\ \text{Frob}_p = 1 & \text{Frob}_p \sim \begin{pmatrix} \gamma_p & 0 \\ 0 & \overline{\gamma_p} \end{pmatrix} & \text{Frob}_p = p \end{array}$$
The Grothendieck-Lefshetz trace formula is

\[ \#E(\mathbb{F}_p) = \sum (-1)^i \text{Tr} (\text{Frob}_p : H^i) = 1 + p - (\gamma_p + \overline{\gamma}_p), \]

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 \( \gamma_p \), 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 \( p \).

\[ S^1_+ := \]

\[ E(\mathbb{F}_p) \text{ has many points ("maximal") } \]

\[ E(\mathbb{F}_p) \text{ has few points ("minimal") } \]

\[ \text{error term} = 0 \]

**Sato–Tate conjecture (1960):** Suppose \( E \) does not have complex multiplication. If we identify \( S^1_+ \iso [0, \pi] \), 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 \( \mu_{\theta_p} \) is the Dirac distribution.

*In other words, the Sato–Tate conjecture is that the \( \theta_p \)'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 \( \theta_p \) 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 $\theta_p$ 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 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: $Gal(K/\mathbb{Q}) \leftrightarrow SU(2)$. 

38
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 $\chi$, 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 $\rho$ is the representation afforded by $\chi$. 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 $\chi$, $L(\chi, s)$ 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

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

satisfies the extra assumption above. (Here $S^m_\chi$ is the $m^{th}$ symmetric power of the representation with character $\chi$ sending $\text{Frob}_p \mapsto \begin{pmatrix} \theta_p & 0 \\ 0 & \theta_p^{-1} \end{pmatrix}$.) Then the Sato-Tate conjecture holds!
Recall our cartoon of the Langlands correspondence:

\[
\begin{array}{c}
\{ \text{“geometric” } n\text{-dimensional rep’ns of } \text{Gal}(K) = \text{Gal}(\overline{K}/K) \} \\
\xrightarrow{\text{finite-to-one}} \\
\{ \text{“automorphic” rep’ns of } \text{GL}_n(\mathbb{A}) \} \\
\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\
L\text{-functions}
\end{array}
\]

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 \(\rho : \text{Gal}(K) \to GL_n \xrightarrow{\text{alg rep’ns}} GL_m\) 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 \(\text{Gal}(K)\). 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 $\text{Gal}(\overline{K}/K)$. Because $\overline{K} = \bigcup_{n \geq 1} K_n$, we have an injection

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

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

$$\text{Gal}(\overline{K}/K) = \lim_{\leftarrow} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$$ 

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

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

(b) Show that $\hat{\mathbb{Z}}$ 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

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

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 $\text{Gal}(L''/K) \to \text{Gal}(L'/K)$. This determines the image of this injection; that is,

$$\text{Gal}(L/K) = \lim_{\leftarrow} \text{Gal}(L'/K).$$

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

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

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

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

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

for $L'/K$ finite Galois.

For a general group $G$, define

$$\hat{G} = \lim_{\leftarrow} \frac{G}{H},$$

$$H \subseteq G \text{ normal finite index}$$

The group $G$ is **profinite** if $G \cong \hat{G}$, otherwise, say $\hat{G}$ 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 $\mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$. What does this group look like? Here’s a picture for $p = 3$: [Diagram of the profinite completion of $\mathbb{Z}_p$]
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

$$\{K \subset L' \subset L\} \leftrightarrow \left\{ \begin{array}{c} \text{closed subgroups} \\ \text{of } \text{Gal}(L/K) \end{array} \right\}$$

$$L^H \leftrightarrow H$$

$$L' \leftrightarrow \text{Gal}(L/L')$$

Moreover, under this bijection,

- finite extensions $\leftrightarrow$ closed and open subgroups
- Galois extensions $\leftrightarrow$ normal subgroups

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 $K$. (So $0\widehat{\mathbb{Z}}$ 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** $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

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 $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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 $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *This is one reason why representations are so important in the Langlands program!*

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

\[
\text{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) = \lim_{\leftarrow \mathbb{Z}/m\mathbb{Z})^\times = \prod_p \mathbb{Z}_p^\times.}
\]

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 Jugendtraum to show that any continuous character \( \chi : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times \) “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 \( \mathfrak{O} \subset K \) be the ring of integers. A place \( \nu \) is an equivalence class of nontrivial multiplicative norms

\[
| \cdot |_\nu : K \to \mathbb{R}_{\geq 0}
\]
on \( K \).

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

- **Finite places**: \( |x|_\nu := \left( \#\mathfrak{O}/\mathfrak{p} \right)^{-\text{val}_\mathfrak{p}(x)} \) for \( \mathfrak{p} \subset \mathfrak{O} \) prime.
- **Real places**: \( |x|_\nu := |i(x)| \) for some real embedding \( i : K \hookrightarrow \mathbb{R} \),
- **Complex places**: \( |x|_\nu := |i(x)|^2 \) 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 \( \#\mathfrak{O}/\mathfrak{p} \) above. The reason for the the above normalization is the beautiful **product formula**: For \( x \in K^\times \),

\[
\prod_{\text{places } \nu} |x|_\nu = 1.
\]

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 à la Artin

Fix a finite abelian Galois extension $L/K$ with abelian Galois group $\text{Gal}(L/K)$. Let $\mathcal{O}_L \subset L$ and $\mathcal{O}_K \subset K$ be the rings of integers, and let $S_f \subset \mathcal{O}_K$ be the set of ramified primes. We have seen that for a prime $p \subset \mathcal{O}_K$ such that $p \not\in S_f$, there is a corresponding conjugacy class $\text{Frob}_p \in \text{Gal}(L/K)$. In general $\text{Frob}_p$ is only defined up to conjugacy, but since we are assuming that $\text{Gal}(L/K)$ is abelian, $\text{Frob}_p$ is a single element. Hence we obtain a map (the Artin map):

$$\mathcal{J}^{S_f} = \bigoplus_{p \not\in S_f} \mathbb{Z}p \rightarrow \text{Gal}(L/K)$$

$$\sum m_p p \mapsto \prod \text{Frob}_p^{m_p}$$

Here $\mathcal{J}^{S_f} \subset \mathcal{J}$ is a subgroup of the group of nonzero fractional ideals $\mathcal{J} = \bigoplus_{\text{primes } p} \mathbb{Z}p$ 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 $v_i \not\in S$. 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 $K^\times$:

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

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

The set $K^{m,1}$ is the set of $\lambda$ which are “$m$ close to 1.” We have the following maps:

$$\begin{array}{cccc}
K^\times & \text{val} & \rightarrow & \mathcal{J} \\
\downarrow & & \downarrow & \rightarrow \mathcal{C}_{\ell_K} \\
K^S & \text{val} & \rightarrow & \mathcal{J}^S \\
\downarrow & & \downarrow & \\
K^{m,1} & \text{val} & \rightarrow & \mathcal{J}^{S_f} \\
\end{array}$$
The Ray class group associated to the modulus $m$ is the quotient
\[ \mathcal{C}^m_K := \mathcal{J}^S / \text{val}(K^{m,1}). \]

**Example 5.14.** If $m = 0$, then $\mathcal{C}^0_K = \mathcal{C} K$ 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
\[ K^S = \left\{ \frac{a}{b} \mid a, b \text{ coprime to } p \right\} = \mathbb{Z}_p^\times, \quad \text{and} \]
\[ K^{m,1} = \left\{ \frac{a}{b} \mid a, b \text{ coprime to } p \text{ and } \text{val}_p(a/b - 1) \geq n \right\} = \left\{ \frac{a}{b} \mid \frac{a}{b} = 1 \mod p^n \right\}. \]
Hence
\[ K^S/K^{m,1} = \mathbb{Z}_p^\times/K^{m,1} = (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathcal{C}^m_K. \]

**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 $\text{supp}(m) \cap \{\text{finite places}\} = S_f$ such that $\text{val}(K^{m,1})$ is contained in the kernel of the Artin map. Moreover, for any modulus $m$ and any quotient $q : \mathcal{C}^m_K \to Q$, there exists an abelian extension $L/K$ ramified only at primes in $\text{supp}(m)$ such that
\[ \mathcal{C}^m_K \xrightarrow{\text{Artin}} \text{Gal}(L/K) \]
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 $\epsilon$ close to 1 for all places $v \in S$, then $\text{val}(\lambda)$ is in the kernel of the Artin map.

**Example 5.19.** Consider the extension $\mathbb{Q}(i)/\mathbb{Q}$, which is the splitting field of the polynomial $x^2 + 1$. The ramified primes are 2 and $\infty$ (but we haven’t discussed what it means for $\infty$ to be ramified, so we are sweeping this under the rug), so $S_f = \{(2)\}$. For any $p \neq 2$, $\text{Frob}_p(i) = ip$, hence in the Galois group, $\text{Frob}_p \leftrightarrow p \mod 4 \in (\mathbb{Z}/4\mathbb{Z})^\times = \text{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. We have
\[ \mathcal{J}^{S_f} = \left\{ \frac{a}{b} \mid a, b \text{ coprime to } 2 \right\} = \mathbb{Z}_2^\times. \]
Hence the Artin map is the natural map
\[ \mathbb{Z}_2^\times \to (\mathbb{Z}/4\mathbb{Z})^\times. \]
Its kernel is the set of all elements satisfying a “congruence condition at 2:”
\[ \left\{ \lambda \in \mathbb{Z}_2^\times \mid \text{val}_2(\lambda - 1) \geq 2 \right\}. \]
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 $\mathcal{C}_K^0 = \mathcal{C}_K$. Hence the existence statement in Theorem 5.17 implies that there exists an unramified everywhere extension $L/K$ with $\text{Gal}(L/K) = \mathcal{C}_K$. This extension is the Hilbert class field.

5.4 Solutions to exercises

Exercise 5.2.
(a) Show that $\hat{\mathbb{Z}} = \prod_{p \text{ prime}} \mathbb{Z}_p$.
(b) Show that $\hat{\mathbb{Z}}$ 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 $\text{Gal}(L/K)$ is closed (therefore compact) in $\prod_{K \leq L \leq \bar{L}} \text{Gal}(L'/K)$.

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

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

for $L'/K$ finite Galois.

Exercise 5.10. Use Kronecker Jugendtraum to show that any continuous character $\chi : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times$ “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.
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 Jugendtraum (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 $\text{Frob}_p$ (then everyone promptly forgot for 40 years).

- **Hilbert (189-1900):** first correct proof of Jugendtraum for $\mathbb{Q}$, emphasis on “places at $\infty$,” introduction of Hilbert class field, 12th 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 $\text{Frob}_p$!), 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:

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

\[
\begin{array}{c}
\mathbb{C} \\
\cup \\
\circ \quad \text{disc} \leftrightarrow \text{Spec } \mathbb{C}[[t]] \\
\cup \\
\times \quad \text{punctured disc} \leftrightarrow \text{Spec } \mathbb{C}((t))
\end{array}
\]

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

\[
\text{Gal} \left( \overline{\mathbb{C}((t))/\mathbb{C}((t))} \right) = \lim_{\leftarrow} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}.
\]

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 $p \subset \mathcal{O}_K$), then we know what it means for a place $v'$ (corresponding to $q \subset \mathcal{O}_L$) of $L$ to “lie over $v$.” $v'$ lies over $v$ precisely when $q$ is a prime above $p$ in the sense of lecture 2 (i.e. $p\mathcal{O}_L \subset q$).

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

\[
\begin{array}{c}
L \xleftarrow{i'} \mathbb{K}' \\
\downarrow \\
K \xleftarrow{i} \mathbb{K}
\end{array}
\]

\[1\]Recall that we saw last lecture that $\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \hat{\mathbb{Z}}$ 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

\[
\begin{array}{ccc}
L & \rightarrow & L_v' \\
\downarrow & & \downarrow \\
K & \rightarrow & K_v
\end{array}
\]

Set

\[
G_v = \{ \sigma \in \text{Gal}(L/K) \mid \sigma \text{ acts continuously on } L_v \} = \begin{cases} 
G_q & \text{if } v \text{ is finite} \\
\{1\} & \text{if } v \text{ is unramified infinite} \\
\mathbb{Z}/2\mathbb{Z} & \text{if } v \text{ is ramified infinite}
\end{cases}
\]

Here $G_q \subset \text{Gal}(L/K)$ is the decomposition group corresponding to the prime $q \subset \mathcal{O}_L$ determining $v'$.

**Remark 6.3.** In the last case (when $v$ is ramified infinite), we get a canonical element $c \in \text{Gal}(L/K)$ 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 $\text{val} : K \rightarrow \mathbb{Z} \cup \{\infty\}$. In $K$ lies its ring of integers $\mathcal{O}_K$, with maximal idea $\mathfrak{m}$ generated by a “uniformizer” $\pi \in \mathfrak{m}$:

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

The field $k_K = \mathcal{O}_K/\mathfrak{m}$ is the residue field. Note that in this setup, $K$, $\mathcal{O}_K$ 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 $\text{val}$ (i.e. $K$ has the topology coming from $\mathcal{O}_K = \lim \mathcal{O}_K/\mathfrak{m}_K^n$), 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 $\sigma \in \text{Gal}(L/K)$ preserves $\mathcal{O}_L/\mathcal{O}_K$ and $\mathfrak{m}_L/\mathfrak{m}_K$, and thus acts on $k_L/k_K$. Hence we get maps 

$$1 \rightarrow I_{L/K} \hookrightarrow \text{Gal}(L/K) \twoheadrightarrow \text{Gal}(k_L/k_K) \rightarrow 1,$$

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

$$1 \rightarrow I_{\overline{K}/K} \hookrightarrow \text{Gal}(\overline{K}/K) \twoheadrightarrow \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \hat{\mathbb{Z}} \rightarrow 1.$$ 

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

1. the diagram

$$
\begin{array}{cccccc}
1 & \longrightarrow & I_{\overline{K}/K}^{ab} & \longrightarrow & \text{Gal}(\overline{K}/K)^{ab} & \longrightarrow & \text{Gal}(\overline{k_K}/k_K) \cong \hat{\mathbb{Z}} \\
\| & & \uparrow r_K & & & & \\
1 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^\times & \overset{\text{val}}{\longrightarrow} & \mathbb{Z}
\end{array}
$$

commutes, and

2. if $L/K$ is finite Galois, then

$$
\begin{array}{ccc}
L^\times & \overset{r_L}{\longrightarrow} & \text{Gal}(\overline{L}/L)^{ab} \\
\downarrow \text{Norm}_{L/K} & & \downarrow \text{res} \\
K^\times & \overset{r_K}{\longrightarrow} & \text{Gal}(\overline{K}/K)^{ab}
\end{array}
$$

commutes.

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

---

2The canonical map $r_K$ is sometimes called the “reciprocity map.”
1. $K = \mathbb{R}$: In the diagram

$$
\begin{align*}
\mathbb{C}^\times & \xrightarrow{r_{\mathbb{C}}} \text{Gal}(\mathbb{C}/\mathbb{C}) = \{1\} \\
\downarrow \text{Norm}_{\mathbb{C}/\mathbb{R}} & \downarrow \\
\mathbb{R}^\times & \xrightarrow{r_{\mathbb{R}}} \text{Gal}(\mathbb{C}/\mathbb{R})
\end{align*}
$$

the map $r_{\mathbb{R}} : -1 \mapsto \text{complex conjugation}$ 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 Norm$_{\mathbb{C}/\mathbb{R}}$).

2. $K = \mathbb{C}((t))$\footnote{Note that $K$ doesn’t quite fit our assumptions so LCFT doesn’t apply, but morally it fits into the same picture.} The map

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

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

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

$$
\begin{array}{cccc}
I_{\overline{K}/K} & \xrightarrow{} & W_K & \xrightarrow{} \mathbb{Z} \\
| & | & \downarrow & | \\
I_{\overline{K}/K} & \xrightarrow{} & \text{Gal}(\overline{K}/K) & \xrightarrow{} \hat{\mathbb{Z}}
\end{array}
$$

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:

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

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

\textbf{Theorem 6.8. (Local Langlands correspondence for $GL_n(K)$) (Harris-Taylor)} There is a bijection

$$
\hom_{cts}(W_K, GL_n(\mathbb{C}))/\text{conj} \overset{1:1}{\longleftrightarrow} \left\{ \text{irreps of } GL_n(K) \text{ in } \mathbb{C}\text{-vector spaces} \right\}.
$$

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

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

$$\text{Hom}_{cts}(W_K, GL_1(\mathbb{C}))_{/\text{conj}} = \text{Hom}_{cts}(W_K, \mathbb{C}^\times)$$

$$= \text{Hom}_{cts}(W_K^b, \mathbb{C}^\times)$$

$$= \text{Hom}_{cts}(K^\times, \mathbb{C}^\times)$$

$$= \{\text{irreps of } GL_1(K)\}.$$

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

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

where $\zeta_n$ is an $n^{th}$ root of unity. Hence

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

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

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

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 $\overline{\mathbb{F}}_p = \bigcup_{p|n} \mathbb{F}_p(\zeta_n)$, we have that

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

We conclude that

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

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

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

where $I_{L/K} = \{\sigma \mid \sigma \text{ acts trivially on } k_L\}$, and $\text{Gal}(k_L/k_K)$ is generated by the canonical generator Frob. Note that $\text{Gal}(L/K)$ preserves $\mathbb{O}_K$, hence $\mathfrak{m}_K$, hence the valuation $\nu_K$, hence acts on $\mathbb{O}_K/\mathfrak{m}_K^3$, hence acts continuously on $L$.

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

54
Exercise 6.13. Prove Lemma 6.12 (Hint: use the fact that any $\sigma \in \text{Gal}(L/K)$ is automatically continuous.)

Set $I := I_{L/K}$, $I_0 := I$, and $I_j := \{\sigma \in I \mid \sigma(\pi)\pi^{-1} \in 1 + m^j_L\}$ 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

$I_0/I_1 \xrightarrow{\sigma(\pi)\pi^{-1}} k^*_L$,
$I_j/I_{j+1} \hookrightarrow (1 + m^j_L)/(1 + m^{j+1}_L) \cong k_L$

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** 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 $\sigma \in \text{Gal}(L/K)$ is automatically continuous.)

\footnote{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 $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is misguided because $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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.

$$\mathbb{Q} \leftrightarrow \text{"étale site" Spec } \mathbb{Q} \text{ (something like a space)}$$

choice of $\overline{\mathbb{Q}} \leftrightarrow$ choice of “base point” of Spec $\mathbb{Q}$

Then the étale fundamental group $\pi_1^{\text{ét}}(\text{Spec } \mathbb{Q}, \mathbb{Q}) = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

The punchline: The fundamental group $\pi_1(X, x)$ depends on base point $x$, but $\text{Rep } \pi_1(X, x) \simeq \{\text{local systems on } X\}$ 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

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

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 $\exp : \text{Lie} G \to G$ 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 $\Gamma$ 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 $\Gamma$ 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 $\Gamma$ factors through a finite group, $\varphi : \Gamma \to \Gamma/N \to G$. \qed

**The Moral:**

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

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 $GL_n(\mathbb{C})$. 

57
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 perspective 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:

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

the “split torus,” and

$$T_a = \left\{ \lambda \in \mathbb{F}_q^{\times} \subset GL_2(\mathbb{F}_q) \mid \text{Norm}(\lambda) = 1 \right\} \simeq \mathbb{Z}/(q+1)\mathbb{Z},$$

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

$$\mathbb{F}_q^{\times} \subset GL_2(\mathbb{F}_q) = GL_2(\mathbb{F}_q).$$

Roughly,

$$\left\{ \text{irred reps of } SL_2(\mathbb{F}_q) \text{ over } \mathbb{C} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \chi : T_s \to \mathbb{C}^\times \right\}_{/\chi \sim \chi^{-1}} \sqcup \left\{ \theta : T_a \to \mathbb{C}^\times \right\}_{/\theta \sim \theta^{-1}}$$

“principal series”

“discrete series”

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 conjugacy classes are roughly in bijection with characteristic polynomials, so the sizes of the sets above are roughly

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

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”

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

58
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,

\[ \{ \text{irred admissible reps of } SL_2(\mathbb{R}) \} \overset{1:1}{\leftrightarrow} \{ \text{cts characters of } T_s \simeq \mathbb{R} \times \mathbb{Z}/2\mathbb{Z} \} \bigcup \{ \text{cts characters of } T_a \simeq SO_2 \simeq S^1 \} \]

“principal series”

“discrete series”

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:

\[ \{ \text{conjugacy classes of max’l tori in } GL_2(K) \} \leftrightarrow \{ \text{semisimple } K \text{-algebras } L \text{ s.t. } \dim_K L = 2 \} \]

\[ L^x \leftrightarrow L \]

There are two cases:

1. Split torus: \( L \simeq K \times K \), so maximal torus is of the form \( L^x \simeq K^x \times K^x \).

2. Anisotropic torus: \( L/K \) degree 2 extension, so maximal torus is of the form \( L^x \).

Applying our analogy from earlier, we might expect

\[ \{ \text{irred blah reps of } GL_2(K) \} \overset{\text{roughly } 1:1}{\leftrightarrow} \{ \text{pairs of characters } \chi_1, \chi_2 : K^x \to \mathbb{C}^x \} \bigcup \{ \text{characters } \theta : L^x \to \mathbb{C}^x \text{ where } L/K \text{ is degree 2} \} \].

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

\[ \{ \text{irred blah reps of } GL_2(K) \} \overset{\text{roughly } 1:1}{\leftrightarrow} \{ \chi_1 \otimes \chi_2 : W_K \to GL_2(\mathbb{C}) \} \bigcup \{ \text{Ind}_{W_L}^{W_K}(\theta) : W_L \to GL_2(\mathbb{C}) \} \].

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 \( \text{Ind}_{W_L}^{W_K}(\theta) \) 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

$$K_j = \{ g \in GL_n(\mathcal{O}_K) \mid g = id \mod m_K^j \}.$$ 

Note that $GL_n(\mathcal{O}_K)/K_j \simeq GL_n(\mathcal{O}_K/m_K^j)$ 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 $\pi \in \mathcal{O}_K \subset K$ be a uniformizer.

1. Establish the Bruhat decomposition:

$$GL_n(K) = \bigsqcup_{\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n \atop \lambda_i \in \mathbb{Z}} GL_n(\mathcal{O}_K) \left( \begin{array}{cccc} \pi^{\lambda_1} & & & \\ & \pi^{\lambda_2} & & \\ & & \ddots & \\ & & & \pi^{\lambda_n} \end{array} \right) GL_n(\mathcal{O}_K)$$

($\text{Hint: Gaussian elimination.}$)

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

3. Hence or otherwise, show that $GL_n(\mathcal{O}_K)$ 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:

\[\mathbb{Z} \times \supset \mathbb{Z}_3^\times \times \text{maximal compact}\]
A space is **totally disconnected** if every point admits a family of compact open neighborhoods; e.g. \( \text{GL}_n(K) \) 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 \( K \) of characteristic 0. We give \( V \) the discrete topology.

**Definition 7.9.** A representation \( \rho : G \to \text{GL}(V) \) is

1. **smooth** if for all \( v \in V \), \( \text{stab}_G v \) is open, and

2. **admissible** if for all open \( K \subset G \), \( V^K \) is finite dimensional.

**Example 7.10.**

1. The trivial representation \( K \) is smooth and admissible, \( K^\infty \) is smooth but not admissible.

2. The standard representation of \( \text{GL}_n(K) \) on \( K^n \) is not smooth, as \( \text{stab}_{\text{GL}_n(K)} v \) 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 \( \mathcal{L}^2(G) \).) We claim that this representation is smooth and admissible.

   - **Smooth:** Let \( \varphi \in \mathcal{F} \). Then for all \( x \in Z_p \), there is a neighborhood \( U_x \) such that \( \varphi|_{U_x} \) is constant. This forms a covering of \( Z_p \) by open neighborhoods of the form \( U_x = x + p^nZ_p \). Since \( Z_p \) is compact, there exists a finite subcovering \( U_{x_1}, \ldots, U_{x_m} \). Then \( \varphi \) is fixed by \( p^nZ_p \), where \( n = \text{Max}\{n_i\} \), so the the stablizer of \( \varphi \) is open, hence the representation is smooth.

   - **Admissible:** A basis of open neighborhoods of 0 is given by \( p^mZ_p, m \geq 0 \). Then

     \[
     \mathcal{F}^{p^mZ_p} = \{ \varphi \mid \varphi \text{ is constant on } p^mZ_p\text{-orbits}\}
     = \{ \varphi : Z/p^mZ \to \mathbb{C} \}
     \]

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

The vector space

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

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,

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

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 \( \pi \in \mathcal{O}_K \subset K \) be a uniformizer.

1. Establish the Bruhat decomposition:

\[
\text{GL}_n(K) = \bigsqcup_{\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n} \text{GL}_n(\mathcal{O}_K) \begin{pmatrix}
\pi^{\lambda_1} & & & \\
& \pi^{\lambda_2} & & \\
& & \pi^{\lambda_3} & \\
& & & \ddots
\end{pmatrix} \text{GL}_n(\mathcal{O}_K)
\]

(\textit{Hint: Gaussian elimination.})

2. Use (\ast) to classify the subgroups \( \text{GL}_n(\mathcal{O}_K) \subset H \subset \text{GL}_n(K) \).

3. Hence or otherwise, show that \( \text{GL}_n(\mathcal{O}_K) \) is a maximal compact subgroup of \( \text{GL}_n(K) \).

**Exercise 7.11.** Show that any smooth finite dimensional representation of \( \text{GL}_n(K) \) factors over \( \det : \text{GL}_n(K) \to K^\times \). (\textit{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 } \text{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 \textit{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 
\[ m_K \subset \mathcal{O}_K \subset K \]
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 
\[ K_j = \{ g \in GL_n(\mathcal{O}_K) \mid g = id \mod m_j^i \} \]
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 $K_0/K_i \simeq GL_n(\mathcal{O}_K/m_i^i)$; 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 
\[ V^{K_i} = \bigoplus_{\rho \in \hat{K}_0/K_i} V^{K_i}(\rho), \]
where $V^{K_i}(\rho)$ is the $\rho$-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 $\rho$. Passing to the limit, we obtain a decomposition 
\[ V = \bigoplus_{\rho \in \hat{K}_0} V(\rho). \]
Here $\hat{K}_0$ 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, $\rho$ 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 $\rho$, we have

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

Hence

$$V^{K_i} = \bigoplus_{\rho \in \widehat{K}_0 \atop \rho|_{K_i} = \text{triv}} V(\rho).$$

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. \qed

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

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

Hence,

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

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 $\text{stab}_{GL_n(K)} \xi$ is open. Define the smooth dual

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

**Lemma 8.4.** Assume $V$ is a smooth representation of $GL_n(K)$. If $V = \bigoplus_{\rho \in \hat{K}_0} V(\rho)$, then $\hat{V} = \bigoplus_{\rho \in \hat{K}_0} V(\rho)^\ast$.

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

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

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:** $|x|_v := (\# \mathcal{O}_K/p)^{-\text{val}_p(x)}$ for some prime $p \subset \mathcal{O}_K$,
- **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 $\mu$ be the additive Haar measure on $K_v$. The measure $\mu$ is unique up to a scalar. Define

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

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

**Example 8.5.**

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

2. $K_v = \mathbb{C}$: For $z \in \mathbb{C}$, and
3. $K = \mathbb{Q}_p$: Recall that $\mathbb{Z}_p = \bigcup_{0 \leq m < p} m + p\mathbb{Z}_p$, 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 $K_j := 1 + m_j^K \subset O_K^\times$ is normal in $K^\times$, and the group

$$K^\times/K_j \simeq \mathbb{Z} \times (O_K/m_j^K)^\times$$

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 $\chi : O_K^\times \to \mathbb{C}$ 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

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

for all $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B\}$. 

67
Example 8.7.  

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

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 \( \chi_1, \chi_2 \), \( I(\chi_1, \chi_2) \) 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 \( |g|^{|1/2} \) 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

\[ \Phi : I(| \cdot |^{1/2}, | \cdot |^{-1/2}) \to \mathbb{C} \]

\[ \varphi \mapsto \int_{K_0} \varphi d\mu. \]

(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 $\Phi$ 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 $\Phi$, 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 $\text{Rep} GL_2(K)$ 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 $\sigma \in \text{Gal}(L/K)$.

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 $L_\theta$ on $\mathbb{P}^1_{\mathbb{F}_q} \setminus \mathbb{P}^1(\mathbb{F}_q)$. Taking the first cohomology yields a cuspidal representation $R_{T_a}^G(\theta)$.

- 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:

$$
\begin{array}{ccc}
\{1\text{-dim'l reps of } L^\times\} & \xrightarrow{\text{Ind}_{W_L}^{W_K}} & \{\text{irred. smooth ad. reps of } GL_1(L)\} \\
\downarrow \text{Ind}_{W_L}^{W_K} & & \downarrow \text{BC=\"base change\"}
\end{array}
$$

$$
\begin{array}{ccc}
\{n\text{-dim'l reps of } K^\times\} & \xrightarrow{\text{BC=\"base change\"}} & \{\text{irred smooth reps of } GL_n(K)\} \\
& & \\
\end{array}
$$

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 \((\rho, V, N)\), where

- \( V \) is an \( n \)-dimensional complex vector space,
- \( \rho : W_K \to GL(V) \) is a continuous representation, and
- \( N \in \text{End}(V) \) is nilpotent such that

\[ \rho(x)N\rho(x)^{-1} = |x|N \quad (*) \]

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 \( \rho = \left( \begin{array}{c|c} |\cdot| \chi & 0 \\ \hline 0 & \chi \end{array} \right) \) for any character \( \chi : W_K \to \mathbb{C}^\times \) and \( N = \left( \begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array} \right) \)

form a Weil-Deligne representation. Indeed, for \( x \in W_K \),

\[ \rho(x)N\rho(x)^{-1} = \left( \begin{array}{c|c} |x|\chi(x) & 0 \\ \hline 0 & \chi(x) \end{array} \right) \left( \begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array} \right) \left( \begin{array}{c|c} |x|^{-1}\chi(x)^{-1} & 0 \\ \hline 0 & \chi(x)^{-1} \end{array} \right) \]

\[ = \left( \begin{array}{c|c} 0 & |x| \\ \hline 0 & 0 \end{array} \right) \]

\[ = |x| \left( \begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array} \right). \]

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 \( \tilde{\text{Frob}} \in W_K \) be any lift of Frobenius. Show that a Weil-Deligne representation is \( F \)-semisimple if and only if \( \tilde{\text{Frob}} \) 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

\[
\left\{ \begin{array}{c|c} F \text{-semisimple} \\ \text{2-dimensional} \\ \text{Weil-Deligne reps} \end{array} \right\} /\sim \leftrightarrow \left\{ \begin{array}{c|c} \text{irred. smooth admiss.} \\ \text{reps of } GL_2(K) \end{array} \right\} /\sim
\]
Moreover, this bijection is given as follows.

\[
\chi_1/\chi_2 = |\cdot|^{\pm 1} : \left( \begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix}, N = 0 \right) \leftrightarrow C(\chi_1, \chi_2)
\]

\[
\chi_1/\chi_2 = |\cdot|^{\pm 1} : \left( \begin{pmatrix} |\chi| \cdot | & 0 \\ 0 & \chi \end{pmatrix}, N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right) \leftrightarrow S(\chi, |\cdot|\chi)
\]

\[
\chi_1/\chi_2 \neq |\cdot|^{\pm 1} : \left( \begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix}, N = 0 \right) \leftrightarrow I(\chi_1, \chi_2)
\]

\[
L/K, \theta : L^\times \to \mathbb{C}^\times : (\text{Ind}_{W_K}^{W_L}(\theta), N = 0) \leftrightarrow BC_{L/K}(\theta)
\]

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 \( \widetilde{\text{Frob}} \in W_K \) be any lift of Frobenius. Show that a Weil-Deligne representation is \( F \)-semisimple if and only if \( \widetilde{\text{Frob}} \) is semisimple.
9 Lecture 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:

\[
\begin{align*}
L & \hookrightarrow \mathcal{O}_L \hookrightarrow \mathfrak{m}_L \xrightarrow{\pi_L} \\
K & \hookrightarrow \mathcal{O}_K \hookrightarrow \mathfrak{m}_K \xrightarrow{\pi_L}
\end{align*}
\]

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

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

**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

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

Then

\[\text{Gal}(L/K) \supset I_0 \supset I_1 \supset I_2 \supset \cdots \supset \{1\}\]

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

**Key Facts:**

1. The ramification filtration is a finite exhaustive filtration.

2. There is an injection $I_0/I_1 \hookrightarrow \mathcal{O}_L^\times/(1 + \mathcal{O}_L^\times) \simeq k_L^\times : \sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L}$. 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 $\text{Gal}(L/K)/I_{L/K}$ 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 $L = \mathbb{Q}_p(\sqrt[\nu]{p})$ of $K = \mathbb{Q}_p$. Here $\pi_L = \nu\sqrt[\nu]{p}$ and $\pi_K = p$ are uniformizers.

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

The Galois group of this extension is

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

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

$$I_{\mathcal{K}/K} \hookrightarrow \text{Gal}(\mathcal{K}/K) \twoheadrightarrow \hatsym{Z}.$$  

We would like to pass to the limit to obtain a ramification filtration of the inertia subgroup $I_{\mathcal{K}/K}$ 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 $I_{L/K}^\lambda$ of the inertia subgroup of the absolute Galois group indexed by rational numbers:

$$\text{Gal}(\mathcal{K}/K) \supset I_{\mathcal{K}/K} \supset I_{\mathcal{K}/K}^{0} \supset \cdots \supset I_{\mathcal{K}/K}^{463/5} \supset \cdots.$$  

This filtration has the property that $\text{Gal}(\mathcal{K}/K)/I_{\mathcal{K}/K} = \hatsym{Z}$ canonically, $I_{\mathcal{K}/K}/I_{\mathcal{K}/K}^{0} \cong \prod_{l \neq p \text{ prime}} \mathbb{Z}_l$ 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 $W_K^{ab} \cong K^\times$ corresponds to the filtration by $1 + m_K^j \subset \mathcal{O}_K$. 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 $\text{Gal}(\overline{K}/K)$ and (2) why $p = 2$ is special in the local Langlands correspondence.

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

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

$$St_4 = \begin{pmatrix} | \cdot |^3 & 0 & 0 & 0 \\ 0 & | \cdot |^2 & 0 & 0 \\ 0 & 0 & | \cdot | & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad N = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

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 $\rho \otimes \chi : \text{Gal}(\overline{K}/K) \to GL(V)$.

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 inertia 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 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 $\text{Gal}(\overline{K}/K)$ 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 $\Gamma$. Then any irreducible $G$-module is either irreducible over $\Gamma$ 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 $\rho : \text{Gal} (\overline{\mathbb{K}}/K) \to GL_2(\mathbb{C})$. By the no small subgroups lemma, the image of $\rho$ must lie in a finite subgroup of $GL_2(\mathbb{C})$, so in the composition of $\rho$ 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 $\text{Gal}(\overline{\mathbb{K}}/K)$ whose image lies in any of the final three finite subgroups? Since $\text{Gal}(\overline{\mathbb{K}}/K)$ 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:

\[
\begin{align*}
\{ & \text{F-semisimple} \\
& \text{n-dimensional} \\
& \text{Weil-Deligne reps} \} / \sim & \leftrightarrow & \{ & \text{irred smooth} \\
& \text{admissible} \\
& \text{reps of } GL_n(K) \} / \sim
\end{align*}
\]

On the left hand side of this bijection, we can consider a special class of \textbf{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 \textbf{spherical representations} of $GL_n(K)$:

\[
\begin{align*}
\{ & \text{Weil-Deligne reps} \\
& \text{s.t. } N = 0 \text{ and } \rho \\
& \text{factors through } \mathbb{Z}: \\
& W_K \twoheadrightarrow \mathbb{Z} \hookrightarrow GL_n(\mathbb{C}) \} / \sim & \leftrightarrow & \{ & \text{reps of } GL_n(K) \\
& \text{admitting a} \\
& \text{GL}_n(\mathcal{O}_K)-\text{fixed vector} \} / \sim
\end{align*}
\]

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 $GL_n(\mathcal{O}_K)$-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

\[
\{ \text{semisimple elements} \} / \text{conj} \leftrightarrow \{ \text{irreducible reps of} \\
\mathcal{H}_{sph} := \mathcal{H}(GL_n(\mathcal{O}_K),GL_n(K)) \} / \sim
\]

This is the \textbf{Satake isomorphism}! We will spend the rest of the lecture explaining this bijection (particularly the right hand side) in more detail.

\textbf{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.

\textbf{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 check that $\text{End}(\text{Ind}^G_N \mathbb{C}) \simeq \mathbb{C}[G/N]$. Hence we have a bijection

\[
\begin{align*}
\{ & \text{irred } G\text{-modules} \\
& \text{with an } N\text{-fixed vector} \} / \sim & \leftrightarrow & \{ \text{irred } G/N\text{-modules} \} / \sim.
\end{align*}
\]
**Case 2:** Consider $H \subset G$ not necessarily normal. Given a $G$-representation $V$, what acts on $V^H$? The Hecke algebra! The operator

$$\pi_H : V \to V^H$$

$$v \mapsto \frac{1}{|H|} \sum_{h \in H} h \cdot v$$

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:

$$
\begin{array}{ccc}
V^H & \xrightarrow{[HgH]} & V^H \\
\downarrow & & \uparrow \pi_H \\
V & \xrightarrow{\cdot g} & V
\end{array}
$$

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

$$\text{End}(\text{Ind}_H^G \mathbb{C}) \cong \mathcal{H}(H, G).$$

Hence

$$\langle \text{Ind}_H^G \mathbb{C} \rangle \cong \mathcal{H}(H, G)\text{-mod}.$$

(Here the angle brackets mean the smallest abelian category generated by kernels, cokernels, extensions, and direct sums.) Deduce that

$$\left\{ \text{irred. } G\text{-modules with } H\text{-fixed vector} \right\} \cong \text{irred } \mathcal{H}(H, G)\text{-modules}.$$
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 $K_0 = GL_n(\mathcal{O}_K)$ the maximal compact subgroup. Then the “big” Hecke algebra of $G$ is

$$H^{\text{big}} = \left\{ \varphi : G \to \mathbb{C} \mid \varphi \text{ locally constant, compact support} \right\}.$$ 

An alternate description is

$$H^{\text{big}} = \bigcup_i \left\{ \varphi : G \to \mathbb{C} \mid \varphi \text{ locally constant on } K_i\text{-double cosets, non-zero on finitely many} \right\}.$$ 

Exercise 9.12. Prove that the two formulations of $H^{\text{big}}$ are equivalent.

The algebra structure on $H^{\text{big}}$ is given by

$$(f * f')(g) = \int_{h \in G} f(h)f'(h^{-1}g)d\mu,$$ 

where $\mu$ is the Haar measure.

Example 9.13. Let $1_{K_i}$ be the indicator function on $K_i$. Then

$$1_{K_i} * 1_{K_i}(g) = \int_{h \in G} 1_{K_i}(h)1_{K_i}(h^{-1}g)d\mu = \begin{cases} 0 & \text{if } g \notin K_i, \\ \int_{K_i} 1_{K_i}d\mu & \text{if } g \in K_i. \end{cases}$$ 

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 $i$, $H^{\text{big}}$ 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

$$H^{\text{sph}} = H(K_0, G) := 1_{K_0}H^{\text{big}}1_{K_0}.$$ 

Exercise 9.15. (Do it!) Prove the Cartan decomposition of $G$:

$$G = \bigcup_{\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n} K_0 \left( \begin{array}{ccc} \pi^{\lambda_1} & & \\ & \pi^{\lambda_2} & \\ & & \ddots \end{array} \right) K_0$$

Hence

$$H^{\text{sph}} = \bigoplus_{\lambda} \mathbb{C}1_{\lambda}.$$
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

$$\mathcal{H}^{sph} \leftrightarrow R(\mathbb{L}GL_n(\mathbb{C})).$$

**Remark 9.17.** The Langlands dual group $\mathbb{L}GL_n(\mathbb{C}) \simeq GL_n(\mathbb{C})$ 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, $R(G)_\mathbb{C} \simeq R(T)_\mathbb{C}^W$, 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:

\[
\begin{align*}
\{\text{"spherical representations;"} & \} \quad \xleftarrow{1:1} \quad \{\text{irreducible modules} \} \\
\text{i.e. smooth admissible} & \quad \{\chi : \mathcal{H}^{sph} \to \mathbb{C} \} \\
\text{irred reps of $G$ with a $K_0$-fixed vector} & \quad \{\theta : R(\mathbb{L}GL_n(\mathbb{C})) \to \mathbb{C} \} \\
& \quad \{\text{conjugacy classes} \} \\
& \quad \{\text{of semisimple elts in $\mathbb{L}GL_n(\mathbb{C})$} \}
\end{align*}
\]

9.6 Solutions to exercises

**Exercise 9.3.** Show that the set $\mu_{p-1}$ 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 $\overline{a} = x_0 \in \mathbb{F}_p$. 

79
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 \( f(a_i) = a_i^{p-1} - 1 = 0 \). 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
\[
\text{End}(\text{Ind}_H^G \mathbb{C}) \simeq \mathcal{H}(H, G).
\]

Hence
\[
\langle \text{Ind}_H^G \mathbb{C} \rangle \sim \mathcal{H}(H, G)\text{-mod}.
\]

(Here the angle brackets mean the smallest abelian category generated by kernels, cokernels, extensions, and direct sums.) Deduce that
\[
\left\{ \text{irred. } G\text{-modules with } H\text{-fixed vector} \right\} \overset{1:1}{\leftrightarrow} \left\{ \text{irred } \mathcal{H}(H, G)\text{-modules} \right\}
\]

**Solution:** By Frobenius reciprocity,
\[
\text{Hom}_G(\text{Ind}_H^G \mathbb{C}, \text{Ind}_H^G \mathbb{C}) \simeq \text{Hom}_H(\mathbb{C}, \text{Res}_H^G \text{Ind}_H^G \mathbb{C}).
\]

As a vector space, \( \text{Res}_H^G \text{Ind}_H^G \mathbb{C} \simeq \mathbb{C}[G/H] \) with \( H \)-action given by \( h \cdot f(gH) = f(h^{-1}gH) \) for \( h \in H, g \in G \). An \( H \)-module homomorphism
\[
\varphi: \mathbb{C} \rightarrow \mathbb{C}[G/H]
\]
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 \( \varphi(1) \in \mathbb{C}[H\setminus G/H] \). Thus,
\[
\text{End}(\text{Ind}_H^G \mathbb{C}) \simeq \mathcal{H}(H, G).
\]

**Exercise 9.11.** Prove that the two formulations of \( \mathcal{H}^{\text{big}} \) are equivalent.

**Exercise 9.14.** (Do it!) Prove the Cartan decomposition of \( G \):
\[
G = \bigsqcup_{\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n} K_0 \begin{pmatrix}
\pi^{\lambda_1} \\
\pi^{\lambda_2} \\
\pi^{\lambda_3} \\
\vdots \\
\pi^{\lambda_n}
\end{pmatrix} K_0
\]

Hence
\[
\mathcal{H}^{\text{sph}} = \bigoplus_{\lambda} \mathbb{C} 1_{\lambda}.
\]

80
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:

<table>
<thead>
<tr>
<th>( p )</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
</tr>
</thead>
<tbody>
<tr>
<td># sols mod ( p )</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( p ) mod 4</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

Then we studied this via representation theory. The Galois group \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) acts on the roots \( \{\sigma_1, \ldots, \sigma_n\} \subset \overline{\mathbb{Q}} \) of \( f(x) \), so we have a permutation representation

\[
\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL(H),
\]

where \( H := \bigoplus_{i=1}^{n} \mathbb{C}\sigma_i \). Then for unramified primes,

\[
\text{# solutions of } f(x) \text{ mod } p = \text{Tr}(\text{Frob}_p, H).
\]

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”

\[
\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to GL(H_{\mathbb{Q}_p}),
\]

where \( H_{\mathbb{Q}_p} = \bigoplus \mathbb{C}\sigma'_i \). This gives us a “categorification” of the table above:

<table>
<thead>
<tr>
<th>( p )</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
</tr>
</thead>
<tbody>
<tr>
<td>( H_{\mathbb{Q}_2} )</td>
<td>( H_{\mathbb{Q}_3} )</td>
<td>( H_{\mathbb{Q}_5} )</td>
<td>( H_{\mathbb{Q}_7} )</td>
<td>( H_{\mathbb{Q}_{11}} )</td>
<td>( H_{\mathbb{Q}_{13}} )</td>
<td>( H_{\mathbb{Q}_{17}} )</td>
<td>( H_{\mathbb{Q}_{19}} )</td>
<td>( H_{\mathbb{Q}_{23}} )</td>
<td></td>
</tr>
</tbody>
</table>

If \( p \) is unramified, then the inertia subgroup \( I \subset \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \) 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

\[
\text{# solutions of } f(x) \text{ mod } p = \text{Tr}([x]).
\]

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 $\geq 1$

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 $\Lambda$:

![Diagram of elliptic curve](image)

The Galois group Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) does not act in any meaningful way on $E(\mathbb{C})$. It does act on $E(\mathbb{Q})$, but this is an enormously complicated set, a little too complicated for us! However, for any prime $\ell$, we can consider the “$\ell^m$-torsion points”:

$$E[\ell^m] := \{x \in E(\mathbb{Q}) \mid \ell^m \cdot x = 0\} \simeq (\mathbb{Z}/\ell^m\mathbb{Z})^2;$$

e.g., for $\ell = 3, m = 1$:

![Diagram of $E[\ell^m]$](image)

There is a natural action of 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 Gal($\overline{\mathbb{Q}}/\mathbb{Q}$). Moreover, if $E_{\mathbb{F}_p}$ is smooth, then

$$\#E(\mathbb{F}_p) = 1 + p - \text{Tr}(\text{Frob}_p, T_\ell(E)).$$

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 $\ell$. This is an embarrassment of riches!

The Tate module $T_\ell(E)$ is an example of "\(\ell\)-adic cohomology:"

$$T_\ell(E) = H^1_\text{ét}(E, \mathbb{Z}_\ell)^\ast.$$ 

In general, given a variety $X$ over a field $k$ and a prime $\ell$ such that multiplication by $\ell$ is non-zero in $k$, there is a continuous action of $\text{Gal}(\overline{k}/k)$ on the $\ell$-adic cohomology groups $H^*_\text{ét}(X_{\overline{k}}, \mathbb{Q}_\ell)$. Again, it is useful to study these representations via their restriction to local Galois groups $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. We can always calculate these after base change to $\text{Spec} \mathbb{Q}_p$ and at primes of good reduction after base change to $\text{Spec} \mathbb{F}_p$. (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**: $H^i_{\text{cris}}(X_{\mathbb{F}_p}/\mathbb{Z}_p)$ (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 $\text{Spec} \mathbb{Z} \times \text{Spec} \mathbb{Z}$.

**Scholze’s ICM picture**: 

83
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 $G_{Q_p} = \text{Gal}(Q_p/Q_p)$, how can we compare $ho : G_{Q_p} \to GL_n(Q_\ell)$ and $\rho' : G_{Q_p} \to GL_n(Q_{\ell'})$?

The problem is the topology. The solution is given by Weil–Deligne representations.

A topological group $\Gamma$ is pro-$p$ if it is profinite and for all open normal subgroups $N \subset \Gamma$, $\Gamma/N$ is a $p$-group.

**Example 10.1.** Two examples of pro-$p$-groups are:

1. wild inertia $\subset G_{Q_p}$, and
2. $1 + p \text{Mat}_n Z_p = K_1 \subset GL_n(Q_p)$.

**Lemma 10.2.** Any continuous group homomorphism

$$\rho : \Gamma \to G$$

from a pro-$p$ group $\Gamma$ to a pro-$\ell$ group $G$ is trivial.
**Corollary 10.3.** For a pro-$p$ group $\Gamma$, any continuous group homomorphism

$$\rho : \Gamma \to GL_n(Q_p)$$

has finite image.

We have seen (via the ramification filtration) the $G_{Q_p}$ has the following structure:

\[
\begin{array}{c}
\text{WILD} \quad \text{pro-}p \\
\text{TAME} \quad \prod_{p \neq \ell} \mathbb{Z}_{\ell} = \mathbb{Z}_p \times \prod_{p \neq \ell} \mathbb{Z}_{\ell'} \\
\text{UNRAMIFIED} \quad \hat{\mathbb{Z}}
\end{array}
\]

Grothendieck showed us that the pro-$\ell'$ group $\prod_{p \neq \ell} \mathbb{Z}_{\ell'} \subset I$ must have finite image. Moreover, $\rho(1_{\ell}) \in GL_n(Q_{\ell})$ 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 $\overline{Q}_{\ell}$ with $\mathbb{C}$, one has a canonical injection

\[
\left\{ \text{cts. reps.} \quad \rho : G_{Q_p} \to GL_n(Q_{\ell}) \right\} \hookrightarrow \left\{ \text{Weil–Deligne reps of } G_{Q_p} \text{ over } \mathbb{C} \right\}.
\]

Notice that the set on the right is independent of $\ell$!

**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 $\hat{G}$ its dual group, determined by the opposite root datum $(X_* \supset R^\vee, X^* \supset R)$. Fix a local field $K$ and set $q = |O_K/m_K|$.

A **Weil–Deligne representation** in $\hat{G}$ is a pair $(\rho, e)$, where

- $\rho : W_K \to \hat{G}(\mathbb{C})$ is a continuous group homomorphism, and
- $e \in \text{Lie } \hat{G}(\mathbb{C})$ 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 $\hat{G}$ is $F$-**semisimple** if $\rho$ 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 $(\rho, e)$, consider $Z_{\hat{G}}(\rho, e) = \{ g \in \hat{G} \mid g \cdot (\rho, e) = (\rho, e) \}$.

Theorem 10.7. (Local Langlands correspondence) There is a canonical correspondence

\[
\begin{array}{ccc}
\{ \text{F-semisimple WD reps in } \hat{G} \} & \xrightarrow{1:\text{finite}} & \{ \text{irred smooth admissible reps of } G(K) \} \\
\text{/} G\text{-conj} & & \text{/} \simeq \\
\end{array}
\]

Fibres of this map should be indexed by irreducible representations of $Z_{\hat{G}}(\rho, e)/Z_{\hat{G}}(\rho, e)^{\circ}$ 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:

\[
\begin{array}{ccc}
\{ \text{TRUM; i.e. } (\rho, e) \text{ s.t. } \rho \text{ factors through } W_K \twoheadrightarrow \mathbb{Z}, \text{ e arbitrary} \} & \xrightarrow{1:\text{finite}} & \{ \text{reps with an Iwahori fixed vector} \} \\
\text{/} \hat{G}\text{-conj} & & \\
\end{array}
\]

By analogous arguments to the ones we made last week for $GL_n$, the set of $\rho$ which factor through $W_K \twoheadrightarrow \mathbb{Z}$ is in bijection with the set of conjugacy classes of semisimple elements in $\hat{G}$. Hence the left hand side of the correspondence above is in bijection with the set

\[
\{(s, e) \mid s \in \hat{G} \text{ semisimple, } e \in \text{Lie } \hat{G} \text{ nilpotent s.t. } ses^{-1} = qe \}/\hat{G}\text{-conj}. 
\]

The right hand side of the correspondence above is in bijection with the set

\[
\{ \text{irred reps of the “Iwahori-Hecke algebra” } H_{\text{aff}} := H(I, G(K)) \}. 
\]

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:

\[
\begin{array}{ccc}
\{ (s, e, \chi) \mid s \in \hat{G}(\mathbb{C}) \text{ semisimple, } e \in \text{Lie } \hat{G} \text{ nilpotent, and } \chi \text{ irred rep of } \pi_0(Z_{\hat{G}}(\rho, e)) \text{ such that } ses^{-1} = qe \} & \xrightarrow{\sim} & \{ \text{irred } H_{\text{aff}}\text{-modules} \}/\simeq \\
\text{/}\hat{G}\text{-conj} & & \\
\end{array}
\]
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 \( q = \#|\mathcal{O}_K/\mathfrak{m}_K| \) 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:

\[
\mathcal{H}_\text{sph} = \mathcal{H}(G(\mathcal{O}_K), G(K)) \xrightarrow{\sim} R(\hat{G}) = \mathcal{O}\left(\text{semisimple conj. classes in } \hat{G}\right) \xrightarrow{\sim} K^0(\text{pt}/\hat{G}) = K^{\hat{G}}(\text{pt})
\]

“constructible”

Similarly, the TRUM case of the LLC (which reduces to the Deligne–Langlands conjecture) follows from the Kazhdan–Lusztig isomorphism:

\[
\mathcal{H}_\text{aff} \xrightarrow{\sim} K^{\hat{G} \times \mathbb{C}^\times} (\text{St})
\]

“constructible”

Indeed, if \( \pi : \tilde{N} = T^* \mathcal{B} \to \mathcal{N} \) is the Springer resolution, \( \mathcal{B}_e = \pi^{-1}(e) \) is the Springer fibre of a nilpotent element \( e \in \mathcal{N} \), and \( \text{St} \) 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 \( K^{Z_{\hat{G} \times \mathbb{C}^\times}(e)}(\mathcal{B}_e) \). Here we can see that

\[
Z_{\hat{G} \times \mathbb{C}^\times}(e) = \{(g,c) \mid c \cdot geg^{-1} = e\} = \{(g,c) \mid geg^{-1} = e^{-1} \cdot e\}
\]

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 \( \mathcal{O}_K = k[[t]] \), where \( k = \mathbb{C} \) or \( \mathbb{F}_q \). Then

\[
\mathcal{H}(G(\mathcal{O}_K), G(K)) = \text{G}(\mathcal{O}_K)-\text{invariant functions on the } \text{affine Grassmanian } G_{\mathcal{R}_G} := G(K)/G(\mathcal{O}_K).
\]

The geometric Satake equivalence is the equivalence of categories:

\[
(\text{Perv}_{G(\mathcal{O}_K)}(G_{\mathcal{R}}, \mathbb{C}), *) \xrightarrow{\sim} (\text{Rep} \hat{G}_\mathbb{C}, \otimes)
\]

“constructible”

“coherent”

This equivalence was key in recent work by V. Lafforgue 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

$$(D^b_{I \times I}(\mathcal{F}l_G), \ast) \xrightarrow{\sim} (D^b_{\text{Coh} \times \mathbb{C}^\times}(\text{St}), \ast)$$

“constructible”  “coherent”

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!
11 Lecture 11 (August 30, 2019): First lecture of the second semester

Recall our setup from last semester. Let $K$ be a local field (i.e. $K$ is a finite extension of $\mathbb{Q}_p$ or $K = \mathbb{F}_q((t))$) with ring of integers $\mathcal{O}$ and residue field $k$:

$$K \supset \mathcal{O} \twoheadrightarrow k$$

Nothing is lost by just thinking in terms of the example

$$\mathbb{Q}_p \supset \mathbb{Z}_p \twoheadrightarrow \mathbb{F}_p.$$ 

Last semester, we worked up to stating the local Langlands correspondence.

Local Langlands correspondence for $GL_n$: There exists a canonical bijection

$$
\begin{align*}
\left\{ \text{irred. smooth admiss. reps of } GL_n(K) \text{ on } \mathbb{C}\text{-vector spaces} \right\} & \overset{1:1}{\longleftrightarrow} \\
\left\{ \text{F-semisimple } n\text{-dimensional Weil-Deligne reps} \right\}
\end{align*}
$$

It’s been a while, so let’s remind ourselves what all of these words mean. The representations on the left hand side of this correspondence are *irreducible* representations which are usually infinite-dimensional. The adjective *smooth* means that every vector has an open stabilizer, and the adjective *admissible* means that for any open subgroup $U \subset GL_n(K)$, $V^U$ is finite-dimensional. We consider the set of such representations up to equivalence.

The objects on the right hand side are $n$-dimensional representations (where $n$ is the same $n$ appearing in $GL_n$ on the left) of the Weil group attached to the field $K$, along with some extra data. Recall that the **Weil group** is a subgroup of the absolute Galois group $\text{Gal}(\overline{K}/K)$ defined by the fact that it fits into the following diagram.

$$
\begin{array}{cccc}
I_{\overline{K}/K} & \longrightarrow & W_K := \varphi^{-1}(\mathbb{Z}) & \longrightarrow & \mathbb{Z} = \langle \text{Frob} \rangle \\
\downarrow & & \downarrow & & . \\
I_{\overline{K}/K} & \longrightarrow & \text{Gal}(\overline{K}/K) & \xrightarrow{\varphi} & \text{Gal}(\overline{k}/k) = \widehat{\mathbb{Z}}
\end{array}
$$

Here $I_{\overline{K}/K}$ is the **inertia subgroup**. A **Weil-Deligne representation** is a triple $(V, \rho, N)$, where

1. $V$ is an $n$-dimensional $\mathbb{C}$-vector space,
2. $\rho : W_K \rightarrow GL(V)$ is a continuous representation, and
3. $N$ is a nilpotent endomorphism of $V$ such that

$$\rho(x)N\rho(x)^{-1} = |x|N$$

for all $x \in W_K$. 

89
Here $| \cdot |$ is the canonical norm on $W_k$, which is uniquely determined by the property that $| \text{Frob}| = |k|$. (See Section 8.1 for a refresher on why this exists.) A Weil-Deligne representation is $F$-semisimple if any lift of Frob acts semisimply.

**Remark 11.1.** For the experts: Weil-Deligne representations are distilled out of continuous representations $W_K \rightarrow GL_n(\mathbb{Q}_\ell)$ via “log of monodromy.” Thus one can think of the right hand side as secretly being genuine representations of a group. It is phrased in this way to get remove the auxiliary choice of a prime number $\ell$.

In general, if we replace $GL_n(K)$ with any split reductive group $G(K)$ (e.g. $SL_n$, $Sp_{2n}$, etc.), then the LLC changes as follows.

**Local Langlands correspondence for split reductive groups:** There exists a canonical finite-to-one map

\[
\begin{align*}
\text{irred. smooth admiss. reps of } G(K) \text{ on } \mathbb{C}\text{-vector spaces} & \rightarrow_{1:1} \text{F-semisimple Weil-Deligne reps of } W_K \text{ in } G^\vee(\mathbb{C})
\end{align*}
\]

In this setting, a **Weil-Deligne representation of $W_K$ in $G^\vee(\mathbb{C})$** is a pair $(\rho, N)$, where

1. $\rho : W_K \rightarrow G^\vee(\mathbb{C})$ is a continuous group homomorphism of the Weil group into the complex Langlands dual group of $G$, and
2. $N \in G^\vee(\mathbb{C})$ such that
\[
\rho(x) N \rho(x)^{-1} = |x| N
\]

for all $x \in W_K$.

Note that condition 2 forces $N \in G^\vee(\mathbb{C})$ to be a nilpotent element.

### 11.1 The unramified story

Last semester we ended the course by unpacking the simplest piece of the LLC, the case of **unramified representations**. Let’s remind ourselves how this story went. By restricting each side of the correspondence above, we obtain a bijection

\[
\begin{align*}
\text{irred smooth admissible } \begin{cases} 
\text{unramified reps of } G(K) \\
\text{(i.e. reps of } G(K) \text{ that admit a non-zero } G(\mathcal{O})\text{-fixed vector)}
\end{cases} & \rightarrow_{1:1} \text{unramified } \begin{cases} 
\text{Weil-Deligne reps; } \\
\text{(i.e. reps which factor } W_K \rightarrow \mathbb{Z} \rightarrow G^\vee(\mathbb{C}) \text{ with } N = 0)
\end{cases}
\end{align*}
\]

By Hecke algebra theory, representations of $G(K)$ with a $G(\mathcal{O})$-fixed vector are in bijection with irreducible modules for the spherical Hecke algebra,

\[\mathcal{H}_{\text{sph}} = \mathcal{H}(G(K), G(\mathcal{O})) := (\text{Fun}_{G(\mathcal{O}) \times G(\mathcal{O})}(G(K), \mathbb{C}), \ast).\]

The functions in this definition are continuous with compact support. On the other hand, unramified Weil-Deligne representations are in bijection with the set of conjugacy classes of semisimple elements in $G^\vee(\mathbb{C})$. Recall the Satake isomorphism.
Theorem 11.2. (Satake isomorphism) There exists a canonical isomorphism

\[ \mathcal{H}_{\text{sph}} \sim \rightarrow [\text{Rep} G^\vee] \otimes \mathbb{Z} \mathbb{C}. \]

This theorem will be a big feature of the course this semester. Let \( T^\vee \subset G^\vee \) be a maximal torus, and \( W \) the Weyl group of \( G^\vee \). By highest weight theory we have

\[ [\text{Rep} G^\vee] \xhookrightarrow{\sim} [\text{Rep} T^\vee] = \mathbb{Z} [X^* (T^\vee)] \]

Hence

\[ [\text{Rep} G^\vee] \otimes \mathbb{Z} \mathbb{C} = \mathbb{C} [X^* (T^\vee)]^W = \mathcal{O} (T^\vee / W) = \mathcal{O} (G^\vee_{ss} / \text{conj}). \]

The spherical Hecke algebra is commutative. Therefore,

{irred. \( \mathcal{H}_{\text{sph}} \)-modules} \leftrightarrow \{ \chi : [\text{Rep} G^\vee] \otimes \mathbb{Z} \mathbb{C} \rightarrow \mathbb{C} \} = \{ \text{semisimple conjugacy classes in } G^\vee (\mathbb{C}) \}

The first bijection follows from the Satake isomorphism and the commutativity of \( \mathcal{H}_{\text{sph}} \), and the second equality is the nullstellensatz. So the Satake isomorphism implies unramified LLC!

Remark 11.3. The goal of the next two Informal Friday Seminars (September 6 and 13) will be to explain the geometric Satake equivalence, which is a categorification of Theorem 11.2

\[ (\text{Perv}_{G(\mathbb{O}) \times G(\mathbb{O})} (G(K), \mathbb{C}, *)) \leftrightarrow (\text{Rep} G^\vee_{\mathbb{C}}, \otimes) \]

11.2 The tamely ramified with unipotent monodromy (TRUM) story

This semester we will focus on the next simplest piece of the LLC, the case of tamely ramified representations with unipotent monodromy. In this setting, the LLC gives us a finite-to-one map:

\[
\begin{cases}
\text{TRUM reps of } G(K) \\
(i.e. those which admit a non-zero Iw-fixed vector)
\end{cases}
\xrightarrow{\text{finite:1}}
\begin{cases}
\text{TRUM Weil-Deligne reps} \\
(i.e. reps which factor } W_K \rightarrow \mathbb{Z} \rightarrow G^\vee (\mathbb{C}) \text{ with } N \text{ arbitrary})
\end{cases}
\]

Here \( Iw \subset G(K) \) is the Iwahori subgroup, which sits in the group \( G(K) \) in the following way:

\[
\begin{array}{ccc}
G(\mathbb{O}) & \xhookrightarrow{\sim} & Iw \\
\downarrow & & \downarrow \\
G(k) & \xhookrightarrow{\sim} & B \text{ (Borel)}
\end{array}
\]
By Hecke algebra theory, TRUM representations of $G(K)$ are in bijection with irreducible representations of the Iwahori-Matsumoto Hecke algebra $\mathcal{H}_{\text{aff}} = \mathcal{H}(G(K), I_w)$. On the other hand, TRUM Weil-Deligne representations are parameterized by the set

$$\{(s, N) \in G^\vee(\mathbb{C}) \times N \mid s N s^{-1} = q N\}_{\text{conj}}.$$ 

Here $s \in G^\vee(\mathbb{C})$ is the semisimple image of Frobenius, $N \subset \text{Lie} G^\vee$ is the nilpotent cone, and $q = |k|$. So the LLC predicts a parameterisation of irreducible $\mathcal{H}_{\text{aff}}$-modules. This prediction is the Deligne–Langland conjecture, and it served as an important early test case of the Langland’s philosophy.

**Goals for the next few weeks:**

1. Discuss the Iwahori-Matsumoto Hecke algebra in some detail.
2. Discuss Kazhdan–Lusztig’s realisation of the affine Hecke algebra $H$ via equivariant $K$-theory: 
   $$H \sim K^{G^\vee \times \mathbb{C}^\times} \text{ (Steinberg)}$$
3. Deduce the Deligne–Langlands conjecture.

Then we will pass to categorifications!

### 11.3 Affine Weyl groups and affine Hecke algebras

Let $(X \supset R, X^\vee \supset R^\vee)$ be a root datum.

**Example 11.4.**

1. $SL_2$: $X = \mathbb{Z} \supset R = \{ \pm 2 \}$, $X^\vee = \mathbb{Z} \supset R^\vee = \{ \pm 1 \}$
2. $PGL_2$: $X = \mathbb{Z} \supset R = \{ \pm 1 \}$, $X^\vee = \mathbb{Z} \supset R^\vee = \{ \pm 2 \}$

   We see from this example that $SL_2$ and $PGL_2$ are interchanged by swapping roots and coroots, so they are Langlands dual groups.

   Let $W_f$ be the finite Weyl group associated to this root datum. Then $W_f$ acts on both $X$ and $X^\vee$. Assume that our root datum $(X \supset R, X^\vee \supset R^\vee)$ is *adjoint*; i.e., $X = \mathbb{Z} R$. (This is the “most complicated case.”)

**Definition 11.5.** The extended affine Weyl group is

$$W_{\text{ext}} = \mathbb{Z} X^\vee \rtimes W_f.$$

The group $W_{\text{ext}}$ acts on $X^\vee_\mathbb{R} := X^\vee \otimes_\mathbb{Z} \mathbb{R}$ by “affine transformations;” that is, $w \in W_f$ acts as usual, $w(\lambda) = w(\lambda)$, and for $\gamma \in X^\vee$, $t_\gamma \in \mathbb{Z} X^\vee$ acts by

$$t_\gamma(\lambda) = \lambda + \gamma.$$  

---

6This definition is the definition according to Iwahori-Matsumoto and Bourbaki, but we warn the reader that it is *not* consistent across all sources! For example, this is not the convention employed in Chriss-Ginzburg.
To understand $W_{\text{ext}}$, we first consider the affine Weyl group $W = \mathbb{Z}R^\vee \rtimes W_f \subset W_{\text{ext}}$. For $\alpha \in R$, $m \in \mathbb{Z}$, $\lambda \in X^\vee_\mathbb{R}$, define

$$s_{\alpha,m}(\lambda) := \lambda - \langle \lambda, \alpha \rangle \alpha^\vee + m\alpha^\vee.$$ 

Clearly,

$$s_{\alpha,m} = t_{m\alpha^\vee} \circ s_\alpha,$$

so $s_{\alpha,m} \in W$, and $t_{m\alpha^\vee} \in \langle s_{\alpha,m} \mid \alpha \in R, m \in \mathbb{Z} \rangle$. We conclude that

$$W = \langle s_{\alpha,m} \mid \alpha \in R, m \in \mathbb{Z} \rangle$$

is an affine reflection group generated by reflections $s_{\alpha,m}$ through the hyperplanes

$$H_{\alpha,m} = \{ \lambda \in X^\vee_\mathbb{R} \mid \langle \lambda, \alpha \rangle = m \}.$$ 

We call the set $\{H_{\alpha,m}\}$ the set of reflecting hyperplanes. Denote by $\mathcal{A}$ the corresponding set of alcoves; that is, the closures of connected components of

$$X^\vee_\mathbb{R} \setminus \bigcup_{\alpha \in R, m \in \mathbb{Z}} H_{\alpha,m}.$$ 

Fix a set of positive roots $R_+ \subset R$, and let

$$A_0 = \{ \lambda \in X^\vee_\mathbb{R} \mid 0 \leq \langle \lambda, \alpha \rangle \leq 1 \text{ for all } \alpha \in R_+ \} \subset \mathcal{A}$$

be the fundamental alcove. The general (very beautiful) theory of reflection groups gives:

1. $W$ is a Coxeter group with Coxeter generators $S := \{ \text{reflections in the walls of } A_0 \}$.

2. The length function may be described by

$$\ell(w) = \# \{ \text{reflecting hyperplanes separating } A_0^{\text{int}} \text{ and } wA_0^{\text{int}} \}.$$ 

3. $A_0$ is a fundamental domain for the $W$-action on $X^\vee_\mathbb{R}$.

So we have an identification

$$W \rightarrow \mathcal{A}$$

$w \mapsto wA_0$

**Example 11.6.** $C_2 = B_2$
Now we move on to $W_{\text{ext}}$. There is an action of $W_{\text{ext}}$ on $\mathcal{A}$ because
\[ t_\gamma \cdot H_{\alpha,m} = H_{\alpha,m + \langle \gamma, \alpha \rangle}. \]

Define
\[ \ell : W_{\text{ext}} \to \mathbb{Z}_{\geq 0} \]
\[ w \mapsto \ell(w) : = \# \{ \text{hyperplanes separating } A_0^{\text{int}} \text{ and } wA_0^{\text{int}} \} \]

Define the length zero elements of $W_{\text{ext}}$ to be
\[ \Omega := \ell^{-1}(0). \]

**Lemma 11.7.** $W_{\text{ext}} = \Omega \ltimes W$.

**Proof.** **Step 1:** $W \subset W_{\text{ext}}$ is normal.

Let $\gamma \in X^\vee$, $\lambda \in X_R^\vee$. Then
\[ t_\gamma s_{\alpha,m} t_\gamma^{-1}(\lambda) = t_\gamma(s_{\alpha,m}(\lambda - \gamma)) \]
\[ = \lambda - \gamma - \langle \lambda - \gamma, \alpha \rangle \alpha^\vee + ma^\vee + \gamma \]
\[ = \lambda - \langle \lambda, \alpha \rangle \alpha^\vee + (\langle \gamma, \alpha \rangle + m) \alpha^\vee \]
\[ = s_{\alpha,(\gamma, \alpha) + m}(\lambda). \]

**Step 2:** $W_{\text{ext}} = W \cdot \Omega$.

Let $w \in W_{\text{ext}}$. Then $wA_0 \in \mathcal{A}$, so by 3. above, there exists $y \in W$ such that $ywA_0 = A_0$. Hence $yw = \omega$ for $\omega \in \Omega$, and $w = y^{-1}\omega$.

**Step 3:** $W \cap \Omega = \{ id \}$.

Any $w \in W \cap \Omega$ is length zero, so $w = id$ by 2. above and the fact that $W$ is a Coxeter group. □

**Lemma 11.8.** (Iwahori-Matsumoto) $w \in W_f$, $\lambda \in X^\vee$,
\[ \ell(t_\lambda w) = \sum_{\substack{\alpha \in R^+ \\cap w^{-1}(\alpha) > 0 \\cap \alpha \in R^+ \\cap w^{-1}(\alpha) < 0}} |\langle \alpha, \lambda \rangle| + \sum_{\substack{\alpha \in R^+ \\cap w^{-1}(\alpha) > 0 \\cap \alpha \in R^+ \\cap w^{-1}(\alpha) < 0}} |\langle \alpha, \lambda \rangle|. \]

**Proof.** Let $x = t_\lambda w$. Then
\[ \ell(x) = \# \{ \text{hyperplanes separating } A_0^{\text{int}} \text{ and } xA_0^{\text{int}} \} \]
\[ = \sum_{\alpha \in R^+} \# \{ m \mid H_{\alpha,m} \text{ separates } A_0^{\text{int}} \text{ and } xA_0^{\text{int}} \}. \]
Now chose a point $p \in A_0$, very close to zero. Then $\langle p, \alpha \rangle$ is small and positive, and

$$
\ell(x) = \sum_{\alpha \in R_+} \# \{ \text{integers between } \langle p, \alpha \rangle \text{ and } \langle xp = \lambda + wp, \alpha \rangle \}
$$

$$
= \sum_{\alpha \in R_+} \begin{cases} 
|\langle \lambda, \alpha \rangle| & \text{if } \langle wp, \alpha \rangle > 0 \\
|\langle \lambda, \alpha \rangle - 1| & \text{if } \langle wp, \alpha \rangle < 0
\end{cases}
$$

$$
= \sum_{\alpha \in R_+ \atop w^{-1} \alpha > 0} |\langle \lambda, \alpha \rangle| + \sum_{\alpha \in R_+ \atop w^{-1} \alpha < 0} |\langle \lambda, \alpha \rangle - 1|.
$$

\[\square\]

**Example 11.9.** For $PGL_2$, $X^\vee = \mathbb{Z}_{\varpi_1}$. Then

$$
\ell(m_{\varpi_1}) = |m|, \text{ and } \ell(m_{\varpi_1}s) = |m - 1|.
$$

Hence $\varpi_1s$ is length zero, and $\Omega = \{id, t_{\varpi_1}s\}$. 

12 Lecture 12 (September 6, 2019): Iwahori–Matsumoto Hecke algebra and Deligne-Langlands conjecture

12.1 The Iwahori–Matsumoto Hecke algebra

Recall our setup from last week. From an adjoint root datum \((X \supset R, X^\vee \supset R^\vee)\), (i.e.; meaning \(X = \mathbb{Z}R\)) we construct

- the finite Weyl group \(W_f\),
- the affine Weyl group \(W = \mathbb{Z}R^\vee \rtimes W_f\), and
- the extended affine Weyl group \(W_{ext} = \mathbb{Z}X^\vee \rtimes W_f\).

We fix a set of positive roots \(R^\vee_+ \subset R^\vee\), then obtain the fundamental alcove \(A_0\), and the corresponding set \(S \subset W\) of Coxeter generators. We define a length function \(\ell\) by

\[
\ell : W_{ext} \to \mathbb{Z}
\]

\[
x \mapsto \#\left\{ \text{reflecting hyperplanes between } A_0^{int} \text{ and } xA_0^{int} \right\}.
\]

We denoted the length zero elements by \(\Omega = \ell^{-1}(0)\), and showed that \(W_{ext}\) is a “quasi Coxeter group,” meaning that

\[W_{ext} = \Omega \rtimes W,\]

\(W\) is a Coxeter group, and \(\Omega\) acts on \(W\) via automorphisms of the Coxeter system.

Example 12.1. For \(PGL_2\),

The affine Weyl group and extended affine Weyl group are

\[W = \langle s, t \mid s^2 = t^2 = id \rangle \subset W_{ext} = \langle s, t, \tau = \omega s \mid s^2 = t^2 = \tau^2 = id, \tau s = t\tau \rangle.\]

We can use the extended affine Weyl group to define a Hecke algebra.

Definition 12.2. The Iwahori–Matsumoto Hecke algebra \(H_{ext}\) is the \(\mathbb{Z}[v^\pm]\)-algebra with basis \(\{H_x \mid x \in W_{ext}\}\) and multiplication

\[H_x H_y = H_{xy} \text{ if } \ell(xy) = \ell(x) + \ell(y)\]

\[H_s^2 = H_{id} + (v^{-1} - v)H_s \text{ if } s \in S.\]

Define \(\mathcal{H} = \langle H_x \mid x \in W \rangle \subset H_{ext}\).
Remark 12.3. 1. \( \mathcal{H} \subset \mathcal{H}_{\text{ext}} \) is a subalgebra.

2. For all \( x \in W_{\text{ext}} \), \( H_x \) is invertible.

3. If \( \tau \in \Omega \), then \( \ell(x\tau) = \ell(x) = \ell(\tau x) \). Hence
\[
\mathcal{H}_{\text{ext}} = \Omega \ltimes \mathcal{H}.
\]

**Question:** Where did the loop presentation \( W_{\text{ext}} = \mathbb{Z}X^\vee \rtimes W_f \) go?

For \( \lambda \in X^\vee \), write \( \lambda = \gamma - \gamma' \) with \( \gamma, \gamma' \in X^\vee_+ \). Define
\[
H_\lambda := H_{t_\gamma} H_{t_{\gamma'}}^{-1}.
\]

Note that \( H_{t_\gamma} \neq H_\lambda \) in general! For example, if \( \lambda \in X^\vee_+ \), then \( H_\lambda = H_{t_\lambda} \), but if \( \lambda \in -X^\vee_+ \), then \( H_\lambda = H_{t_{-\lambda}}^{-1} \).

**Why is this well-defined?** Assume that \( \lambda = \gamma - \gamma' = \mu - \mu' \) for \( \gamma, \gamma', \mu, \mu' \in X^\vee_+ \). To show that \( H_\lambda \) is well-defined, we need to show that
\[
H_{t_\gamma} H_{t_{\gamma'}}^{-1} H_{t_\zeta} = H_{t_\mu} H_{t_{\mu'}}^{-1} H_{t_\zeta}.
\]

If we choose \( \zeta \in X^\vee_+ \) very dominant, then \( \zeta - \mu' \) is dominant and
\[
H_{t_{\zeta-\mu}} H_{t_{\mu'}} = H_{t_{\gamma}} H_{t_{t_{\gamma'-\mu}}} = H_{t_{\gamma}} H_{t_{t_{\gamma'-\mu}}} = H_{t_{\mu}} H_{t_{\zeta-\mu}}.
\]

This is equivalent to showing that for \( \zeta \in X^\vee \),
\[
H_{t_\gamma} H_{t_{\gamma'}}^{-1} H_{t_\zeta} = H_{t_\mu} H_{t_{\mu'}}^{-1} H_{t_\zeta}.
\]

The first and fourth equalities follow from the fact that the lengths of \( t_{\zeta-\mu} \) and \( t_{\mu'} \) add by the Iwahori–Matsumoto lemma (Lemma 11.8). Hence,
\[
H_{t_\gamma} H_{t_{\gamma'}}^{-1} H_{t_\zeta} = H_{t_\gamma} H_{t_{\gamma'-\mu}} = H_{t_{\gamma + \zeta - \mu}} = H_{t_{\mu}} H_{t_{\gamma'-\mu}} = H_{t_{\mu}} H_{t_{\zeta-\mu}} = H_{t_{\mu}} H_{t_{\mu'}^{-1}} H_{t_\zeta},
\]

so \( H_\lambda \) is well-defined.

**The upshot:** When studying representations of an algebra, it is useful to have a large commutative subalgebra. This is what we have just accomplished for the Iwahori–Matsumoto Hecke algebra: the map \( \lambda \mapsto H_\lambda \) determines an embedding
\[
\mathbb{Z}[v^{\pm 1}][X^\vee] \hookrightarrow \mathcal{H}_{\text{ext}}.
\]

We can use this commutative subalgebra to describe the center of \( \mathcal{H}_{\text{ext}} \).

**Theorem 12.4.** (Bernstein) For any \( \lambda \in X^\vee_+ \), define
\[
z_\lambda := \sum_{\mu \in W_f \lambda} H_\mu.
\]

Then the center \( Z(\mathcal{H}_{\text{ext}}) \) of \( \mathcal{H}_{\text{ext}} \) is a free \( \mathbb{Z}[v^{\pm 1}] \)-module with basis \( \{ z_\lambda \mid \lambda \in X^\vee_+ \} \), and
\[
Z(\mathcal{H}_{\text{ext}}) = (\mathbb{Z}[v^{\pm 1}][X^\vee])^{W_f}.
\]

97
Now we can state the Bernstein presentation of $\mathcal{H}_{\text{ext}}$.

**Theorem 12.5.** (Bernstein presentation) The Iwahori–Matsumoto Hecke algebra admits the following presentation.

1. $\langle H_s \mid s \in S_f \rangle$ generate a finite Hecke algebra (“finite part”).
2. $H_\lambda H_\gamma = H_{\lambda + \gamma}$ for all $\lambda, \gamma \in X^\vee$ (“lattice part”).
3. For $\lambda \in X^\vee, s_\alpha \in S_f$,
   \[
   H_{s_\alpha} H_{s_\alpha(\lambda)} - H_\lambda H_{s_\alpha} = (v - v^{-1}) \left( \frac{H_\lambda - H_{s_\alpha(\lambda)}}{1 - H_{-\alpha}} \right) \\
   = (v - v^{-1})(H_\lambda + H_{\lambda - \alpha} + \cdots + H_{s_\alpha(\lambda) + \alpha}).
   \]

In other words, we have
\[
\mathcal{H}_{\text{ext}} \simeq \mathbb{Z}[v^{\pm 1}][X^\vee] \otimes \mathcal{H}_f.
\]

We will check the relations for $\text{PGL}_2$. First note that if 3. holds for $\lambda$ and $\gamma$, then it holds for $\lambda + \gamma$:
\[
H_{s_\alpha} H_{s_\alpha(\lambda) + s_\alpha(\gamma)} = (v - v^{-1}) \left( \frac{H_\lambda - H_{s_\alpha(\lambda)}}{1 - H_{-\alpha}} \right) H_{s_\alpha(\gamma)} + H_\lambda H_{s_\alpha} H_{s_\alpha(\gamma)} \\
= (v - v^{-1}) \left( \frac{H_{\lambda + s_\alpha(\gamma)} - H_{s_\alpha(\lambda) + s_\alpha(\gamma)} + H_{\lambda + \gamma} - H_{\lambda - s_\alpha(\gamma)}}{1 - H_{-\alpha}} \right) + H_{\lambda + \gamma} H_{s_\alpha} \\
= (v - v^{-1}) \left( \frac{H_{\lambda + \gamma} - H_{s_\alpha(\lambda + \gamma)}}{1 - H_{-\alpha}} \right) + H_{\lambda + \gamma} H_{s_\alpha}.
\]

In particular, if 3. is true for $\lambda$, then it is true for $-\lambda$.

**For $\text{PGL}_2$:** We will check 3. for $\lambda = \varpi$. We have that $\langle \varpi, \alpha \rangle = 1$, $\tau = t_\varpi s_\alpha$, so $t_\varpi = \tau s_\alpha$, and $H_{\varpi} = H_\tau H_{s_\alpha}$. We compute
\[
H_{s_\alpha} H_{-\varpi} - H_{\varpi} H_{s_\alpha}^{-1} = H_{s_\alpha} H_{s_\alpha}^{-1} H_\tau - H_\tau H_{s_\alpha} H_{s_\alpha} \\
= H_\tau - H_\tau (1 + (v^{-1} - v) H_{s_\alpha}) \\
= (v - v^{-1}) H_\tau H_{s_\alpha} \\
= (v - v^{-1}) H_{\varpi}.
\]

### 12.2 The Deligne–Langlands conjecture

Now we return to the LLC. Let $K$ be a local field with ring of integers $\mathcal{O}$ and residue field $k$. Define $q := |k|$. Let $G/K$ be a split reductive group, and $(X \supset R, X^\vee \supset R^\vee)$ the corresponding root datum.
Recall that the Deligne–Langlands conjecture tells us that we should expect the following relationships:

\[
\begin{aligned}
\{ \text{TRUM reps of } G(K) \} & \xrightarrow{\text{finite}:1} \{ \text{TRUM Weil-Deligne reps} \} \\
\{ \text{irred } \mathcal{H}(G(K), Iw)\text{-modules} \} & \xrightarrow{\sim} \{ (s, x) \in G_C^\vee \times g_C^\vee \text{ s.t. } s \text{ is ss, } x \text{ nilp and } sxs^{-1} = qx \} /_{\text{conj}}
\end{aligned}
\]

The following theorem relates the extended affine Hecke algebra of Iwahori–Matsumoto to this story.

**Theorem 12.6.** (Iwahori–Matsumoto)

1. \(G(K) = \bigsqcup_{w \in W_{ext}} Iw \cdot w \cdot Iw\) (‘Bruhat decomposition’)

2. There is an isomorphism of algebras

\[\mathcal{H}_{ext} \otimes_{\mathbb{Z}[v^{\pm 1}]} \mathbb{C} \xrightarrow{\sim} \mathcal{H}(G(K), Iw)\]

where \(\mathbb{C}\) is a \(\mathbb{Z}[v^{\pm 1}]\)-algebra via \(v \mapsto (\sqrt{q})^{-1} \in \mathbb{R}_+ \subset \mathbb{C}\).

Moreover, under 2., \(H_x\) is mapped to the indicator function on \(Iw \cdot x \cdot Iw\), up to a scalar.

**Example 12.7.** Let \(G = GL_n\), and fix a uniformizer \(\pi \in \mathcal{O}\). Then

\[W_{ext} = \left\langle \begin{array}{c}
\text{permutation matrices} \\
\text{"finite part"}
\end{array} \right\rangle \times \left\langle \begin{pmatrix}
\pi^{\lambda_1} & \cdots & 0 \\
0 & \ddots & 0 \\
0 & \cdots & \pi^{\lambda_n}
\end{pmatrix}
\right\rangle.
\]

By Theorem 12.6, we can understand TRUM representations of \(G(K)\) by studying irreducible \(\mathcal{H}_{ext}\)-modules. Denote by \(Z := \text{Z}(\mathcal{H}_{ext}) = (\mathbb{Z}[v^{\pm 1}][X^\vee])^{W_f}\). By Quillen’s Lemma (which is an infinite-dimensional version of Schur’s Lemma), \(Z\) acts by scalars on any irreducible \(\mathcal{H}_{ext}\)-module. The Bernstein presentation tells us that \(\mathcal{H}_{ext}\) is finite over \(R := \mathbb{Z}[v^{\pm 1}][X^\vee]\). Since \(R\) is also finite over \(R^{W_f}\), we conclude that any irreducible \(\mathcal{H}_{ext}\)-module is finite-dimensional, and, in fact, is of dimension \(\leq |W_f|^2\).

Hence, the Deligne–Langlands conjecture predicts the following relationships.

\[
\begin{aligned}
\{ \text{irreps}/\mathbb{C} \text{ of } \mathcal{H}_{ext} \} & \xrightarrow{\text{finite}:1} \{ (s, x) \in G_C^\vee \times g_C^\vee \text{ s.t. } s \text{ is ss, } x \text{ nilp and } sxs^{-1} = qx \} /_{\text{conj}} \\
\{ \text{irreps of } Z \} & \xrightarrow{\sim} \{ \text{pairs } (s', v) \in G_C^\vee \times \mathbb{C}^x \} /_{G_C^\vee \text{ conj}} \xrightarrow{-----} \{ (s, x) \in G_C^\vee \times \mathbb{C}^x \} /_{G_C^\vee \text{ conj}}
\end{aligned}
\]
The dashed arrow should match $v^{-1} \leftrightarrow \sqrt{q}$.

**Remark 12.8.**

1. We are no longer forced to take $q = |k|$.

2. In the diagram above, we are repeatedly using the fact from last semester that

   \[
   \{\text{characters } \chi : \mathbb{Z}[X^r][W] \to \mathbb{C}\} \leftrightarrow \{\text{semisimple elts of } G \text{ up to conjugacy}\}.
   \]

An easy and interesting case: Consider the case when $s = id$ and $q = 1$. In this case, the right side of the dashed arrow is

\[
\{x \in \mathfrak{g}_C^\vee \text{ nilpotent}\}/G^\vee_{\text{conjugacy}} = \text{“nilpotent orbits.”}
\]

This provides a hint that we should not expect to have a good algebraic grip on the problem of understanding the irreducible representations of $H_{\text{ext}}$, because nilpotent orbits are complicated and not combinatorial in general. For the next lecture and a half, we will dive into this geometry.

### 12.3 Geometric setting

For notational convenience, we will temporarily swap $G \leftrightarrow G^\vee$ in this section. Let $G/\mathbb{C}$ be a complex reductive group, and $N \subset \text{Lie } G = : \mathfrak{g}$ the nilpotent cone.

**Remark 12.9.** For $GL_n$, it is tempting to define $\mathcal{N}$ as the variety

\[
\{x \in \mathfrak{gl}_n(\mathbb{C}) \mid x^n = 0\}.
\]

However, this results in a non-reduced scheme, because the ideal corresponding to the equation $x^n = 0$ is not radical. A better definition is to consider

\[
\{x \in \mathfrak{gl}_n(\mathbb{C}) \mid \text{coefficients of the characteristic polynomial vanish}\}.
\]

This still captures what we know as a nilpotent matrix, but results in a better geometric object. (In particular, it is a reduced scheme.)

In general, we define the nilpotent cone as follows. Consider the adjoint quotient map

\[
\mathfrak{g} \xrightarrow{q} \mathfrak{g}/G = \mathfrak{h}/W.
\]

The equality $\mathfrak{g}/G = \mathfrak{h}/W$ follows from Chevalley’s theorem. For $\mathfrak{gl}_n$, the map $q$ is “take coefficients of the characteristic polynomial,” so this captures what we wanted in Remark 12.9. We define

\[
\mathcal{N} = q^{-1}(0).
\]

**Fundamental facts about the nilpotent cone:**

1. $\mathcal{N}$ is irreducible, reduced, and normal.

2. $G$ has finitely many orbits on $\mathcal{N}$, and all are even-dimensional (over $\mathbb{C}$).
Example 12.10. If $G = GL_n$, then

$$\left\{ \begin{array}{c} \text{nilpotent} \\ \text{matrices} \end{array} \right\}_{\text{conj}} \leftrightarrow \left\{ \begin{array}{c} \text{Jordan} \\ \text{normal} \\ \text{form} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{partitions} \\ \lambda \vdash n \end{array} \right\}$$

Moreover, if we denote by $O_\lambda$ the orbit corresponding to the partition $\lambda$, then

$$O_\mu \subset O_\lambda \iff \mu \leq \lambda \text{ in dominance order}.$$ 

We can examine these orbit relations explicitly for small $n$.

$n = 2$: 

$$\mathcal{N} = \left\{ x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \text{Tr} \, x = \det x = 0 \right\} = \left\{ x = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \mid \det x = -a^2 - bc = 0 \right\} \subset \mathbb{C}^2.$$ 

A $\mathbb{R}$-picture of this is:

$n = 3$: For $n = 3$, the picture is more of a caricature.

Exercise 12.11. Try to do this for large $n$ (perhaps 7 or 8) and see that this poset is rather ugly; in particular, it is not graded.
12.4 The Springer resolution

We can study these nilpotent orbits by using a resolution of singularities of the nilpotent cone. Let $\mathcal{B}$ be the variety of Borel subalgebras in $\mathfrak{g}$. For $\mathfrak{gl}_n$, this is the variety of complete flags in $\mathbb{C}^n$.

**Definition 12.12.** The *Springer resolution* is the map

$$\tilde{\mathcal{N}} = \{(x, b) \in \mathcal{N} \times \mathcal{B} \mid x \in b\} \simeq T^*\mathcal{B}$$

which sends $(x, b) \mapsto x$.

Next week we will study the Springer resolution more carefully, and show that it is proper, smooth, and a resolution of singularities. For $GL_n$,

$$\tilde{\mathcal{N}} = \{(x, \{0\} = V_0 \subset V_1 \subset \cdots V_n = \mathbb{C}^n) \mid x \text{ preserves flag } \iff xV^i \subset V^{i-1}\}.$$

**Example 12.13.** We examine $GL_n$ for small $n$ again.

$n = 2$: The variety of Borel subalgebras is $\mathcal{B} = \mathbb{P}^1 \mathbb{C} = \{\text{lines in } \mathbb{C}^2\}$, and the Springer resolution looks like:

$n = 3$: The variety of Borel subalgebras is $\mathcal{B} = \{(\ell, P) \mid \ell \subset P \subset \mathbb{C}^2\}$ and a caricature of the Springer resolution looks like:
We will explain in more detail how we arrived at this picture next week.
Today we are going to pick up where we left off last week and continue to discuss the geometry of nilpotent orbits. To begin, we will discuss in more detail our claim from last week that $\tilde{N} \simeq T^*B$.

Let $G$ be an algebraic group and $\mathfrak{g}$ its Lie algebra. Canonically, we can express the tangent bundle of $G$ as $TG = G \times \mathfrak{g}$, since the Lie algebra can be identified with $T_e (G)$. Hence if $X$ is a homogeneous space for $G$ (i.e. $G$ acts on $X$ transitively), then we have a surjection $TG = G \times \mathfrak{g} \rightarrow TX$, and for $x \in X$, $T_x X = \mathfrak{g} / \text{Lie}(\text{stab}_G x)$. Similarly, there is a canonical identification of the cotangent bundle of $G$ $T^*G = G \times \mathfrak{g}^*$ and for a homogeneous space $X$, $T^*X \hookrightarrow T^*G$.

Moreover, for $x \in X$, $T_x X = (\text{Lie}(\text{stab}_G x))^\perp \subset \mathfrak{g}^*$.

Now assume that $G$ is semisimple and let $B$ be the variety of Borel subalgeras of $\mathfrak{g}$. Once we choose a Borel subalgebra $B \subset G$, we can identify $B \simeq G/B$ since $\text{stab}_G b = B$. Last lecture we introduced the following space

$\tilde{N} = \{(b, x) \in B \times \mathcal{N} | x \in b\}$.

**Claim 13.1.** There is a canonical isomorphism $\tilde{N} \simeq T^*B$.

**Proof.** For a point $b \in B$, the tangent space to $B$ at $b$ is $T_b B = \mathfrak{g} / (\text{Lie}(\text{stab}_G b) = b)$. Hence,

$T^*B = \{(b, v) \in B \times \mathfrak{g}^* | v \in b^\perp\}.$

Recall the Killing form $\kappa : \mathfrak{g} \times \mathfrak{g} \rightarrow \mathbb{C}$, $\kappa(x, y) = tr(ad x ad y)$. This is a symmetric, nondegenerate bilinear form. Fix a Cartan subalgebra $\mathfrak{h} \subset \mathfrak{b}$, and we obtain a triangular decomposition $\mathfrak{g} = \mathfrak{n}_- \oplus \mathfrak{h} \oplus \mathfrak{n}_+$, with $\mathfrak{b} = \mathfrak{h} \oplus \mathfrak{n}_+$. The restriction $\kappa|_{\mathfrak{h} \times \mathfrak{h}}$ is nondegenerate, and $\kappa$ gives a nondegenerate pairing $\kappa : \mathfrak{n}_- \times \mathfrak{n}_+ \rightarrow \mathbb{C}$.

Hence under the identification $\mathfrak{g} \simeq \mathfrak{g}^*$ via the Killing form, $b^\perp \subset \mathfrak{g}^*$ corresponds to $\mathfrak{n}_+ \subset \mathfrak{g}$. We conclude that

$T^*B = \{(b, x) \in B \times \mathfrak{g} | x \in \mathfrak{b} \text{ is nilpotent}\}$

$= \{(b, x) \in B \times \mathcal{N} | x \in \mathfrak{b}\}$

$= \tilde{N}.$

\[\square\]
13.1 Many examples of Springer fibres

“The richness of Springer fibres cannot be underestimated.”

Recall the Springer resolution

$$\tilde{N} = \{(x, b) \in N \times B \mid x \in b\} \simeq T^*B$$

\[\downarrow \pi_s \]

\[N\]

Definition 13.2. Let \(x \in O_{\lambda} \subset N\) be a point in a \(G\)-orbit. The associated Springer fibre \(F_{\lambda}\) is

\(F_{\lambda} := \pi_s^{-1}(x)\).

By equivariance, this is independent of the choice of \(x \in O_{\lambda}\), up to isomorphism.

Let \(G = SL_n\). This section is devoted to studying Springer fibres for \(n = 2, 3, 4\). Recall that for \(G = SL_n\),

\[\tilde{N} = \{(F^i, x) \in \text{complete flags in } \mathbb{C}^n \times N \mid x \text{ preserves } F^i\} = \{(F^i, x) \mid xF^i \subset F^{i-1}\}.

Example n = 2: The nilpotent cone is the quadric cone

\[N = \left\{ \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in \mathfrak{sl}_2 \mid -a^2 - bc = 0 \right\} \subset \mathbb{C}^3.

A \(\mathbb{R}\)-picture:
A table of orbits:

<table>
<thead>
<tr>
<th>$\lambda$</th>
<th>$\dim \mathcal{O}_\lambda$</th>
<th>$\text{codim } \mathcal{O}_\lambda$</th>
<th>$\text{Springer fibre}$</th>
<th>$\dim \text{fibre}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>0</td>
<td>$\mathbb{P}^1 \mathbb{C}$</td>
<td>0</td>
</tr>
</tbody>
</table>

**Example $n = 3$: A caricature:**

We’d like to construct a table as we did in the previous example, but to do so, we need to determine the dimension\(^7\) of the nilpotent orbits. This is easy for the regular nilpotent orbit and the zero orbit. But what about the other orbit $\mathcal{O}_\lambda$? Well we know that the matrix

$$e = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

is in the orbit, and we observe that

$$\text{Lie } (\text{stab}_{SL_3} e) = \text{stab}_{\text{Lie } SL_3} e = \ker \text{ad } e.$$ 

A computation shows that

$$\ker \text{ad } e = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & 0 \\ 0 & d & -2a \end{pmatrix} \mid a, b, c, d \in \mathbb{C} \right\}$$

\(^7\)If you’d like to understand some variety, it is a good idea to know its dimension!
is 4-dimensional, hence the orbit \( O_\lambda \) is \((8 - 4 = 4)\)-dimensional. We also need to determine the Springer fibre corresponding to this orbit. We have that

\[
F_\lambda = \{(L \subset P \subset \mathbb{C}^3) \mid e\mathbb{C}^3 \subset P, eP \subset L, \text{ and } eL = 0\},
\]

but what does this look like? Well we know that

\[
0 \subset \text{im} e \subset \ker e \subset \mathbb{C}^3,
\]

and the condition that a flag in \( F_\lambda \) must satisfy \( eL = 0 \) implies that \( L \subset \ker e \). We see that there are two possibilities for flags in \( F_\lambda \):

- \( \{L = \text{im} e, \text{ free choice of } P, \text{ as long as } L \subset P\} \simeq \mathbb{P}^1 \mathbb{C} \)
- \( \{P = \ker e, \text{ free choice of } L, \text{ as long as } L \subset P\} \simeq \mathbb{P}^1 \mathbb{C} \)

These two cases intersect when \( L = \text{im} e \) and \( P = \ker e \), which is a single point, so our Springer fibre looks like two \( \mathbb{P}^1 \mathbb{C} \)'s joined at a point. With this, we can complete our table of orbits:

<table>
<thead>
<tr>
<th>( \lambda )</th>
<th>[ ]</th>
<th>[ ]</th>
<th>[ ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \dim O_\lambda )</td>
<td>6</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>( \text{codim } O_\lambda )</td>
<td>0</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>( \text{Springer fibre} )</td>
<td>( pt )</td>
<td>( \mathbb{B} )</td>
<td>( \mathbb{B} )</td>
</tr>
<tr>
<td>( \dim \text{fibre} )</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

**Example \( n = 4 \):** Drawing pictures is no longer so reasonable, but we can still count dimensions and make our table. The dimension of \( \mathcal{B} \) is the number of positive roots (which for \( SL_4 \) is 6), so we know that \( \dim T^* \mathcal{B} = 12 \).

To find the dimensions of the Springer fibres, we can play a similar game to what we did in the previous example. Consider the orbit \( O_\lambda \) corresponding to

\[
\lambda = \[ \]
\]

The matrix

\[
e = \begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0
\end{pmatrix}
\]

is in \( O_\lambda \), and we have that

\[
0 \subset \text{im} e = \ker e \subset \mathbb{C}^4.
\]

The Springer fibre is

\[
F_\lambda = \{(L \subset P \subset H \subset \mathbb{C}^4) \mid e\mathbb{C}^4 \subset H, eH \subset P, eP \subset L, eL = 0\}.
\]

Again, we have two possibilities:
• (“easy component”) \{P = \text{im} e = \ker e, \text{free choice of } L, H \text{ as long as } L \subset P \subset H\} \simeq \mathbb{P}^1\mathbb{C} \times \mathbb{P}^1\mathbb{C} =: \Sigma_1

• (“hard component”) \{H = e^{-1}L\} =: \Sigma_2. There is a natural map \Sigma_2 \to \mathbb{P}^1\mathbb{C} sending (L \subset P \subset H) \mapsto L, and the fibre over \overline{L} is \{(L' \subset P \subset e^{-1}L' = H)\} \simeq \mathbb{P}^1\mathbb{C}, so \Sigma_2 is a \mathbb{P}^1\mathbb{C}\text{-bundle over } \mathbb{P}^1\mathbb{C}.

The diagonal \Delta \subset \Sigma_1 embeds into \Sigma_2 as the zero section, so these two components are glued together along a \mathbb{P}^1\mathbb{C}.

We’ve established that the second component \Sigma_2 is a \mathbb{P}^1\mathbb{C}\text{-bundle over } \mathbb{P}^1\mathbb{C}, but which one?

Claim 13.3. \Sigma_2 = \mathbb{P}(\mathcal{O}(1) \oplus \mathcal{O}(-1)) is the “second Hirzebruch surface.”

For justification of this claim, see Geordie’s hand-written notes. We finish this example by constructing our table.

<table>
<thead>
<tr>
<th>\lambda</th>
<th>\dim \mathcal{O}_\lambda</th>
<th>\codim \mathcal{O}_\lambda</th>
<th>\text{Springer fibre}</th>
<th>\dim \text{fibre}</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12</td>
<td>0</td>
<td>pt</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>2</td>
<td>\Sigma_1 \cup \mathbb{P}^1\mathbb{C} \Sigma_2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>4</td>
<td>\mathcal{B}_{SL_3} \cup 2 \text{ other comp.}</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>6</td>
<td>\mathcal{B}_{SL_4}</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>12</td>
<td>\Sigma_2</td>
<td>6</td>
</tr>
</tbody>
</table>

Now that we’ve constructed four tables, we can make some observations about patterns we see.

Observations:

• \(2 \dim F_\lambda = \codim \mathcal{O}_\lambda\)

• For any \(\lambda\), one (“easy”) component of \(F_\lambda\) is isomorphic to a flag variety of a smaller group.

• Fibres are equidimensional\(^8\) and components appear to be smooth\(^9\).

Remark 13.4. An audience member “Mr. Wiggins” also observed that in our examples, \(\dim T^*\mathcal{B}\) is divisible by all of the \(\codim \mathcal{O}_\lambda\), a property we coined “Wiggins divisibility.” (Though we are not sure if this is a general phenomenon...)

Many of our observations hold in general. Here are some fundamental properties of Springer fibers.

\(^8\)This is really remarkable!

\(^9\)Sadly this fails in bigger examples.
Theorem 13.5. Let $G$ be an a semisimple algebraic group.

1. The Springer resolution $\pi_s : \widetilde{N} \to N$ is a $G$-equivariant, projective resolution of singularities, and is an isomorphism over $N_{\text{reg}} = \{ x \in N \mid \dim Z_G X = \text{rank} g \}$.

2. For a nilpotent orbit $O_\lambda \subset N$, the corresponding Springer fibre $F_\lambda := \pi_s^{-1}(x), x \in O_\lambda$ is equidimensional, and $\dim F_\lambda = \frac{1}{2} \text{codim}(O_\lambda \subset N)$.

3. $H_{\text{odd}}(F_\lambda, Z) = 0$.

Remark 13.6.  
1. $H_{\text{even}}(F_\lambda, Z)$ is well-studied (for example, its Betti numbers are known).
2. Part 2. of the theorem implies that $\pi_s$ is semismall and all strata are relevant.
3. In type $A$, $F_\lambda$ have cell decompositions, $\mathbb{C}^0 \sqcup (\mathbb{C}^1)^2 \sqcup \cdots$. This cell decomposition implies 3. of the theorem for type $A$, but existence of cell decompositions is unknown in exceptional types.
4. In type $A$,

$$\# \{ \text{components of } F_\lambda \} = \dim(\text{irrep of } S_n \text{ indexed by } \lambda).$$

In fact, there exists a canonical bijection

$$\left\{ \begin{array}{c} \text{standard Young} \vspace{1mm} \\ \text{tableaux of shape } \lambda \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{components} \vspace{1mm} \\ \text{of } F_\lambda \end{array} \right\}.$$

13.2 The conormal space

Let

$$X = \bigsqcup_{\lambda \in \Lambda} X_\lambda$$

be a stratefied variety. For example, $\mathbb{C} = \mathbb{C}^\times \sqcup \{0\}$. Consider the space

$$\bigcup_{\lambda \in \Lambda} TX_\lambda \subset TX.$$

This is a horrible space! In our example, $T\mathbb{C} = \mathbb{C} \times \mathbb{C}$, and

$$\bigcup TV_\lambda = \{(x,y) \in \mathbb{C}^2 \mid x \neq 0 \text{ or } x = 0, y = 0\}.$$ 

Here’s a picture:
In contrast to this, the conormal space

\[ T^*_\Lambda X := \bigcup_{\lambda \in \Lambda} T^*_\lambda X \subset T^* X, \]

where \( T^*_\lambda X = \{ \xi \in T^*_x X \text{ for } x \in X_\lambda \mid \xi \text{ vanishes on } TX_\lambda \} \) is very nice. In our example of \( \mathbb{C} = \mathbb{C}^* \sqcup \{0\}, T^*_\Lambda \mathbb{C} = \{(x, y) \in \mathbb{C}^2 \mid xy = 0\}: \)

Properties of \( T^*_\Lambda X: \)

1. \( T^*_\Lambda X \) is a closed subvariety of \( T^* X. \)

2. \( \dim T^*_\lambda X = \dim X_\lambda + \text{codim}(X_\lambda \subset X) = \dim X \) is independent of \( \lambda! \) (So we have a “democracy of strata.”)

3. The components of the conormal space are in bijection with the strata.

The conormal space is a fundamental object in microlocal geometry.

**Warning:** the intersection pattern of \( T^*_\Lambda X \) may be very complicated.

An important object in our story arises as a conormal variety, the Steinberg variety.
13.3 The Steinberg variety

Let $H$ be a group that acts on a variety $X$ on the right, and a variety $Y$ on the left. We can form the balanced product

$$X \times_H Y := X \times Y / (xh, y) \sim (x, hy).$$

This space may not exist as a variety in general, but in all examples we will encounter, it does.

Choose a Borel subgroup $B \subset G$, so $B \simeq G/B$. Then consider the variety

$$G \times_B G/B \sim \to G/B \times G/B$$

$$(g, g'B) \mapsto (gg'B, g'B)$$

The set of $G$-orbits on $G \times_B G/B$ is equal to the set of $B$-orbits on $G/B$, which is parameterized by $W$ by the Bruhat decomposition. So we have a stratification

$$\mathcal{B} \times \mathcal{B} = \bigsqcup_{x \in W} O_x.$$

In type $A$, this stratification is given by “flags in relative position $x$.”

Example 13.7. There is a stratification of $\mathbb{P}^1 \mathbb{C} \times \mathbb{P}^1 \mathbb{C}$ given by

$$\mathbb{P}^1 \mathbb{C} \times \mathbb{P}^1 \mathbb{C} = \Delta \sqcup (\mathbb{P}^1 \mathbb{C} \times \mathbb{P}^1 \mathbb{C}) \setminus \Delta.$$

Pairs of flags in $\Delta$ are in relative position $id$ (i.e. they are equal), and flags in $(\mathbb{P}^1 \mathbb{C} \times \mathbb{P}^1 \mathbb{C}) \setminus \Delta$ are in relative position $s$.

Remark 13.8. The variety of Borel subalgebras $\mathcal{B}$ does not depend on any choices, so the product $\mathcal{B} \times \mathcal{B}$ does not depend on any choices. Since we can define the Weyl group as the set of $G$-orbits on $\mathcal{B} \times \mathcal{B}$, this gives us a canonical definition of the Weyl group that does not depend on a choice!

Definition 13.9. The Steinberg variety

$$St = \{(b, b', x) \in \mathcal{B} \times \mathcal{B} \times \mathcal{N} \mid x \in b, x \in b'\}$$

is given by the fibre product

$$\begin{array}{c}
\text{St} \\
\downarrow \\
\tilde{N} \\
\downarrow \\
\mathcal{N} \\
\downarrow \\
\tilde{N}
\end{array}$$

where the maps are

$$\begin{array}{c}
(b, b', x) \\
\downarrow \\
(b, x) \\
\downarrow \\
x
\end{array}$$

and

$$\begin{array}{c}
(b, b', x) \\
\downarrow \\
(b', x) \\
\downarrow \\
x
\end{array}$$
**Exercise 13.10.** (Solution can be found in Geordie’s hand-written notes.) Show that the Steinberg variety \( St \) is the conormal variety of

\[
B \times B = \bigsqcup_{x \in W} O_x.
\]

**Corollary 13.11.** There is a canonical bijection

\[
\begin{align*}
\{ \text{irred comp of } St \} & \leftrightarrow W. \\
\end{align*}
\]

Fix \( \lambda \), and two components \( C, C' \) of \( F_\lambda \). We have the following diagram

\[
\begin{array}{ccc}
\pi_s^{-1}(O_\lambda) & \rightarrow & O_\lambda \times C \\
\downarrow & & \downarrow \\
O_\lambda & \rightarrow & O_\lambda
\end{array}
\]

The set \( \{(x, c, c') \mid x \in O_\lambda, c \in C, c' \in C'\} \) is a subvariety in \( St \) of dimension

\[
\dim O_\lambda + \dim C + \dim C' = \dim O_\lambda + \frac{1}{2} \text{codim}(O_\lambda \subset N) + \frac{1}{2} \text{codim}(O_\lambda \subset N) = \dim N = \dim B \times B.
\]

The components of \( St \) all have dimension \( \dim B \times B \), so we have a bijection

\[
\{\text{components of } St\} \leftrightarrow \{(O_\lambda, C, C') \text{ as above}\}.
\]

In type \( A \), this is a bijection between

\[
W \leftrightarrow \{ (\lambda, T, T') \mid T, T' \text{ are standard Young tableaux of shape } \lambda \}.
\]

This is the Robinson-Schensted correspondence!
Lecture 14 (October 11, 2019): Springer correspondence, Borel-Moore homology, convolution algebras

We pick up in the setting of the last lecture, the Springer resolution:

\[ \tilde{N} \simeq T^*B \]
\[ F_x := f^{-1}(x) \]
\[ \pi_s : \tilde{N} \subset g \]
\[ \pi_G : \tilde{g} \supset \tilde{g}_{r,s} \]

Roughly, the Springer correspondence states that \( W \) acts on \( H^*(F_x; \mathbb{Q}) \), and one obtains all irreducible representations of \( W \) in top cohomology. Note that this does not come from an action of \( W \) on \( F_x \)! This is in contrast to Deligne-Lusztig theory and other settings where we obtain representations of a group in the cohomology of varieties on which the group acts. In the first part of today’s lecture, we’ll work towards a precise statement of the Springer correspondence.

Remark 14.1. In type A, the Springer correspondence explains why irreducible representations of the symmetric group and nilpotent orbits are both classified by the same combinatorial data (Young diagrams).

Grothendieck-Springer alteration: Let

\[ \tilde{g} = \{(x, b) \in g \times B | x \in b\} \]

In type A, this is equal to

\[ \{(x, F) \in g \times \mathcal{F}lags | xF^i \subset F^i\} \]

Remark 14.2. Note that \( \tilde{g} \subset B \times g \), and its dual is \( \tilde{N} = T^*B \). (This is because the dual of \( x \in b \) is \( x \in b^\perp = n \).)

The key diagram is the following:

\[ \tilde{N} \subset \tilde{g} \supset \tilde{g}_{r,s} \]
\[ \pi_s : \tilde{N} \subset g \supset g_{r,s} \]

where \( g_{r,s} = \{x \in g | x \text{ regular semisimple}\} \). Note that \( g \neq N \cup g_{r,s} \).

Theorem 14.3. 1. The map \( \pi_s \) is semismall.

2. The map \( \pi_G \) is small (i.e., \( \pi_{G,*}k[g][\text{dim } g] = IC(g_{r,s}, \mathcal{L}) \)).

3. Over \( g_{r,s} \), \( \pi_G \) is a \( W \)-torsor. (Here \( W \) is the Weyl group of \( G \).)
For example, in type A,
\[ \mathfrak{g}_{r,s} = \{ x \in \mathfrak{g} \mid x \text{ is semisimple with distinct eigenvalues} \}. \]
To give a flag \( F \) preserved by \( x \) is equivalent to an ordering of the eigenvalues of \( x \). This is a \( S_n \)-torsor.

Now we are ready to state the Springer correspondence precisely. Given \( x \in \mathcal{N} \), let \( A_G(x) \) be the component group of the centralizer: \( A_G(x) := C_G(x)/C_G(x)^0 \).

**Theorem 14.4.** (Springer correspondence)
1. \( \pi_{ss} Q_{\tilde{\mathcal{N}}}^{\dim \tilde{\mathcal{N}}} = \bigoplus_{x \in \mathcal{N}/G, \rho \in \text{Irr} A_G(x)} H_{\text{top}}(F_x) \rho \otimes IC(G \cdot x, \mathcal{L}_{\rho}) \).
2. (**Most important**) \( \text{End}(\pi_{ss} Q_{\tilde{\mathcal{N}}}^{\dim \tilde{\mathcal{N}}}) = \text{End}(\pi_G Q_{\tilde{\mathcal{g}}}^{\dim \tilde{\mathcal{g}}}) = kW \).
3. \( \{ H_{\text{top}}(F_x) \rho \} \) are all irreducible representations of \( W \).

**Remark 14.5.** Part 2. of the theorem is true over \( \mathbb{Z} \), and indeed over any ring. But part 1. fails over arbitrary rings because the decomposition theorem fails.

How might we approach part 2.? Three possible approaches:

(a) **Borho - MacPherson:**
- First note that because \( \tilde{\mathcal{g}} \to \mathfrak{g} \) is small, the fact that \( \text{End}(\pi_G Q_{\tilde{\mathcal{g}}}^{\dim \tilde{\mathcal{g}}}) = kW \) is obvious. Indeed,
  \[ \text{End}(\pi_G Q_{\tilde{\mathcal{g}}}) = \text{End}(\pi_{G, reg, ss}) = \text{End}_W(W) = kW, \]
  with the first equality following from smallness.
- Then BM point out that we have a homomorphism
  \[ \text{End}(\pi_G Q_{\tilde{\mathcal{g}}}) \xrightarrow{r} \text{End}(i^* \pi_G Q_{\tilde{\mathcal{g}}}) = \text{End}(\pi_{ss} Q_{\tilde{\mathcal{N}}}) \]
  where \( i : \mathcal{N} \hookrightarrow \mathfrak{g} \); and, miraculously, \( r \) is an isomorphism. (Proof sketch: The map \( r \) is injective because the action of \( W \) on \( H^*(\mathcal{B}) \) is faithful, then compare dimensions.)

(b) **Fourier transform:** (Springer’s original approach) Because \( \tilde{\mathcal{N}} \) and \( \tilde{\mathcal{g}} \) are dual in \( \mathcal{B} \times \mathfrak{g} \), \( k_{\tilde{\mathcal{N}}} \) and \( k_{\tilde{\mathcal{g}}} \) are Fourier transforms of one another. This implies that the endomorphism rings are equal:
  \[ \text{End}(\pi_{ss} k_{\tilde{\mathcal{N}}}) = \text{End}(\pi_G k_{\tilde{\mathcal{g}}}) = kW. \]

(c) **Convolution algebras:** (in Chris-Ginzburg)

The next part of the lecture will explain this approach. For impatient readers, we’ll give away the ending:

**The punchline:** There is a notion of homology (Borel-Moore homology, \( H_{BM} \)) such that \( \text{End}(\pi_{ss} k_{\tilde{\mathcal{N}}}) \) is canonically equal to \( H_{BM}(\text{Steinberg variety}) \). This gives a concrete realisation of this endomorphism algebra.
14.1 Borel-Moore homology

Let $X$ be an algebraic variety, $k$ a field, $p : X \to pt$, and $k_X$ the constant sheaf on $X$. Here are four notions of (co)homology:

- $H^*(X; k) = H^*(p_* k_X)$ - cohomology (cochains)
- $H^*_c(X; k) = H^*(p_! k_X)$ - cohomology with compact support
- $H_*(X; k) = H_{-*}(p_! \omega_X)$ - homology (chains)
- $H^B_*(X; k) = H^{-*}(p_* \omega_X)$ - Borel-Moore homology (locally finite chains)

Here $\omega_X$ is the dualising sheaf, $\mathbb{D} k_X$. The canonical example is the following.

Example 14.6. Let $X = \{ z \in \mathbb{C} \mid 0 < |z| < 1 \}$. Then

$H_0(X; \mathbb{Z}) = \mathbb{Z}$, $H_1(X; \mathbb{Z}) = \mathbb{Z}$, $H_2(X; \mathbb{Z}) = 0$.

If we compute Borel-Moore homology, we get

$H_0^B(X; \mathbb{Z}) = 0$, $H_1^B(X; \mathbb{Z}) = \mathbb{Z}$, $H_2^B(X; \mathbb{Z}) = \mathbb{Z}$ “fundamental class”.

In the first computation ($H^B_0$), the formal generator of $H_0$ is now a boundary, so we get 0. In the second computation ($H^B_1$), we can now have cycles from the edge to the center, and these are not boundaries. In the third computation ($H^B_2$), the “fundamental class” is a triangulation of $X$.

From now on in this course, $H_* = H^B_*$. 

Key properties of Borel-Moore homology:

1. If $X \hookrightarrow M$ is a closed embedding of $X$ into a smooth, $\mathbb{C}$-dimension $d$ variety $M$, then we have local Poincaré duality: $\omega_M \simeq k_M[2d]$. Hence

$$H_*(X; k) = H^{-*}(X, \omega_X)$$

$$= H^{-*}(X, i^! \omega_M)$$

$$= H^{-*}(M, i_* i^! \omega_M[2d])$$

$$= H^{2d-*}(M, i_* i^! \omega_M)$$

$$= H^{2d-*}(M, M \setminus X; k).$$

2. $H_*(-)$ is not functorial for arbitrary maps, but for proper maps $p$, we have $p_*$. 

115
3. For an open inclusion $U \hookrightarrow X$, we have restriction

$$H_*(X) \to H_*(U).$$

(Thought exercise: Why? In terms of chains?)

4. If $X$ is equidimensional of dimension $d$ with components $X_1, X_2, \ldots, X_m$, then

$$H_{2d}(X) = \bigoplus \mathbb{Z}[X_i],$$

where $[X_i]$ are the fundamental classes of the components.

**Geometric convolution algebras:** Let $X_1, X_2, X_3$ be smooth varieties of dimensions $d_1, d_2, d_3$, respectively, and

$$Z_{12} \subset X_1 \times X_2, \quad Z_{23} \subset X_2 \times X_3$$

closed subvarieties (“correspondences”). (For example, we could take $Z_{12} = \text{graph}(f)$ for some $f : X_1 \to X_2$.) Define

$$Z_{12} \circ Z_{23} := \{(x_1, x_3) \in X_1 \times X_3 \mid \text{there exists } x_2 \in X_2 \text{ s.t. } (x_1, x_2) \in Z_{12}, (x_2, x_3) \in Z_{23}\}.$$

(So in our example, $\text{graph}(f) \circ \text{graph}(g) = \text{graph}(g \circ f)$.) We have projections

$$\begin{array}{ccc}
X_1 \times X_2 \times X_3 & \xrightarrow{p_{12}} & X_1 \times X_2 \\
| & & | \\
X_1 \times X_3 & \xrightarrow{p_{13}} & X_1 \times X_2 \times X_3 \\
| & & | \\
X_2 \times X_3 & \xrightarrow{p_{23}} & X_2 \times X_3
\end{array}$$

We make the following **properness assumption:** From now on, assume that the map

$$p_{13} : p_{12}^{-1}(Z_{12}) \cap p_{23}^{-1}(Z_{23}) \to X_1 \times X_3$$

is proper.

**Definition 14.7.** We define a **convolution product** on homology:

$$H_i(Z_{12}) \times H_j(Z_{23}) \to H_{i+j-2d_2}(Z_{12} \circ Z_{23})$$

$$(c_{12}, c_{23}) \mapsto p_{13*}(p_{12}^*c_{12} \cap p_{23}^*c_{23})$$

Here $\cap$ is the intersection product in Borel-Moore homology.

**Most important cases:** Let $\tilde{X} \xrightarrow{f} X$ be a proper map of a smooth variety $\tilde{X}$ to $X$, and let $X_i = \tilde{X}$ for $i = 1, 2, 3$. Here are two cases of the construction above:

1. Let $Z_{12} = Z_{23} = Z_{12} \circ Z_{23} = \tilde{X} \times_X \tilde{X} \subset \tilde{X} \times \tilde{X}$. Then the convolution product gives an associative algebra structure on $H_*(\tilde{X} \times \tilde{X})$ (with messy gradings).
2. Let \( Z_{12} = \tilde{X} \times_X \tilde{X} \), \( Z_{23} = f^{-1}(X) \), \( Z_{12} \circ Z_{23} = Z_{23} \). Then the convolution product gives us a map

\[
H_*(\tilde{X} \times_X \tilde{X}) \times H_*(f^{-1}(X)) \to H_*(f^{-1}(X)).
\]

This gives \( H_*(f^{-1}(X)) \) the structure of a \( H_*(\tilde{X} \times \tilde{X}) \)-module.

So whenever we have a smooth proper map into our variety, we obtain from this formalism an associative algebra and a collection of modules (one for each fibre) over that algebra. Seems promising!

**Conceptual explanation of convolution algebras:** Let \( f \) be as above, with the fibre product diagram

\[
\begin{array}{ccc}
\tilde{X} \times_X \tilde{X} & \xrightarrow{g} & \tilde{X} \\
\downarrow g & & \downarrow f \\
\tilde{X} & \xrightarrow{f} & X
\end{array}
\]

**Claim:** \( \text{End}'(f_*k_{\tilde{X}}) = H_*(\tilde{X} \times_X \tilde{X}) \)

**Proof.** We will only check the statement on the level of vector spaces. Let \( d_X := \dim \mathbb{C} X \). We have

\[
\text{Hom}'(f_*k_{\tilde{X}}, f_*k_{\tilde{X}}) = \text{Hom}'(f^*f_*k_{\tilde{X}}, k_{\tilde{X}}) \\
= \text{Hom}'(f^*f_*k_{\tilde{X}}, k_{\tilde{X}}) \\
= \text{Hom}'(g^*g^*k_{\tilde{X}}, k_{\tilde{X}}) \\
= \text{Hom}'(k_{\tilde{X} \times_X \tilde{X}}, g^!k_{\tilde{X}}) \\
= \text{Hom}'(k_{\tilde{X} \times_X \tilde{X}}, g^!\omega_{\tilde{X} \times_X \tilde{X}}[-2d_X]) \\
= H^{*-2d_X}(\tilde{X} \times_X \tilde{X}, \omega_{\tilde{X} \times_X \tilde{X}}) \\
= H_{2d_X-2}(\tilde{X} \times_X \tilde{X}).
\]

Here we are using properness of \( f \) (second equality), adjunctions (first equality, fourth equality), proper base change (third equality), and local Poincaré duality (fifth equality). \( \square \)

**The Upshot:** Up to gradings,

\[
H_*(\tilde{X} \times_X \tilde{X}) = \text{End}'(f_*k_{\tilde{X}}),
\]

and with some work we can show that multiplication matches on both sides. Similarly,

\[
(f_*k_{\tilde{X}})_x = H_*(f^{-1}(X)),
\]

and the module structure comes from the action \( \text{End}'(f_*k_{\tilde{X}}) \circ (f_*k_{\tilde{X}})_x \).

**Connection to the Spring correspondence:**
Let $\tilde{N} \to \mathcal{N}$ be the Springer resolution, and

$$St := \tilde{N} \times_{\mathcal{N}} \tilde{N} = \text{conormal space to the } G\text{-space } B \times B = \bigcup_{x \in W} T^*_x,$$

the Steinberg variety. (See lecture 13.) Here $T^*_x$ is the conormal bundle to the $G$-orbit $O_x \subset B \times B$. Recall that $St$ is equidimensional and all components have dimension equal to $N := \dim B \times B = \dim T^*B$.

The convolution product in Borel-Moore homology gives us a map

$$H_{2N}(St) \times H_{2N}(St) \xrightarrow{*} H_{4N-2\dim T^*B}(St) = H_{2N}(St).$$

This gives $H_{2N}(St)$ the structure of an algebra!

**Theorem 14.8.** As algebras,

$$H_{2N}(St) = kW.$$

By the theory earlier, the action of $kW$ on $H_i(F_x)$ yields the Springer action. And we end up with $W$-modules everywhere!
15 Lecture 15 (October 18, 2019): More convolution algebras, Kazhdan–Lusztig isomorphism, Bezrukavnikov's equivalence (rough statement)

Last week we ended with a discussion on convolution algebras. We'll start today by continuing this discussion. Consider the following two settings:

1. Let $G$ be a group and $H \subset G$ a subgroup. With the operation $*$ of convolution of functions, the vector space $\text{Fun}(G, \mathbb{C})$ of complex-valued functions on $G$ has the structure of an algebra. This is just the group algebra, $\text{Fun}(G, \mathbb{C}) \simeq \mathbb{C}[G]$. The subspace $\text{Fun}_{H \times H}(G, \mathbb{C})$ of $H$-biinvariant functions forms a subalgebra. This is a Hecke algebra. As many of us are aware, its representation theory is very complicated in general!

2. Now let $X$ be a finite set. The vector space $\text{Fun}(X \times X, \mathbb{C})$ of complex-valued functions on $X \times X$ can also be given the structure of an algebra. In this setting, the convolution product is given as follows. Let $X \times X \times X \xrightarrow{p_{12}} X \times X \xleftarrow{p_{13}} X \times X \xrightarrow{p_{23}} X \times X$ be the natural projections. Then for $f, g \in \text{Fun}(X \times X, \mathbb{C})$, define $f \ast g \in \text{Fun}(X \times X, \mathbb{C})$ by

$$(f \ast g)(x, z) := \sum_{y \in X} f(x, y)g(y, z)$$

for $(x, z) \in X \times X$. In other words,

$$f \ast g = p_{13}!(p_{12}^*f \boxtimes p_{23}^*g).$$

With $\ast$, $(\text{Fun}(X \times X, \mathbb{C}), \ast)$ is an algebra. In fact, it's a familiar algebra. Let $e_{x,y}$ be the indicator function on $(x, y) \in X \times X$. Then $e_{x,y} \ast e_{y,z} = \delta_{y,z} e_{x,z}$. Hence,

$$(\text{Fun}(X \times X, \mathbb{C}), \ast) \simeq \text{Mat}_{X \times X}(\mathbb{C}).$$

Some Variants:

(a) Let $X \to Y$ be a map of sets, then we can construct the convolution algebra

$$\text{Fun}(X \times_Y X, \mathbb{C}) \simeq \prod_{y \in Y} \text{Mat}_{f^{-1}(y) \times f^{-1}(y)}(\mathbb{C}).$$

---

10This is why we don’t meet this algebra as often as we meet the Hecke algebra - it’s “too easy,” in the sense that it is just a matrix ring. However, when we categorify, it becomes more interesting, so we are more likely to encounter it (or recognize it!) in categorified settings.
We can formulate Mashke’s theorem in this language. For a finite group $G$, let $Y = \{\text{irreps of } G\}$, $X = \bigsqcup_{\rho \in Y} \{\text{basis of } \rho\}$, and $X \to Y$ the map which assigns to a basis element the corresponding representation. Then Mashke’s Theorem that the group algebra is semisimple is the following statement:

**Theorem 15.1.** (Mashke’s Theorem)

$$(\text{Fun}(G, \mathbb{C}), \ast) \simeq (\text{Fun}(X \times_Y X, \mathbb{C}), \ast).$$

This realizes a complicated algebra (the group algebra) in terms of much simpler pieces (matrix rings).

(b) If our sets $X,Y$ come with the additional structure of an action by a group $\Gamma$, and $X \to Y$ is a $\Gamma$-equivariant map of sets, then we can construct the convolution algebra

$$\text{Fun}^\Gamma(X \times_Y X, \mathbb{C}).$$

**The Upshot:** There are two types of convolution algebras, one is hard (Hecke algebras), and the other is easy (Fun$(X \times X, \mathbb{C})$). The hard one is of great significance in representation theory. A strategy that we use in representation theory is to try to realise the hard type as the easy type.

### 15.1 Equivariant $K$-theory

Let $G$ be an algebraic group acting on a variety $X$. Then we can formulate the notion of an equivariant coherent sheaf,

$$\mathcal{F} \in \text{Coh}_G(X),$$

as a coherent sheaf $\mathcal{F}$ on $X$, coupled with some extra data. Roughly speaking, one can think of an equivariant coherent sheaf on $X$ as being an equivariant sheaf together with an algebraic action on its sections.

**Remark 15.2.** If $\mathcal{F}$ is locally free, then $\mathcal{F}$ corresponds to a vector bundle $V \to X$ on $X$. In this setting, $G$-equivariance of $\mathcal{F}$ corresponds to an algebraic $G$-action on $V$ which is compatible with projection. In particular,

$$\text{Coh}_G(pt) \simeq \text{Rep} G,$$

where $\text{Rep} G$ is the category of algebraic representations of $G$.

Define two types of equivariant $K$-groups:

$$K^G(X) := \text{Grothendieck group of } G\text{-equivariant coherent sheaves on } X;$$

$$K_G(X) := \text{Grothendieck group of } G\text{-equivariant vector bundles on } X.$$

---

11 For an excellent description of this construction, see notes from Emily’s Sept 20, 2019 talk in the Informal Friday Seminar. Notes from Emily’s (and all other) IFS talks can be found at https://sites.google.com/view/ifssydney/home
Remark 15.3.  (a) Very loosely,

\[ K^G(X) \leftrightarrow \text{“Borel–Moore homology,”} \]
\[ K_G(X) \leftrightarrow \text{“cohomology.”} \]

(b) There are higher $K$-groups, $K_i^G(X), K_i^G(X)$, which we will ignore here. (Already $K^G_0(X) = K^G(X)$ and $K^G_0(X) = K^G_0(X)$ are rich enough.)

(c) There is a natural map

\[ K^G(X) \to K^G(X). \]

If $X$ is smooth, then we can use resolutions by coherent sheaves to show that this map is an isomorphism.

(d) We have to be careful with functors between $K$-groups. For example, if $X \to pt$ is projection and $X$ is affine, then $f_*O_X = \Gamma(X, O_X)$ is usually infinite dimensional. So in general, we need to work to justify that functors we wish to use preserve Coh, or at least $D^b(\text{Coh})$.

As we did for $H_*$, we have a convolution product in $K$-theory. We imitate the set-up of the previous lecture: Let $X_1, X_2, X_3$ be smooth varieties of dimensions $d_1, d_2, d_3$, respectively, and

\[ Z_{12} \subset X_1 \times X_2, \quad Z_{23} \subset X_2 \times X_3 \]

closed subvarieties, with projections $p_{ij}, i, j = 1, 2, 3$ as before. Given $F \in \text{Coh}(Z_{12}), G \in \text{Coh}(Z_{23})$, define

\[ F * G := p_{13*}(p_{12}^* F \otimes p_{23}^* G) \in D^b(\text{Coh}(Z_{12} \circ Z_{23})). \]

As we emphasized in Remark 15.3, we need to justify that this product is well-defined. But sure enough, the push-forward $p_{13*}$ preserves coherence because $p_{13}$ is proper, and the pull-backs $p_{12}^*, p_{23}^*$ are okay because $p_{12}$ and $p_{23}$ are flat. Hence $*$ induces a product

\[ K_0(Z_{12}) \times K_0(Z_{23}) \to K_0(Z_{12} \circ Z_{23}) \]

which descends to a product

\[ K^G(Z_{12}) \times K^G(Z_{23}) \to K^G(Z_{12} \circ Z_{23}). \]

Example 15.4. Let $X$ be a finite set, and $X \to pt$ projection to a point. In this case, elements of $\text{Coh}(X \times X)$ are “matrices of vector spaces,” and

\[ * : \text{Coh}(X \times X) \times \text{Coh}(X \times X) \to \text{Coh}(X \times X) \]

is “multiplication of matrices.” That is, for vector spaces $V_{ij}$,

\[
\begin{pmatrix}
V_{11} & V_{12} \\
V_{21} & V_{22}
\end{pmatrix} \times \begin{pmatrix}
V_{11}' & V_{12}' \\
V_{21}' & V_{22}'
\end{pmatrix} = \begin{pmatrix}
V_{11} \otimes V_{11}' \oplus V_{12} \otimes V_{12}' & V_{11} \otimes V_{12}' \oplus V_{12} \otimes V_{22}' \\
V_{21} \otimes V_{11}' \oplus V_{22} \otimes V_{12}' & V_{21} \otimes V_{12}' \oplus V_{22} \otimes V_{22}'
\end{pmatrix}.
\]

The $K$-group is $K_0(X \times X) = \text{Fun}(X \times X, \mathbb{Z})$.

Remark 15.5. Lusztig noticed that certain categories of the form $\text{Coh}^\Gamma(X \times X)$, where $\Gamma$ is a group acting on a finite set $X$, are central to the classification of unipotent character sheaves.
15.2 Kazhdan–Lusztig isomorphism

With this we have enough machinery to state the Kazhdan–Lusztig isomorphism. Let $(X \supset R, X^\vee \supset R^\vee)$ be a root datum, $W_{ext} = W_f \ltimes ZX^\vee$ the extended affine Weyl group, and $H_{ext}$ the affine Hecke algebra. (See Lecture 11 for a refresher on these objects.) Let $G^\vee$ be the corresponding algebraic group, $\mathcal{N}^\vee \subset g^\vee$ the nilpotent cone, and $St^\vee := T^*B^\vee \times_{\mathcal{N}^\vee} T^*B^\vee$ the Steinberg variety. (See Lecture 13.)

**Theorem 15.6.** (Kazhdan–Lusztig) We have canonical isomorphisms.

\[
\begin{align*}
\mathcal{H}_{ext} & \sim \to K^{G^\vee \times \mathbb{C}^\times}(St^\vee) \\
\text{forget}_{\mathbb{C}^\times-\text{action}} \downarrow & \quad \downarrow \\
ZW_{ext} & \sim \to K^{G^\vee}(St^\vee)
\end{align*}
\]

Here $\mathbb{C}^\times$ acts on $T^*B^\vee$ by dilation along the fibres.

Here are two examples of how Theorem [15.6] gives us insight into the representation theory of affine Hecke algebras.

1. (Bernstein) As we have discussed, there is an inclusion of algebras:

\[
Z[v^{\pm 1}][X^\vee] \subset \mathcal{H}_{ext} \\
\lambda \mapsto H_\lambda
\]

Bernstein noticed that the center of $\mathcal{H}_{ext}$ can be realized as $W_f$-invariants of this subalgebra:

\[
Z[v^{\pm 1}][X^\vee]^{W_f} = Z(\mathcal{H}_{ext}).
\]

We can see this in terms of the Kazhdan–Lusztig isomorphism. Recall that for a map $X \to Y$ between finite sets, we have

![Diagram](image)

and $\text{Fun}(\text{diag}, \mathbb{C}) \subset \text{Fun}(X \times Y, \mathbb{C})$ are “diagonal matrices.” Applying this to the diagonal $T^*B^\vee \subset St^\vee$, we can think of

\[
K^{G^\vee \times \mathbb{C}^\times}(T^*B^\vee) \subset K^{G^\vee \times \mathbb{C}^\times}(St^\vee)
\]

as “diagonal matrices.” Now by homotopy,

\[
K^{G^\vee \times \mathbb{C}^\times}(T^*B^\vee) = K^{G^\vee \times \mathbb{C}^\times}(B^\vee),
\]

and since $K^{B^\vee}(pt) = [\text{Rep} B^\vee] = Z[X^\vee]$ and $K^{C^\times}(pt) = [\text{Rep} C^\times] = Z[v^{\pm 1}]$,

\[
K^{G^\vee \times \mathbb{C}^\times}(B^\vee) = K^{G^\vee \times \mathbb{C}^\times}(G^\vee/B^\vee) = K^{B^\vee \times \mathbb{C}^\times}(pt) = Z[v^{\pm 1}][X^\vee].
\]
So the subalgebra $\mathbb{Z}[v^{\pm 1}]X^\vee$ sits inside $H_{\text{ext}}$ as “diagonal matrices” in the $G^\vee \times \mathbb{C}^\times$-equivariant $K$-group of $St^\vee$. Moreover, $K^{G^\vee \times \mathbb{C}^\times}(pt)$ is clearly central in $K^{G^\vee \times \mathbb{C}^\times}(St^\vee)$, and this gives the Bernstein center:

$$K^{G^\vee \times \mathbb{C}^\times}(pt) = (K^{B^\vee \times \mathbb{C}^\times}(pt))^{W_f} = (\mathbb{Z}[v^{\pm 1}]X^\vee)^{W_f}.$$  

2. The Kazhdan–Lusztig basis of $H_{\text{ext}}$ leads to the notion of (left, right, two-sided) cells. Lusztig noticed that the sets

$$\left\{ \text{poset of 2-sided cells} \right\} \leftrightarrow \left\{ \text{nilpotent orbits in } \mathcal{N}^\vee \right\}$$

appear to match.

He also noticed other remarkable parallels, such as

$$\text{2-sided cell is finite } \iff \text{reductive part of the centralizer is finite}.$$  

These parallels convince one rather quickly that this correspondence is deep.

We can use Theorem 15.6 to understand this observation of Lustig. Consider the projections

$$\xymatrix{ \text{St}^\vee \ar[dr]_p \ar[ddr] \ar[dl] \ar[ddll] \ar[ddrrr] & & \text{T}^*\mathcal{B}^\vee \ar[dl] \ar[dr] & \text{T}^*\mathcal{B}^\vee \ar[ddll] \ar[ddrrr] \\
\mathcal{N}^\vee }$$

Convolution makes it clear that any closed $G^\vee$-invariant subvariety $Z \subset \mathcal{N}^\vee$ gives rise to a two-sided ideal in $K^{G^\vee \times \mathbb{C}^\times}(St^\vee)$:

$$\{ [M] \mid \text{supp } M \subset p^{-1}(Z) \}.$$

---

12Pictures of 2-sided cells in rank 2 can be found on Lusztig’s webpage: [http://www-math.mit.edu/~gyuri/picture.html](http://www-math.mit.edu/~gyuri/picture.html)
Hence we get a filtration of $\mathcal{H}_{ext}$ by nilpotent orbits in $\mathcal{N}$. Lusztig and Bezrukavnikov showed that the filtration of $\mathcal{H}_{ext}$ coming from 2-sided cells agrees with this filtration coming from geometry, explaining Lusztig’s observation that the 2-sided cell order matches the order on nilpotent orbits.

3. We won’t explain this in detail due to time constraints, but one can show relatively easily that Theorem 15.6 implies the Deligne–Langlands conjecture (Section 12.2) on representations of $\mathcal{H}_{ext}$, as long as $q$ is not a root of unity.

15.3 Bezrukavnikov’s equivalence: rough outline

Now we are finally in the position to approach the second half of the title of this course. Here is a rough outline of the flow of ideas that lead to Bezrukavnikov’s equivalence:

- **Langlands correspondence**: A correspondence between sets satisfying a whole host of properties, and with many extraordinary consequences in number theory and beyond.

- **Weil**: In the function field case, an automorphic form\(^{13}\) can be regarded as a (very special) function

  \[
  f : \text{Bun}_G(\mathbb{F}_q) := \left\{ \text{iso classes of } G\text{-bundles on } \text{smooth curves}/\mathbb{F}_q \right\} \to \mathbb{C}.
  \]

- **Grothendieck**: Functions on a variety should be understood as shadows of sheaves (function-sheaf correspondence). Here are some examples.

  - **E.g. 1**: Characters of $GL_n(\mathbb{F}_q)$ are shadows (trace of Frob) of certain $\ell$-adic sheaves on $G$, “character sheaves.”

  - **E.g. 2**: Interesting analytic functions should satisfy many differential equations (i.e. should be solutions of a holonomic $\mathcal{D}$-module).

- **Drinfeld**: The Langlands correspondence should be approached using Grothendieck’s dictionary. At its most basic level, this philosophy asserts that automorphic forms in the function field case should arise as traces of Frobenius of certain sheaves on the moduli space of $G$-bundles. At a more sophisticated level, we should expect an equivalence of categories

  \[
  D^b(\text{Sh(Bun}_G)) \leftrightarrow D^b(\text{Coh(Loc}_G)),
  \]

  i.e. a “geometric Langlands correspondence.” This allows us to work over $\mathbb{C}$, and provides fertile connections to physics, higher category theory, etc.

\(^{13}\)We haven’t gone into what an automorphic form is yet in this course. For a global field $K$ it is a function of a special form on a certain quotient of the adelic points of a reductive group. In the function field case, Weil realised that this quotient parametrises $G$-bundles on the corresponding curve. In other words, in the function field case an automorphic form can be regarded as a function of the form given above.
Remark 15.7. Geometric Langlands is for function fields. The classical Langlands correspondence isn’t. So they seem to be living in different worlds, but the hope is that they are actually related. For many years this appeared to many as a pretty wild idea. However, recently the geometric Langlands program has been shown to have consequences that number theorists really care about. For example Fargues showed [Far18] that geometric Langlands for the Fargues-Fontaine curve implies (part of) the LLC for any $p$-adic group!

- **Ginzburg**: A small piece of geometric Langlands should be controlled by a categorification of the Kazhdan–Lusztig isomorphism

\[ \mathcal{H}_{ext} \simeq K^{G^\vee \times \mathbb{C}^\times} (St^\vee). \]

What is sought is a fundamental monoidal category that arises in two Langlands dual ways. Recall that the geometric Satake equivalence categorifies $\mathcal{H}^{sph} = K^G(pt)$ (Theorem 11.2). Thus this equivalence can be seen as one layer of difficulty beyond the geometric Satake equivalence.

- **Bezrukavnikov**: realization of (several) such equivalences:

\[ K^{G^\vee \times \mathbb{C}^\times} (St^\vee) \rightsquigarrow \text{Coh}^{G^\vee \times \mathbb{C}^\times} (St^\vee) \text{ “coherent side”} \]

\[ \mathcal{H}_{ext} \rightsquigarrow D^b_{Iw}(G((t))/Iw) \text{ “constructible side”} \]

Theorem 15.8. (Bezrukavnikov’s equivalence, most basic version) Let $Iw \subset G((t))$ be an Iwahori subgroup, and $Iw_0 \subset Iw$ the pro-unipotent radical. There is an equivalence of monoidal categories

\[ \left( D^b_{Iw_0}(G((t))/Iw), * \right) \simeq \left( D^b \text{Coh}^{G^\vee \times \mathbb{C}^\times} (\widetilde{St}^\vee), * \right). \]

where $\widetilde{St}^\vee = \widetilde{g}^\vee \times_{\widehat{G}^\vee} \widetilde{g}^\vee$ and the hat indicates the pro-unipotent completion.

Remark 15.9. There are several aspects of the above that need explanation, hopefully this will occur over the coming weeks and months!
16 Lecture 16 (November 1, 2019): Motivating the constructible side of Bezrukavnikov’s equivalence

Last lecture we ended by stating (modulo several undefined pieces) Bezrukavnikov’s equivalence:

\[ \left( \frac{D^b_{Iw}(G((t))/I\omega), \ast}{\ast} \right) \cong \left( D^b \text{Coh}^{G^\vee \times C^\vee} (\widetilde{St}^\vee), \ast \right). \]

Our goal for today is to motivate the constructible side of this equivalence. To do so, we will explain Grothendieck’s function-sheaf correspondence in slightly more detail than is usually done. The starting place is the Weil conjectures.

16.1 Weil conjectures

The Weil conjectures were a collection of statements (made by Weil while in jail in \( \sim \) 1943) about counting the number of points on an algebraic variety over a finite field. Let \( X \) be a smooth projective algebraic variety over \( \mathbb{F}_q \). Then we can ask about the number of points \( \#X(\mathbb{F}_q^n) \) for all \( n \). Weil conjectured that a generating series built out of \( \#X(\mathbb{F}_q^n) \) has remarkable properties. He also pointed out that his conjecture would follow from an interpretation of \( \#X(\mathbb{F}_q^n) \) as the trace of an operator on a vector space, by taking traces of its powers. The Grothendieck–Lefschetz trace formula, which we briefly visited in the context of elliptic curves in Lecture 4, provides such an interpretation.

Grothendieck–Lefschetz trace formula: Let \( \ell \) be a prime not dividing \( q \), and \( X \) as above (but not necessarily projective). Then

\[ \#X(\mathbb{F}_q^n) = \text{sTr}(\text{Frob}_q^n \circ H^i_c(X_{\mathbb{F}_q}, \mathbb{Q}_\ell)) := \sum_i (-1)^i \text{Tr} \left( \text{Frob}_q^n \circ H^i_c(X_{\mathbb{F}_q}, \mathbb{Q}_\ell) \right). \quad (16.1) \]

Here \( H^i_c(X_{\mathbb{F}_q}, \mathbb{Q}_\ell) \) denotes the compactly supported étale cohomology of \( X_{\mathbb{F}_q} \), the base change of \( X \) to \( \text{Spec} \mathbb{F}_q \). If \( X/k \), then \( H^*_c(X, \mathbb{Q}_\ell) \) has a continuous action of \( \text{Gal}(\overline{k}/k) \). The symbol \( \text{sTr} \) in (16.1) stands for “supertrace.” Let’s see what this formula means in examples.

Example 16.1. Let \( X = \mathbb{P}^1_{\mathbb{F}_q} \), then the cohomology and action of Frobenius are given by the following table:

<table>
<thead>
<tr>
<th>( i )</th>
<th>( H^i_c(X_{\mathbb{F}<em>q}, \mathbb{Q}</em>\ell) )</th>
<th>Frob action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>( \mathbb{Q}_\ell )</td>
<td>( \circ q )</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>( \mathbb{Q}_\ell )</td>
<td>( \circ 1 )</td>
</tr>
</tbody>
</table>

Hence,

\[ \text{sTr} \left( \text{Frob}_q^n \circ H^* \right) = 1 + q^n = \#X(\mathbb{F}_q^n). \]
Example 16.2. Let $X = \mathbb{G}_m$. Then the action of Frobenius on cohomology is:

<table>
<thead>
<tr>
<th>$i$</th>
<th>$H^i_c(X_{\overline{\mathbb{F}}<em>q}, \mathbb{Q}</em>\ell)$</th>
<th>Frob action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$\mathbb{Q}_\ell$</td>
<td>$\otimes q$</td>
</tr>
<tr>
<td>1</td>
<td>$\mathbb{Q}_\ell$</td>
<td>$\otimes 1$</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Hence,

$$s\text{Tr} \left( \text{Frob}_q^n \otimes H^* \right) = q^n - 1 = #\mathbb{G}_m(\mathbb{F}_q^n) = #\mathbb{F}_q^\times.$$

Example 16.3. Let $X = \text{Spec} \mathbb{F}_q^2 / \text{Spec} \mathbb{F}_q$. Then

$$X(\mathbb{F}_q^n) = \text{Hom}(\text{Spec} \mathbb{F}_q^n, \text{Spec} \mathbb{F}_q^2) = \text{Hom}_{\mathbb{F}_q}\text{-alg}(\mathbb{F}_q^2, \mathbb{F}_q^n) = \begin{cases} 0 & n \text{ odd,} \\ 2 & n \text{ even.} \end{cases}$$

On the geometric side,

$$X_{\overline{\mathbb{F}}_q} = \text{Spec} \mathbb{F}_q \times_{\text{Spec} \mathbb{F}_q} \text{Spec} \mathbb{F}_q^2 = \text{Spec}(\mathbb{F}_q \otimes_{\mathbb{F}_q} \mathbb{F}_q^2) = \text{Spec} \mathbb{F}_q \sqcup \text{Spec} \mathbb{F}_q \simeq \mathbb{F}_q \times \mathbb{F}_q.$$

Remark 16.4. For analogy, an easier version of the computation above is the following. We can realize

$$\mathbb{C} \simeq \mathbb{R}[x]/(x^2 + 1).$$

Then

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}[x]/(x^2 + 1) = \mathbb{C}[x]/(x - i)(x + i) \simeq \mathbb{C} \times \mathbb{C}.$$

The Upshot: The variety $X_{\overline{\mathbb{F}}_q}$ consists of 2 points which are interchanged by $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. So our table of cohomology is

<table>
<thead>
<tr>
<th>$i$</th>
<th>$H^i_c(X_{\overline{\mathbb{F}}<em>q}, \mathbb{Q}</em>\ell)$</th>
<th>Frob action</th>
</tr>
</thead>
<tbody>
<tr>
<td>$&gt; 0$</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>$\overline{\mathbb{Q}}<em>\ell \oplus \overline{\mathbb{Q}}</em>\ell$</td>
<td>$\otimes \begin{pmatrix} 0 &amp; 1 \ 1 &amp; 0 \end{pmatrix}$</td>
</tr>
</tbody>
</table>

and

$$s\text{Tr} \left( \text{Frob}_q^n \otimes H^* \right) = \begin{cases} 0 & n \text{ is odd,} \\ 2 & n \text{ is even.} \end{cases}$$
The Grothendieck–Lefschetz formula and the examples above can be realized as shadows
of something happening on the level of sheaves. Let $k$ be a field. Then, roughly,

$$\text{Spec} \ k = \text{pt} / \text{Gal}(\overline{k}/k).$$

In other words, one can think of Spec $k$ as something like the classifying space of its absolute
Galois group. There is a bijection

$$\text{étale cohomology sheaves on } \text{Spec} \ k \cong \text{finitely generated}\n\text{Z}/\ell^m\text{Z-modules with an action of } \text{Gal}(\overline{k}/k)$$

finite-dimensional continuous
representations of $\text{Gal}(\overline{k}/k)$
on $\mathbb{Q}_\ell$-vector spaces

Let $\mathcal{F} \in D^b_c(X, \mathbb{Q}_\ell)$ be a object in the bounded derived category of constructible $\mathbb{Q}_\ell$-sheaves
on $X$. Then for any $x \in X(\mathbb{F}_q^n)$, we get an inclusion

$$\text{Spec} \mathbb{F}_q^n \hookrightarrow X,$$

and hence an object $i^* \mathcal{F} \in D^b_c(\text{Spec} \mathbb{F}_q^n, \mathbb{Q}_\ell)$. Applying the supertrace of Frobenius to this
object results in an element of $\mathbb{Q}_\ell$. In this way, we get a map

$$D^b_c(X, \mathbb{Q}_\ell) \xrightarrow{f} \prod_{n \geq 1} \text{Fun}(X(\mathbb{F}_q^n) \to \mathbb{Q}_\ell).$$

If $\mathcal{F} \to \mathcal{G} \to \mathcal{F}' \xrightarrow{+1} \mathcal{F}$ is a distinguished triangle in $D^b_c(X, \mathbb{Q}_\ell)$, then $f(\mathcal{F}) + f(\mathcal{F}') = f(\mathcal{G})$. In
other words, $f$ factors through the Grothendieck group:

$$[D^b_c(X, \mathbb{Q}_\ell)] \xrightarrow{f} \prod_{n \geq 0} \text{Fun}(X(\mathbb{F}_q^n), \mathbb{Q}_\ell).$$

A consequence of the Chebotarev density theorem (Theorem 1.3) is that this map is injective;
that is, for a given $q^n$, the collection of all of the functions $f(\mathcal{F})$ completely determine the class
of $\mathcal{F}$ in the Grothendieck group. Now, Grothendieck tells us how to view this relationship.

**Grothendieck’s philosophy**: Interesting functions $X(\mathbb{F}_q^n) \to \mathbb{C}, \mathbb{Q}_\ell$, etc. should be shadow-

ows of interesting sheaves.

Lusztig provided us with an extraordinary example of a case where Grothendieck’s phi-
losophy is exactly true.

**Example 16.5.** (Lusztig’s theory of character sheaves) There exists a set

$$\{ \mathcal{F}_\chi \in D^b_c(\text{GL}_n, \mathbb{Q}_\ell) \}$$

such that $\mathcal{F}_\chi$ yield all irreducible characters $\chi : \text{GL}_n(\mathbb{F}_q^n) \to \mathbb{C}$ of all $\text{GL}_n(\mathbb{F}_q^n)$ “at once.”
16.2 The Hecke algebra, revisited

In the second half of this lecture, we will describe another example of Grothendieck’s philosophy: the Hecke category. To start, we will recall the origin of the Hecke algebra.

Let $G$ be a split reductive group over a finite field $\mathbb{F}_q$ and $B \subset G$ a Borel subgroup. We can define a convolution algebra

$$H_{\mathbb{F}_q} = \{ \text{Fun}_{B(\mathbb{F}_q) \times B(\mathbb{F}_q)}(G(\mathbb{F}_q), \mathbb{C}), \ast \}$$

of complex-valued $B(\mathbb{F}_q)$-biinvariant functions on $G(\mathbb{F}_q)$. A priori, the structure of this algebra seems to depend on $q$, but Iwahori found a presentation of $H_{\mathbb{F}_q}$ which depends almost only on the Weyl group. Let $(W, S)$ be the Coxeter system associated to $B \subset G$. Iwahori’s presentation has generators $\{ T_s \mid s \in S \}$, and relations

$$T_s^2 = (q - 1)T_s + q, \quad T_s T_t \cdots = T_t T_s \cdots,$$

where the products on the second line are of $m_{st} = \text{order}(st)$ generators. In Iwahori’s presentation, the element $T_s$ corresponds to the indicator function $\mathbbm{1}_{B_s B} \in \text{Fun}_{B(\mathbb{F}_q) \times B(\mathbb{F}_q)}(G(\mathbb{F}_q), \mathbb{C})$. Iwahori’s presentation demonstrated that the Hecke algebra $H_{\mathbb{F}_q}$ is “defined over $\mathbb{Z}[q]$.”

The quadratic relation may look a little mysterious at first, but it has a natural geometric origin.

**Origin of the quadratic relation:** Take $G = \text{SL}_2(\mathbb{F}_q)$ and $B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$. Then on one hand,

$$\mathbbm{1}_G \ast \mathbbm{1}_G = \text{pushforward of the constant function on } G \times_B G \under the multiplication map } G \times_B G \xrightarrow{m} G$$

But on the other hand, there is a natural isomorphism

$$G \times_B G \xrightarrow{\sim} G/B \times G$$

$$(g, h) \mapsto (gB, gh)$$

and the multiplication map factors through this isomorphism:

$$\begin{array}{ccc}
G \times_B G & \xrightarrow{\sim} & G/B \times G \\
\downarrow m & & \downarrow \text{proj to } G \\
G & &
\end{array}$$

Hence,

$$\mathbbm{1}_G \ast \mathbbm{1}_G = \text{pushforward of constant function on } G/B \times G \under the projection to } G$$

$$= |G/B| \cdot \mathbbm{1}_G$$

$$= (1 + q) \mathbbm{1}_G.$$
From this, we deduce the quadratic relation: Since $1_G = 1_{B \times B} + 1_B = T_s + 1$, we have

$$T_s^2 + 2T_s + 1 = (T_s + 1)^2 = (q + 1)(T_s + 1) = (q + 1)T_s + q + 1 = (q - 1)T_s + q + 2T_s + 1.$$ 
Hence $T_s^2 = (q - 1)T_s + q$.

The geometric origin of the Hecke algebra suggests a categorification via Grothendieck’s philosophy. Let $G$ be a split reductive group over $\mathbb{F}_q$, and $B \subset G$ a Borel subgroup. Define the (first incarnation of) the Hecke category to be

$$\mathcal{H} := D^b_{B \times B}(G, \mathbb{Q}_\ell),$$

the $B \times B$-equivariant derived category of étale $\mathbb{Q}_\ell$-sheaves, in the sense of Bernstein-Lunts. We won’t describe the precise construction of this category, but in its first approximation we can consider objects in $D^b_{B \times B}(G, \mathbb{Q}_\ell)$ to be étale sheaves which are constructible for $B \times B$-orbits.

The convolution of functions in $H_{\mathbb{F}_q}$ can be upgraded to a convolution product on sheaves. Let $\mathcal{F}, \mathcal{G} \in D^b_{B \times B}(G)$. We have maps

$$\cdots \quad \xrightarrow{p_1} \quad \xrightarrow{p_2} \quad \cdots$$

Then if $\mathcal{F}, \mathcal{G} \in D^b_{B \times B}(G, \mathbb{Q}_\ell)$, we define

$$\mathcal{F} \ast \mathcal{G} := \text{mult}_*(\widetilde{\mathcal{F}} \mathcal{G}) \in D^b_{B \times B}(G, \mathbb{Q}_\ell),$$

where $\widetilde{\mathcal{F}} \mathcal{G} \in D^b_{B \times B}(G \times B, \mathbb{Q}_\ell)$ corresponds to $\text{res}^{B \times B \times B}_{B \times B \times B}(p_1^* \mathcal{F} \times p_2^* \mathcal{G})$ under the equivalence

$$D^b_{B \times B \times B}(G \times G, \mathbb{Q}_\ell) \simeq D^b_{B \times B \times B}(G \times B \times G, \mathbb{Q}_\ell).$$

**Example 16.6.** Let $k = \mathbb{Q}_\ell$, and $G = \text{SL}_2$. Then

$$k_{\text{SL}_2} \ast k_{\text{SL}_2} = \text{mult}_*(k_{\text{SL}_2 \times \text{SL}_2}) = H^* (\mathbb{P}^1) \otimes k_{\text{SL}_2}.$$ 
This is the categorified version of the Hecke algebra equality $1_G \ast 1_G = (1 + q)1_G$ that we discussed earlier!

\[\text{Be careful! This approximation is just an approximation and can get you in trouble if you take it too literally...}\]
16.3 Perverse sheaves on $\mathbb{P}^1\mathbb{C}$

The time has come for an interlude. For the rest of this lecture we will shift gears and consider the variety $\mathbb{P}^1\mathbb{C}$ with the stratification $\Lambda$ given by

$$\mathbb{P}^1\mathbb{C} = \{0\} \sqcup C_\infty.$$

Denote by $\{0\} \hookrightarrow \mathbb{P}^1\mathbb{C} \xhookleftarrow{} C_\infty$ the natural inclusions. It is very important in what is coming to understand perverse sheaves on $\mathbb{P}^1\mathbb{C}$ with the stratification $\Lambda$, so we will discuss this (and generalizations) in the upcoming lectures. So what are the perverse sheaves on $\mathbb{P}^1\mathbb{C}$?

Here's an algebraic answer (c.f. Emily's talk on nearby cycles in the Informal Friday Seminar):

$$\text{Perv}_\Lambda(\mathbb{P}^1\mathbb{C}, k) \simeq \left\{ V_1 \xleftrightarrow[v \circ c] \ V_0 \mid v \circ c = 0 \right\},$$

where $V_i$ are finite-dimensional $k$ vector spaces representing the nearby cycles at 0 (the vector space $V_1$) and the vanishing cycles at 0 (the vector space $V_0$). From this perspective, we can see that there are five indecomposable objects:

1. $\mathbb{0} \xrightarrow{k \sim i_*k_0}$, skyscraper at 0

2. $\mathbb{k} \xrightarrow{0 \sim} \text{constant sheaf}$

3. $\mathbb{k} \xrightarrow{i_0 \sim k}$, $\mathcal{I}_\infty \xrightarrow{\text{head}} \mathcal{I}_0 \xrightarrow{\text{socle}}$

4. $\mathbb{k} \xrightarrow{j_*k_n \sim k}$, $\mathcal{I}_0 \xrightarrow{j_*k_n \sim \text{(Somm-Weil)}} (\text{Somm-Weil})$

---

15 All IFS talk notes can be found on the IFS website: [https://sites.google.com/view/ifssydney/home](https://sites.google.com/view/ifssydney/home)
5. \( k \xrightarrow{=} k \oplus k \leadsto \text{“big projective/tilting sheaf”} \)

In the next lecture we will go into more detail and describe perverse sheaves on general curves.
17 Lecture 17 (March 6, 2020): Constructible and perverse sheaves on curves

Today we continue our interlude of the previous lecture and discuss perverse sheaves on curves. We are working toward understanding Beilinson glueing on curves, which will be the main topic of next week’s lecture. Let \( k \) be a field, fixed throughout, and let \( X/\mathbb{C} \) be a variety, viewed with the classical topology. Let \( V \) be a \( k \)-vector space. We have the notion of a constant sheaf \( V_X \) with values in \( V \):

\[
V_X(U) := \{ f : U \to V \text{ continuous} \},
\]

where \( V \) is viewed with the discrete topology. This leads to the notion of a local system, which is a locally constant sheaf with finite-dimensional stalks.

**Theorem 17.1.** If \( X \) is connected, there is a bijection

\[
\left\{ \text{local systems on } X \right\} \leftrightarrow \operatorname{Rep}(\pi_1(X,x)).
\]

**Remark 17.2.** The difference between local systems and vector bundles is captured with the following picture.

Here the pink lines are intended to denote the sections of our local systems/vector bundles. Vector bundles with flat connections are equivalent to local systems. However, local systems form an abelian category, whereas vector bundles do not.

The notion of a local system leads us to the notion of a constructible sheaf: A sheaf \( \mathcal{F} \) on \( X \) is constructible if there exists a stratification \( X = \bigsqcup_{\lambda \in \Lambda} X_\lambda \) of \( X \) by a finite number of subvarieties \( X_\lambda \) such that \( \mathcal{F}|_{X_\lambda} \) is a local system for all \( \lambda \in \Lambda \). Finally, the notion of a constructible sheaf leads to the notion of the bounded derived category of constructible sheaves:

\[
D^b_c(X,k) := \left\{ \mathcal{F} \mid \mathcal{H}^i(\mathcal{F}) \text{ is constructible for all } i, \text{ and } \mathcal{H}^i(\mathcal{F}) = 0 \text{ for } |i| > 0 \right\} \subset D^b \left( \text{sheaves of } k\text{-vector spaces on } X \right).
\]
From now on, assume that $X$ is a connected, smooth curve.

Choose a set of points $\{x_1, \ldots, x_m\}$, and let $U$ denote their complement in $X$. Fix the stratification $\Lambda$:

$$X = U \sqcup \{x_1\} \sqcup \cdots \sqcup \{x_m\}.$$ 

**Theorem 17.3.** There is an equivalence

$$\left\{ \text{$\Lambda$-constructible sheaves on } X \right\} \sim \left\{ \begin{array}{l} \mathcal{L} \text{ local system on } U, \\ V_1, \ldots, V_m \text{ finite-dimensional vector spaces} \\ \text{maps } \phi_i : V_i \to (\mathcal{L}_{n_i})^{\mu_i} \end{array} \right\}.$$

Here $n_i \in X$ is a “nearby point” to $x_i$, and $\mathcal{L}_{n_i}$ denotes the stalk, which carries a monodromy operator $\mu_i$ given by a small loop around $x_i$ (see the diagram below). Note that the stalk depends on the choice of nearby point $n_i$, but the invariants in the stalk do not!

17.1 Perverse sheaves

One way to visualize an object $\mathcal{F} \in D^b_{\text{c}}(X)$ is via its table of stalks:

<table>
<thead>
<tr>
<th></th>
<th>$i-1$</th>
<th>$i$</th>
<th>$i+1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U$</td>
<td>$\cdots$</td>
<td>$\mathcal{H}^i(\mathcal{F}</td>
<td>_U)$</td>
</tr>
<tr>
<td>$x_1$</td>
<td>$\cdots$</td>
<td>$\mathcal{H}^i(\mathcal{F}</td>
<td>_{x_1})$</td>
</tr>
<tr>
<td>$x_2$</td>
<td>$\cdots$</td>
<td>$\mathcal{H}^i(\mathcal{F}</td>
<td>_{x_2})$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
</tbody>
</table>

We will use these tables frequently in the remainder of this lecture.

The category of **perverse sheaves**

$$\text{Perv}_\Lambda(X) \subset D^b_{\text{c}}(X)$$
is defined as the heart of the $t$-structure
\[ D^\leq_{\Lambda} := \left\{ \mathcal{F} \left| \begin{array}{l} H^i(\mathcal{F}|_U) = 0 \text{ for } i \geq 0 \\ H^i(\mathcal{F}|_{x_i}) = 0 \text{ for } i > 0 \end{array} \right. \right\}, \quad D^\geq_{\Lambda} = \mathbb{D}(D^\leq_{\Lambda}). \]

Here $\mathbb{D}$ denotes Verdier duality. We have two possibilities for what the table of stalks can look like for a perverse sheaf in $\text{Perv}_\Lambda(X)$:

<table>
<thead>
<tr>
<th>support</th>
<th>$-2$</th>
<th>$-1$</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_i$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$U$</td>
<td>0</td>
<td>$\mathcal{L}$</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>skyscraper</th>
<th>$-2$</th>
<th>$-1$</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_i$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$U$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$W'$</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A general strategy when trying to understand an abelian category is to try to produce and study exact functors from that category to a well-understood category (like Vect or representations of a group). For perverse sheaves, this strategy proves to be somewhat complicated, and brings nearby and vanishing cycles into our world.

**Theorem 17.4.** (to be explained)

\[
\text{Perv}_\Lambda(X) \cong \left\{ \begin{array}{l}
\mathcal{L} \text{ local system on } U, \\
V_1, \ldots, V_m \text{ finite-dimensional vector spaces ("vanishing cycles"), maps } V_i \xrightarrow{\nu} \mathcal{L}_{\mu_i} \text{ s.t. } \nu \circ u = \text{id} - \mu_i
\end{array} \right\}
\]

**Remark 17.5.** The category $\text{Perv}_\Lambda(X)$ is Verdier self-dual. The category of $\Lambda$-constructible sheaves is not:

\[
\mathbb{D}(\text{A-constructible sheaves}) \simeq \{ \phi_i : \mathcal{L}_{\mu_i} \to V_i \}
\]

**Example 17.6.** Here are some examples of perverse sheaves.

- If $i : \{x_j\} \hookrightarrow X$, then $i_* k$ is perverse.
- The constant sheaf $k_{x_j}$ on $\{x_j\}$ is perverse.
- For a local system $\mathcal{L}$ on $X$, $\mathcal{L}[1]$ is perverse. (This follows because $\mathbb{D}\mathcal{L}[1] \cong \mathcal{L}'[1]$, where $\mathcal{L}'$ denotes the dual local system.)
- Let $j : U \hookrightarrow X$ and $\mathcal{L}$ a local system on $U$. Then we claim that $j_! \mathcal{L}[1]$ and $j_* \mathcal{L}[1]$ are both perverse. Because $j_!$ is extension by zero, computing the stalks of $j_! \mathcal{L}[1]$ is easy:

<table>
<thead>
<tr>
<th>support</th>
<th>$-2$</th>
<th>$-1$</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_i$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$U$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Computing the stalks of the direct image $j_* := Rj_*$ is trickier. Let $x \in X$ be a point. Then

\[ H^i((j_* \mathcal{L})_x) = \lim_{B(x, \epsilon)} H^i(B(x, \epsilon) \cap U, \mathcal{L}) \]

\[ = \begin{cases} 
\mathcal{L}_x & \text{if } x \in U, \\
H^i(B(x, \epsilon) \setminus \{x\}, \mathcal{L}) & \text{if } x \not\in U.
\end{cases} \]
How can we compute the cohomology \( H^i(B(x, \epsilon) \setminus \{x\}, \mathcal{L}) \)? The space \( B(x, \epsilon) \setminus \{x\} \) is homotopic to \( S^1 \). We can compute the cohomology of \( S^1 \) with coefficients in \( \mathcal{L} \) using the two-term complex

\[
V \xrightarrow{id-\mu} V.
\]

Hence \( H^0(S^1, \mathcal{L}) = V^\mu \), the invariants of \( \mu \) \( \odot \) \( V \), and \( H^1(S^1, \mathcal{L}) = V_\mu \), the coinvariants. (Alternatively, one can see that \( H^0(S^1, \mathcal{L}) = V^\mu \) directly, and conclude that \( H^1(S^1, \mathcal{L}) = V_\mu \) by Poincaré duality.) Hence, the table of stalks of \( j_* \mathcal{L}[1] \) is

| \( U \) | -2 | -1 | 0 | 1 |
|\( x_i \) | 0 | \( \mathcal{L} \) | 0 | 0 |

Because \( \mathcal{D}(j_* \mathcal{L}) = j_! \mathcal{D}(\mathcal{L}) \), we can conclude from these computations that \( j_* \mathcal{L}[1] \) and \( j_! \mathcal{L}[1] \) are both perverse. In other words, \( j_* \) and \( j_! \) are exact for the perverse \( t \)-structure.

Next we turn our attention to classifying the simple objects in \( \text{Perv}_\Lambda(X) \). Recall that there is a natural map \( j_! \to j_* \).

Given \( \mathcal{L} \) a local system on \( U \), define

\[
IC(X, \mathcal{L}) := j_!(\mathcal{L}) := \text{Im}(j_! \mathcal{L}[1] \to j_* \mathcal{L}[1]).
\]

This is not obvious, but by a construction of Deligne, we have

\[
IC(X, \mathcal{L}) = \tau_{\leq -1}(j_* \mathcal{L}[1]),
\]

where \( \tau_{\leq -1} \) is the truncation functor in the standard (not perverse) \( t \)-structure. Hence the table of stalks for \( IC(X, \mathcal{L}) \) is

| \( U \) | -2 | -1 | 0 | 1 |
|\( x_i \) | 0 | \( \mathcal{L} \) | 0 | 0 |

\begin{itemize}
  \item **Remark 17.7.** We see from the remarks above that when \( X \) is a curve, all IC sheaves are shifts of actual constructible sheaves. This is not the case in general!
  \item **Example 17.8.** Consider a local system \( \mathcal{L} \) on \( U \) such that the monodromy \( \mu \) does not have 1 as an eigenvalue. Then \( id - \mu \) is invertible. Hence \( V_\mu = V^\mu = 0 \). Recall that the general form of the tables of stalks of \( j_! \mathcal{L}[1] \) and \( j_* \mathcal{L}[1] \) are

\[
j_! \mathcal{L}[1]: \begin{array}{c|cccc}
\hline
\overline{U} & -2 & -1 & 0 & 1 \\
\overline{x_i} & 0 & \mathcal{L} & 0 & 0 \\
\hline
\end{array}
\quad j_* \mathcal{L}[1]: \begin{array}{c|cccc}
\hline
\overline{U} & -2 & -1 & 0 & 1 \\
\overline{x_i} & 0 & \mathcal{L} & 0 & 0 \\
\hline
\end{array}
\]

So the fact that \( V_\mu = V^\mu = 0 \) implies that the natural map \( j_! \mathcal{L}[1] \to j_* \mathcal{L}[1] \) is an isomorphism. We conclude that in this case

\[
IC(X, \mathcal{L}) = j_! \mathcal{L}[1] = j_* \mathcal{L}[1].
\]

136
Theorem 17.9. The category $\text{Perv}_{\Lambda}(X)$ is a finite-length abelian category with simple objects

$$\{IC(X, \mathcal{L}) \mid \mathcal{L}|_U \text{ is irreducible}\} \cup \{i_*k \mid i : \{x_i\} \hookrightarrow X\}.$$

For any irreducible local system $\mathcal{L}$ on $U$, we have the distinguished triangle

$$\tau_{\leq -1}(j_*\mathcal{L}[1]) \to j_*\mathcal{L}[1] \to \tau_{\geq 0}(j_*\mathcal{L}[1]) \xrightarrow{+1}$$

$$IC(X, \mathcal{L}) \to j_*\mathcal{L}[1] \to (V_\mu)_0 \xrightarrow{+1}$$

in $D^b_c(X, k)$. There is something distinctive about this triangle: all objects are perverse sheaves! Hence, this is an exact sequence and we've found our first composition series. We can draw this composition series with an “egg diagram:”

$$j_*\mathcal{L}[1] = \begin{array}{c}
\frac{\bigvee_{\mu}}{\text{IC}(x, \mathcal{I})} \\
\end{array}$$

(17.1)

Example 17.10. Here is a special case of the construction above. Let $D$ be a disc and

$$D^\times \xrightarrow{j} D \xleftarrow{i} \{0\}$$

the natural inclusions. Then the composition series of $j_*k_{D^\times}[1]$ is

$$j_*k_{D^\times}[1] = \begin{array}{c}
\frac{\bigvee_{\mu} k_{\circ}}{\text{IC}(\mathcal{I}, \mathcal{O})} \\
\end{array}.$$ 

Example 17.11. Let

$$U \xrightarrow{j} X \xleftarrow{i} Z := X \setminus U$$

be the natural inclusions. Then in $D^b_c(X, k)$ we have the distinguished triangle

$$ji^!j_X \to k_X \to i_*i^*k_X \xrightarrow{+1}.$$  

(17.2)

By turning triangles, we obtain

$$i_*k_Z \to j_ik_U[1] \to k_X[1] = IC(X) \xrightarrow{+1}.$$
All objects in this triangle are perverse sheaves, so this is a composition series! Hence we have the following egg:

\[ j_*k_{D\times}[1] = \frac{\mathcal{I}(\{ x \in \mathbb{A}^1 \})}{k_2}. \]

We could also have obtained this by dualizing (17.1).

**Remark 17.12.** Constructible sheaves on \( X \) are not necessarily finite length (see (17.2)). However, perverse sheaves are. This is one of the reasons why we are so fond of them.

Before moving on to glueing, we will do one more fun calculation. We return to the local case:

\[ D^\times \to D \leftarrow \{0\} \]

Let \( \mathcal{L}_n \) be a local system on \( D^\times \) with monodromy given by a single Jordan block of size \( n \):

\[ J_n = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & \ddots \\ \ddots & \ddots & 1 \\ 1 & & \end{pmatrix} \]

Our goal is to describe \( j_!\mathcal{L}_n[1] = \text{Im}(j_!\mathcal{L}_n[1] \to j_*\mathcal{L}_n[1]) \) in this setting. Recall that the functors \( j_! \) and \( j_* \) are exact because \( j \) is affine, and we have the building blocks

\[ j_*k_{D\times}[1] = \frac{\mathcal{I}(\{ x \in \mathbb{A}^1 \})}{\mathcal{I}(\mathbb{A}^1)} \]

138
In local systems on $D^\times$, we have

\[ \mathcal{L}_n = \cdots \xrightarrow{j_!} \mathcal{L}_1 \xrightarrow{j_!} \mathcal{L}_0 \xrightarrow{j_!} 0 \]

Remark 17.13. In this example, we see that the functor $j_!$ preserves injections and surjections, but is NOT exact. This is the case in general.

### 17.2 Nearby and vanishing cycles, Beilinson glueing

Let $D$ be the disc, $D^\times$ the punctured disc, and $\tilde{D}^\times$ its universal cover. Let

\[ \{0\} \xrightarrow{i} D \xrightarrow{j} D^\times \xleftarrow{p} \tilde{D}^\times \]

be the natural maps.

**Motivation:** We want to define the “stalk” of a perverse sheaf at singular points.

Recall the nearby cycles functor $\psi_f$ (c.f. Emily’s Oct 18, 2019 IFS talk or Laurentiu’s Feb 21/28, 2020 IFS series): For a local system $F$ on $D^\times$,

\[ \psi_f(F) = i^* j_* p_* p^* F \]
\[ = i^* j_* p_* (p^* F \otimes k_{\tilde{D}^\times}) \]
\[ = i^* j_* (F \otimes p_* k_{\tilde{D}^\times}). \]

Here the third equality follows from the projection formula. The sheaf $p_* k_{\tilde{D}^\times}$ is the “universal local system on $D^\times$.” It is an infinite-dimensional local system with stalk $k[x^{\pm 1}]$ and monodromy $x$.

Recall that the monodromy $\mu \circ \psi_f(F)$, so we get a decomposition into generalized eigenspaces:

\[ \psi_f(F) = \bigoplus \psi_f^\lambda(F). \]

By far the most important of these eigenspaces corresponds to $\lambda = 1$, the “unipotent nearby cycles.” Indeed, from this, we can recover all others:

\[ \psi_f^1(F) = \psi_f^1(F \otimes k_{\lambda - 1}). \]
From now on, set
\[ \psi(F) := \psi_f^1(F). \]

Let \( \mathcal{L}_{unip} \) be the **universal unipotent local system**. This is the local system with stalk \( k[[u]] \) at 1 and monodromy given by multiplication by \( 1 + u \). In other words,
\[
\mathcal{L}_{unip} = \lim_{\leftarrow} \mathcal{L}_n,
\]
where \( \mathcal{L}_n \) is our local system from earlier with stalk \( k[u]/(u^n) \) and monodromy multiplication by \( 1 + u \). (Think: “completion of the augmentation ideal” should give the same answer.)

**Idea:**

1. We should think that
\[ \psi(F) = \lim_{\leftarrow} (i^* (j_* (F \otimes \mathcal{L}_n))). \]

2. unipotent \( \xrightarrow{\sim} H^0(D^\times, F) = V^\mu \)
\[ H^1(D^\times, F) = V_\mu \]
How do we recover \( V \)?

We will see in the next lecture that after tensoring with the local system given by a big Jordan block, we can recover \( V \) and its monodromy via taking global sections. This appears to be a basic idea behind Beilinson’s construction.

Hence it makes sense to define
\[
\psi(F) = H^1(D^\times_\epsilon, F \otimes \mathcal{L}_n)
\]
for \( n \) large.
Lecture 18 (March 13, 2020): Nearby cycles, vanishing cycles, and Beilinson glueing on curves

Throughout this lecture, we will work in the following setting. Let $D$ be the disc, $D^\times$ the punctured disc, and

$$D^\times \xrightarrow{j} D \xleftarrow{i} \{0\}$$

the natural inclusions.

Our goal for this lecture is to explain the proof of Beilinson glueing\(^{16}\). We’ll pick up where we left off last week. Let

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

be the standard basis for $\mathfrak{sl}(2, \mathbb{C}) = \mathbb{C} f \oplus \mathbb{C} h \oplus \mathbb{C} e$. Clebsch–Gordan tells us about how the tensor product of two irreducible finite-dimensional $\mathfrak{sl}(2, \mathbb{C})$-modules decomposes:

**Theorem 18.1.** (Clebsch–Gordan) Let $L_n, L_m$ be irreducible finite-dimensional $\mathfrak{sl}(2, \mathbb{C})$-modules of highest weight $n, m$, respectively. Then

$$L_n \otimes L_m = L_{|n-m|} \oplus \cdots \oplus L_{n+m-2} \oplus L_{n+m}.$$ 

A consequence of this theorem is that for $n$ large, there are $m + 1$ summands, so

$$(L_n \otimes L_m)^e = \text{highest weight vectors in above sum} = \mathbb{C}^{m+1} \simeq L_m.$$ 

(Here the superscript denotes Lie algebra invariants; i.e. the kernel of the action

$$e \cdot v \otimes w = ev \otimes w + v \otimes ew$$

of $e$ on $L_n \otimes L_m$.) Moreover, this is more than just an isomorphism of vector spaces: the action of $-e \otimes 1$ on $(L_n \otimes L_m)^e$ aligns with the action of $e$ on $L_m$. Hence (be exponentiating) we have the following corollary to Clebsch–Gordan’s theorem.

**Corollary 18.2.** Let $V$ be a finite-dimensional vector space and $\phi$ a unipotent endomorphism of $V$. Let $J_n$ be a $(n+1)$-dimensional vector space and

$$\phi' = \begin{pmatrix} 1 & 1 \\ & \ddots \\ & & 1 \\ & & & 1 \end{pmatrix}$$

a Jordan block of size $n + 1$. For $n$ large,

$$(V \otimes J_n)^{\phi \otimes \phi'} \simeq V,$$

and this isomorphism is equivariant with respect to the action of $1 \otimes (\phi')^{-1}$ on the LHS and $\phi$ on the RHS.

\(^{16}\)In addition to Beilinson’s original paper [Bei87], the notes [Mor18] of Sophie Morel are an excellent reference for this material.
Hence by tensoring with a Jordan block and taking invariants, we can recover the whole vector space and its monodromy action.

**Remark 18.3.** (Aside for the Lie theorists) Let \( g/\mathbb{C} \) be a semisimple Lie algebra, and \( V \) a finite-dimensional \( g \)-module. For \( \lambda \) sufficiently dominant,

\[
\Delta_\lambda \otimes V \simeq \bigoplus_{\gamma_i \in \Gamma} \Delta_{\lambda + \gamma_i},
\]

where \( \Delta_\mu \) is the Verma module of highest weight \( \mu \) and \( \Gamma \) is the multiset of weights of \( V \). Moreover, there is an isomorphism of \( \mathfrak{n}_+ \)-modules:

\[
(\Delta_\lambda \otimes V)^b \simeq V.
\]

Now we return to the world of perverse sheaves. A perverse sheaf \( \mathcal{M} \in \text{Perv}(D^\times) \) is the same thing as a vector space \( V \) and monodromy endomorphism \( \mu \circ V \). Let \( \mathcal{L}_n \) be the local system with stalk \( k[x]/(x^n) \) and monodromy \( \phi = 1 + x \), as in Lecture 17. In light of Corollary 18.2 and the third bullet point in Example 17.6, for \( n \) large enough, we could define a functor \( \psi \) by

\[
\psi(\mathcal{M}) = H^0(j_*(\mathcal{M} \otimes \mathcal{L}_n)) = (V \otimes J_{n-1})^{\mu \otimes \phi} = V.
\]

This will end up being our definition which allows us to see certain features in the arguments below. The key lemma of today’s lecture tells us that this definition stabilizes for large \( n \).

**Lemma 18.4.** Let \( \mathcal{M} \in \text{Perv}(D^\times) \). For a fixed \( m \), the kernel and cokernel of

\[
\begin{array}{ccc}
\mathcal{L}_n & \xrightarrow{x^m} & \mathcal{L}_n \\
\downarrow j_i & & \downarrow j_* \\
\mathcal{M} \otimes \mathcal{L}_n & & \mathcal{M} \otimes \mathcal{L}_n
\end{array}
\]

stabilize for large \( n \), and are canonically isomorphic.

**Proof.** We will prove the lemma when \( \mathcal{M} \) has rank 1 (i.e. \( \mathcal{M} \) corresponds to the vector space \( k \) with monodromy given by multiplication by \( \lambda \in k^\times \).)

**Case 1:** monodromy \( \lambda \neq 1 \). Then

\[
\begin{align*}
j_i(\mathcal{M} \otimes \mathcal{L}_n) & = j_*(\mathcal{M} \otimes \mathcal{L}_n).
\end{align*}
\]

(See Example 17.8.) The theorem follows in this case because the kernel and cokernel of \( \mathcal{L}_n \overset{x^m}{\longrightarrow} \mathcal{L}_n \) stabilize for \( m \) fixed, \( n \) large and \( j_i, j_* \) are exact.

**Case 2:** monodromy \( \lambda = 1 \); i.e. \( \mathcal{M} = k_{D^\times}[1] \) is the trivial local system. We will illustrate what is happening in this case through an example. Let \( m = 2 \) and \( n = 3 \). We can see what
the maps $\mathcal{L}_3 \xrightarrow{x^2} \mathcal{L}_3$, $j_! \mathcal{L}_3 \xrightarrow{x^2} j_! \mathcal{L}_3$ and $j_! \mathcal{L}_3 \xrightarrow{x^2} j_* \mathcal{L}_3$ are doing on egg diagrams:

As $n$ gets larger, the eggs in the illustration above get longer and the image of $j_*$ gets bigger, but the kernel and cokernel stay the same size.

**Remark 18.5.** What Beilinson actually proves is that

$$\lim_{\leftrightarrow} j_!(\mathcal{M} \otimes \mathcal{L}_n) \simeq \lim_{\leftrightarrow} j_* (\mathcal{M} \otimes \mathcal{L}_n),$$

where ‘$\lim_{\leftrightarrow}$’ is appropriately defined. We’ll sum this up with the slogan “middles agree.” We already saw this happening above, and will see it happening again in our next example.

**Example 18.6.** Here is a 2-dimensional example. Let

$$\mathbb{C}^2 \xrightarrow{xy} \mathbb{C},$$

and consider $\text{Perv}_\Lambda(\mathbb{C}^2)$, where $\Lambda$ is the stratification via coordinate hyperplanes and their
complement $U$.

Let $\mathcal{M} = k_U[2]$, and denote by $IC_1 = IC_{\{y=0\}}$, $IC_2 = IC_{\{x=0\}}$, and $IC_0 = IC_{\{x=y=0\}}$. The composition series of $j_! k_U[2]$ is given by the following egg:

\[
\begin{array}{c}
\text{j}_! k_U[2] = \\
\downarrow \\
IC_X \\
\uparrow \\
IC_0 \\
\end{array}
\]

Then the key Lemma can be seen on egg diagrams:

**Definition 18.7.** (Beilinson) Let $X \xrightarrow{f} D$, $U = f^{-1}(D^\times)$, and $Z = f^{-1}(0)$. For a perverse sheaf $\mathcal{M} \in \text{Perv}(U)$ and $n$ large, define functors $\psi_f, \Xi_f : \text{Perv}(U) \to \text{Perv}(X)$ by

- $\psi_f(\mathcal{M}) = \ker(x^0) \cong \text{coker}(x^0)$ “unipotent nearby cycles”

144
• $\Xi_f(\mathcal{M}) = \ker(x^1) \simeq \text{coker}(x^1)$ “maximal extension”

The perverse sheaf $\psi_f(\mathcal{M})$ is supported on $Z$ and $\Xi_f(\mathcal{M})$ is supported everywhere.

**Example 18.8.** Let $\mathcal{M} = k_U[1]$, then we can see the images of these functors in eggs:

![Diagram showing examples of functors in eggs]

**Example 18.9.** In our 2-dimensional example, Example 18.6 we have:

![Diagram showing examples of functors in eggs]

**Lemma 18.10.** The functors $\psi_f$ and $\Xi_f$ are exact, and we have functorial short exact sequences

1. $j! \hookrightarrow \Xi_f \twoheadrightarrow \psi_f$
2. $\psi_f \hookrightarrow \Xi_f \twoheadrightarrow j^*$

Moreover, the canonical map $\psi_f \to \Xi_f \to \psi_f$

agrees with monodromy $-1$.

**Proof.** See Geordie’s handwritten notes on the course website.

**Definition 18.11.** Let $\mathcal{M} \in \text{Perv}(D)$. The unipotent vanishing cycles functor is defined by

$$\phi_f(\mathcal{M}) = H^0 \left( \begin{array}{c} \Xi_f(\mathcal{M}_U) \\ \oplus \\ j_!(\mathcal{M}_U) \\ \oplus \\ j^*(\mathcal{M}_U) \\ -1 \\ \mathcal{M} \end{array} \right)$$
All maps in the diagram above are the canonical ones.

**Remark 18.12.** 1. The map $j_! \to \Xi_f$ is injective, and the map $\Xi_f \to j_*$ is surjective, so the cocomplex above only has cohomology in degree 0, and hence $\phi_f$ is an exact functor on $\emph{Perv}(D)$.

2. $x$ induces a monodromy endomorphism of $\Xi_f, \psi_f, \phi_f$.

**Example 18.13.** Let $X = D$ and $\mathcal{M} = j_! k_D[1]$. To compute $\phi_f(\mathcal{M})$, we need to compute the zeroeth cohomology.

![Diagram]

The image of the first map is

![Image of the first map]

The kernel of the second map is

![Image of the kernel]

146
Notice that because of the sign in the second map, the image will always be contained in the kernel. Hence $\phi_f(M)$ is equal to

$$H^0(\mathcal{N}) \cong \frac{\ker}{\im} = IC_0.$$

**Example 18.14.** If $\mathcal{M} = k_D[1]$, then using the same method as above, we compute

$$\phi_f(M) = H^0 \left( \begin{array}{c}
\frac{IC_0}{IC_0} \\
\frac{IC_0}{IC_0} \\
\frac{IC_0}{IC_0} \\
\frac{IC_0}{IC_0}
\end{array} \right).$$

Here, the kernel and image are equal:

$$\ker = \im = \left( \begin{array}{c}
\frac{IC_0}{IC_0} \\
\frac{IC_0}{IC_0} \\
\frac{IC_0}{IC_0} \\
\frac{IC_0}{IC_0}
\end{array} \right).$$

Notice that the extra piece of the kernel in the previous example is now a subsheaf of the image:

$$\left( \begin{array}{c}
\frac{IC_0}{IC_0} \\
\frac{IC_0}{IC_0} \\
\frac{IC_0}{IC_0} \\
\frac{IC_0}{IC_0}
\end{array} , 0 \right) \subset \im.$$

Hence $\phi_f(M) = 0$.

**Exercise 18.15.** Show that

$$\phi_f(\Xi_f(k_D[1])) = IC_0^\oplus 2,$$

and show that the monodromy endomorphism is not trivial.
Example 18.16. Let \( \mathcal{M} = IC_X \), for \( X = \mathbb{C}^2 \), and \( \mathbb{C}^2 \xrightarrow{f_{xy}} \mathbb{C} \) as earlier. Then

\[
\phi_f(\mathcal{M}) = H^0
\]

\[
\mathcal{I}_x \xrightarrow{\mathcal{I}_x \otimes \mathcal{I}_x} \mathcal{I}_x \xrightarrow{\mathcal{I}_x \otimes \mathcal{I}_x} \mathcal{I}_x
\]

18.1 Glueing

With this machinery, Beilinson shows us how we can glue perverse sheaves. To state the theorem we return to a slightly more general setting.

\[
\begin{array}{ccc}
Z & \xleftarrow{i} & X & \xrightarrow{j} & U \\
\downarrow & & \downarrow f & & \downarrow \\
\{0\} & \xleftarrow{\rightarrow} & D & \xrightarrow{\rightarrow} & D^x
\end{array}
\]

Theorem 18.17. (Beilinson)

\[
Perv(X) \simeq \left\{ \begin{array}{c}
\mathcal{M}_U \in Perv(U), \\
\mathcal{M}_Z \in Perv(Z)
\end{array} \right\}
\]

\[
\psi_f(\mathcal{M}_U) \xrightarrow{\text{monodromy} \cdot -1} \psi_f(\mathcal{M}_U)
\]

“pieces” \quad “glue”

Remark 18.18. Beilinson’s theorem glues perverse sheaves on an open set to perverse sheaves on a closed set. Glueing perverse sheaves on two open sets is much easier because perverse sheaves form a stack.

Example 18.19. Returning to our setting of \( X = D = D^x \sqcup \{0\} \), a perverse sheaf on \( D^x \) (resp. \( \{0\} \)) is the same thing as a vector space with automorphism \( \mu \circ V \) (resp. a vector space \( W \)). Hence

\[
Perv_{\text{constructible}}(D) = \left\{ \begin{array}{c}
V \circ \mu \text{ invertible}, \\
W \text{ vector space}
\end{array} \right\}
\]

\[
f \xrightarrow{\mu - \text{id}} g \xrightarrow{} V
\]

\[
W
\]

148
Let us explain why Beilinson glueing holds. We start with a general definition. Let $\mathcal{A}$ be an abelian category. A **diad** in $\mathcal{A}$ is

$$
Q := C_- \xrightarrow{\beta_-} B \xleftarrow{\alpha_-} A \xrightarrow{\alpha_+} C_+
$$

These form a category $\text{Diads}(\mathcal{A})$ in an obvious way.

Given a diad, we can associate a complex

$$
Q' = C_- \xrightarrow{(\alpha_- - \beta_-)} A \oplus B \xleftarrow{(\alpha_+ - \beta_+)} C_+,
$$

and another diad

$$
r(Q) := \ker \alpha_+ \xrightarrow{\text{coker } \alpha_-} H^0(Q)
$$

**Lemma 18.20.** $r^2 = id$

**Proof.** We will take this lemma as a black box. \hfill \square

Given this,

$$
\Xi_f(\mathcal{M}) \\
\simeq \text{diads of the form } j_! \mathcal{M} \oplus j_* \mathcal{M} \\
\mathcal{M} \\
\Xi_f(\mathcal{M}) \\
\simeq \text{diads of the form } \psi_f(\mathcal{M}) \oplus \psi_f(\mathcal{M}) \\
\phi_f(\mathcal{M}) \\
\simeq \text{pairs } \left(\mathcal{M}_U, \psi_f(\mathcal{M}) \to \phi_f(\mathcal{M}) \to \psi_f(\mathcal{M}) \mid \psi_f(\mathcal{M}) \xrightarrow{\text{monodromy}^{-1}} \psi_f(\mathcal{M})\right)
$$

The second equality is obtained via applying our equivalence $r$ on diads.
19 Lecture 19 (March 27, 2020): Overview of proof that the derived category of perverse sheaves agrees with constructible derived category

Recall the setting of the last lecture: Let $X/\mathbb{C}$ be a variety with the metric topology and $P_X := \text{Perv}(X, k)$. Beilinson described for us how to glue perverse sheaves on $X$. More specifically, we have the following set-up:

$$
\begin{array}{ccc}
Z & \xrightarrow{i} & X \\
\downarrow & & \downarrow j \\
\{0\} & \xleftarrow{i^!} & \mathbb{A}^1 \xleftarrow{i^!} \mathbb{A}^1 \setminus \{0\}
\end{array}
$$

We can move between the bounded derived categories of constructible sheaves on $X$, $Z$, and $U$ by pushing and pulling:

$$
D^b_c(Z) \xrightarrow{i^*} D^b_c(X) \xrightarrow{j^*} D^b_c(U)
$$

The functors $i^* = i^!$, $j^* = j^!$ preserve perverse sheaves, and if $j$ is affine, then $j^*, j^!$ are exact and also preserve perverse sheaves. However, $i^*$, $i^!$ do not!

Last lecture, we constructed two other exact functors

$$
x \odot \psi_f : P_U \to P_Z \ "\text{unipotent nearby cycles}" \\
x \odot \Xi_f : P_U \to P_X \ "\text{maximal extension}"
$$

which each have a “monodromy” $x$. These functors fit into short exact sequences

$$
0 \to j_!\mathcal{M} \xrightarrow{j^*} \Xi_f \mathcal{M} \xrightarrow{\psi_f} \mathcal{M} \to 0 \\
0 \to \psi_f \mathcal{M} \xrightarrow{\Xi_f} j_* \mathcal{M} \to 0
$$

for any $\mathcal{M} \in P_U$. We then used $\psi_f$ and $\Xi_f$ to construct another exact functor

$$
x \odot \phi_f : P_X \to P_Z \ "\text{unipotent vanishing cycles}" \\
$$

which we should think about as the “stalk of a perverse sheaf along $Z$.” It was defined as

$$
\phi_f \mathcal{M} = H^0 \left( \begin{array}{c}
\Xi_f \mathcal{M}_U \\
\oplus \\
\mathcal{M}
\end{array} \right)
$$
for $M \in P_X$.

**Easy (and useful) fact:** For $M \in P_Z$,

$$\phi_f(i_*M) \simeq M.$$

The main result of last lecture was **Beilinson gluing**, which gave an equivalence of categories:

$$
P_X \simeq \left\{ \begin{array}{c}
M \in P_U \\
N \in P_Z
\end{array} \right\} \xrightarrow{\psi_fM} \left\{ \begin{array}{c}
\psi_fM \\
N
\end{array} \right\} \xrightarrow{1-\mu} \left\{ \begin{array}{c}
\psi_fM \\
N
\end{array} \right\}
$$

$$
\mathcal{F} \mapsto \left\{ \begin{array}{c}
\mathcal{F}_U \in P_U \\
\phi_f\mathcal{F} \in P_Z
\end{array} \right\} \xrightarrow{\psi_f\mathcal{F}_U} \left\{ \begin{array}{c}
\psi_f\mathcal{F}_U \\
\phi_f\mathcal{F}
\end{array} \right\}
$$

The goal of today’s lecture is to use these tools to prove the following theorem.

**Theorem 19.1.** $D^b(P_X) \simeq D^b_c(X)$.

This result is a beautiful example of a bigger philosophy. Often we have a triangulated category we wish to understand, and within it a collection of well-behaved objects which we understand better than the rest. Then we might hope to reconstruct the entire triangulated category from our special collection of objects. In many situations we cannot, but this is an example where we can. In the poetry of Beilinson, “the niche $D$ where $P_X$ dwells may be recovered from $P_X$.”

**Recall:** Let $\Lambda$ be a stratification of $X$. Associated to this stratification is the category $\text{Perv}_\Lambda(X)$ of $\Lambda$-constructible perverse sheaves on $X$. Our category $P_X$ is the limit of such categories:

$$P_X = \text{Perv}(X) = \lim_{\Lambda} \text{Perv}_\Lambda(X).$$

**Remark 19.2.** If $\Lambda$ is a fixed stratification, usually

$$D^b(\text{Perv}_\Lambda(X)) \neq D^b_c(X).$$

**Example 19.3.** Let $X = \mathbb{P}^1\mathbb{C}$ with the trivial stratification $\Lambda$. Then

$$\text{Perv}_\Lambda(X) = \text{local systems on } X \simeq \text{Vect}_{f.d.}^k.$$  

However,

$$D^b(\text{Vect}_{f.d.}^k) \neq D^b_c(X)$$

because $\text{Ext}^i(k_X, k_X) = H^i(X) \neq 0$ for $i = 2$, but the category $\text{Vect}_{f.d.}^k$ is semisimple, so there are no higher exts.
We see in this example that differences in Ext groups prevented us from obtaining our desired derived equivalence. This illustrates a more general phenomenon which we will examine now.

**Definition 19.4.** A nice, path connected space $X$ with base point $x \in X$ is $K(\pi, 1)$ if

1. $\pi_i(X) = 1$ for $i > 1$, and
2. $\pi_1(X) = \pi$.

Equivalently, $X$ is $K(\pi, 1)$ if its universal cover is contractible.

**Exercise 19.5.** Show (easier) that $$\text{Rep}_{f.d.} k\pi \xrightarrow{\sim} k\text{-local systems on } X \quad V \leftrightarrow \mathcal{L}_V$$

and (harder) that $$\text{Ext}^i(V, V') \cong \text{Ext}^i(\mathcal{L}_V, \mathcal{L}_{V'}).$$

**Lemma 19.6.** Let $F : D_1 \to D_2$ be a triangulated functor of triangulated categories. Assume that $D_1, D_2$ have $t$-structures with hearts $C_1, C_2$, respectively, such that $F : C_1 \xrightarrow{\sim} C_2$ is an equivalence, and $D_i = \langle C_i \rangle_\Delta$ for $i = 1, 2$ (i.e. the $t$-structures giving $C_i$ are nondegenerate). Then the following are equivalent.

(a) $F$ is an equivalence.

(b) For any objects $M, N \in C_1$, $F : \text{Hom}^i_{D_1}(M, N) \xrightarrow{\sim} \text{Hom}^i_{D_2}(F(M), F(N))$. In other words, the “Exts agree”.

(c) (Won’t be used) Assume that $D_1 = D^b(C_1)$. For any $x \in \text{Hom}^i_{D_2}(F(M), F(N))$, there exists an injection $N \hookrightarrow N'$ such that $x$ is zero in $\text{Hom}^i_{D_2}(F(M), F(N'))$; i.e. under the natural map $$\text{Hom}^i_{D_2}(F(M), F(N)) \to \text{Hom}^i_{D_2}(F(M), F(N'))$$

$$x \mapsto 0.$$  

This condition is called “effaceability.”

**Proof.** (a) $\implies$ (b) is immediate.

(b) $\implies$ (a) can be shown by induction and the long exact sequence. \qed

**Example 19.7.** Let $X$ be $K(\pi, 1)$. Then

$$D^b(\text{Rep}_{f.d.} k\pi) \xrightarrow{\sim} D^b_A(X).$$

Example [19.3] illustrated that this is not necessarily the case when $X$ is not $K(\pi, 1)$. 

152
19.1 Yoneda extensions

To understand part (c) of Lemma 19.6, we need some facts about Yoneda extensions. Let $\mathcal{A}$ be an abelian category. For objects $M, N$ in $\mathcal{A}$, define a category $E^i(M, N)$ with

- objects: acyclic complexes
  $$N \to C^1 \to C^2 \to \cdots \to C^i \to M$$

- morphisms: chain complex maps of the form
  $$\begin{array}{cccccc}
  N & \to & C^1 & \to & C^2 & \to & \cdots & \to & C^i & \to & M \\
  \downarrow & id & \downarrow & & \downarrow & & \cdots & & \downarrow & id & \\
  N & \to & \widetilde{C}^1 & \to & \widetilde{C}^2 & \to & \cdots & \to & \widetilde{C}^i & \to & M
  \end{array}$$

Lemma 19.8. (Definition)

$$\text{Ext}^i(M, N) = \text{connected components of } E^i(M, N)$$

$$0 \leftrightarrow \text{split complexes in } E^i(M, N)$$

Remark 19.9. In Lemma 19.8, two extensions are in the same “connected component” if one can pass from one to the other going along arrows in our categories in either direction. More formally, we can build a space with 0 (resp. 1) simplices given by objects (resp. arrows) in $E^i(M, N)$; then connected component takes on its topological meaning. One can show two objects

$$N \to C^1 \to C^2 \to \cdots \to C^i \to M$$

and

$$N \to \widetilde{C}^1 \to \widetilde{C}^2 \to \cdots \to \widetilde{C}^i \to M$$

in $E^i(M, N)$ are in the same connected component if there exists a commutative diagram

$$\begin{array}{cccccc}
  N & \to & C^1 & \to & C^2 & \to & \cdots & \to & C^i & \to & M \\
  \downarrow & id & \downarrow & & \downarrow & & \cdots & & \downarrow & id & \\
  N & \to & D^1 & \to & D^2 & \to & \cdots & \to & D^i & \to & M \\
  \downarrow & id & \downarrow & & \downarrow & & \cdots & & \downarrow & id & \\
  N & \to & \widetilde{C}^1 & \to & \widetilde{C}^2 & \to & \cdots & \to & \widetilde{C}^i & \to & M
  \end{array}$$

with

$$N \to D^1 \to D^2 \to \cdots \to D^i \to M$$

also in $E^i(M, N)$.

Exercise 19.10. Show directly that with $\text{Ext}^i$ defined as in Lemma 19.8

$$\text{Ext}^i(M, N) = \text{Hom}^i_{D(\mathcal{A})}(M, N).$$

Make no assumptions on $\mathcal{A}$. 153
What about functoriality? In our usual definition of Ext^i in the derived category, it is obvious that Ext^i is a functor. With this new definition, it is not so obvious. In other words, given N \rightarrow N', how to we obtain a morphism Ext^i(M, N) \rightarrow Ext^i(M, N')? Here is how:

- Given with N \rightarrow N' and an element of Ext^i(M, N) represented by the complex

  \[
  N \rightarrow C^1 \rightarrow C^2 \rightarrow \cdots \rightarrow C^i \rightarrow M,
  \]

  we obtain a complex representing an element of Ext^i(M, N') by forming the push-out

  \[
  \begin{array}{ccc}
  N & \rightarrow & C^1 \\
  \downarrow & & \downarrow \\
  N' & \rightarrow & P
  \end{array}
  \quad \quad
  \begin{array}{ccc}
  & \rightarrow & C^2 \\
  & \rightarrow & \vdots \\
  & \rightarrow & C^i \\
  & \rightarrow & M
  \end{array}
  \]

  Here P = (C^1 \oplus N')/N. This gives a morphism Ext^i(M, N) \rightarrow Ext^i(M, N').

- Similarly, for M \rightarrow M', we can use the pull-back to form a morphism Ext^i(M, N) \rightarrow Ext^i(M', N).

An important consequence of this is the following. If \( x \in \text{Ext}^i(M, N) \) is represented by the complex

\[
N \xrightarrow{f} C^1 \rightarrow C^2 \rightarrow \cdots \rightarrow C^i \rightarrow M,
\]

then applying the construction above to the morphism \( f : N \rightarrow C^1 \), we obtain

\[
\begin{array}{ccc}
N & \rightarrow & C^1 \\
\downarrow & & \downarrow \\
C^1 & \rightarrow & (C^1 \oplus C^1)/N \\
\downarrow & & \downarrow \\
(\)C^1 & \rightarrow & \cdots \\
\rightarrow & \rightarrow & C^i \\
\rightarrow & \rightarrow & M
\end{array}
\]

But since \((C^1 \oplus C^1)/N = C^1 \oplus (C^1/N)\), the lower sequence splits, and hence represents zero in \text{Ext}^i(M, C^1). In other words,

\[
\text{Ext}^i(M, N) \xrightarrow{\text{Ext}^i(f, N)} \text{Ext}^i(M, C^1) \xrightarrow{x \mapsto 0}.
\]

This is the origin of effaceability.

**Exercise 19.11.** Prove (ii) \( \Rightarrow \) (iii) and (iii) \( \Rightarrow \) (ii) in Lemma 19.6. (Hint: See Geordie’s hand-written notes if you are stuck.)

A key ingredient in Beilinson’s theorem is:

**Theorem 19.12.** Let \( X/\mathbb{C} \) be a smooth variety. Then there exists a Zariski open set \( U \subset X \) which is \( K(\pi, 1) \).

This theorem explains philosophically why Beilinson’s theorem is true: for perverse sheaves, we can always refine our stratification to include this \( K(\pi, 1) \) open set. We will see this more precisely when we discuss the proof of Beilinson’s theorem.
Example 19.13. Any curve becomes $K(\pi, 1)$ after deleting a point!

(Here the arrows indicate homotopy equivalences and the $x$’s are missing points.)

We will roughly explain the proof of Theorem 19.12. There are two main ingredients:

1. “Noether normalization,” (NN): If $Z \subset \mathbb{A}^n$ is of dimension $d$, then a generic projection $\mathbb{A}^n \to \mathbb{A}^d$ is finite when restricted to $Z$. Here’s a caricature:

2. “Extensions of $K(\pi, 1)$ are $K(\pi, 1)$,” ($EK(\pi, 1)$): If

$$
\begin{array}{ccc}
F & \longrightarrow & E \\
\downarrow & & \downarrow \\
B & & \\
\end{array}
$$

is a fibre bundle, then if $B$ is $K(\pi, 1)$, $E$ is connectd, and either $F$ is discrete or $K(\pi, 1)$, then $E$ is $K(\pi, 1)$. (Follows from the long exact sequence of homotopy groups.)

With these tools in our toolbox, the proof proceeds as follows.

Step 1: Reduction to $X \subset \mathbb{A}^1$, Zariski standard open\footnote{“Zariski standard open” means that $X$ is of the form $D(f) = \{z \in X \mid f(z) \neq 0\}$ for some regular function $f$.}. Without loss of generality, we may assume that $X$ is affine. By (NN), we can find a finite map $f : X \to \mathbb{A}^d$. Over a standard
open $U' \subset \mathbb{A}^d$, this map is étale. Hence we have a fibration

$$\begin{array}{c}
\text{finite} \\
\downarrow
\end{array} \begin{array}{c}
U \\
\downarrow
\end{array} \begin{array}{c}
U'
\end{array}$$

so by $(E^{K}(\pi, 1))$, if $U'$ is $K(\pi, 1)$, then $U$ is $K(\pi, 1)$.

**Step 2:** Induction on dimension. By $(\text{NN})$, there exists a projection $f : \mathbb{A}^n \to \mathbb{A}^{n-1}$ such that on the hypersurface $Z = X \setminus U$, $f$ is finite with fibres consisting of $m$ points:

$$\begin{array}{c}
U \hookrightarrow \mathbb{A}^n \\
\downarrow f
\end{array} \begin{array}{c}
\mathbb{A}^{n-1} \\
\downarrow f
\end{array} \begin{array}{c}
\{m \text{ points}\}
\end{array}$$

Over an open $V \subset \mathbb{A}^{n-1}$, this map will be étale, hence

$$\begin{array}{c}
U' \hookrightarrow U \\
\downarrow
\end{array} \begin{array}{c}
V' \hookrightarrow V
\end{array}$$

is fibred in $\mathbb{C} \setminus \{m \text{ points}\}$. By induction, we can shrink $V$ to $V'$ such that $V'$ is $K(\pi, 1)$. Hence $U'$ is $K(\pi, 1)$ too by $(E^{K}(\pi, 1))$. \qed

The goal for the rest of the lecture is to prove Beilinson’s theorem for curves; that is, for a curve $X$, we wish to show that

$$D^b(P_X) \simeq D^b_c(X).$$

To start, we have the following fact [BBDG18, Bei87]. There exists a triangulated functor

$$\text{real} : D^b(P_X) \to D^b_c(X)$$

called the “realization functor” which is the identity on $P_X$. (This holds for general $X$, not just curves.) We will show that real is an equivalence of categories.

By Lemma 19.6, it is enough to show that for $M, N \in P_X$,

$$\text{Hom}_{D^b(P_X)}^j(M, N) \simeq \text{Hom}_{D^b_c(X)}^j(M, N).$$

Moreover, because $P_X$ is finite length, we can use the long exact sequence in Ext to reduce to the case where $M, N$ are irreducible objects.

Recall that in lecture 17 we classified irreducible perverse sheaves on curves. There were two types: (1) skyscrapers, and (2) $IC$ sheaves supported everywhere.

**Step 1:** Let $M, N$ be skyscrapers: $M = i_*k_x$, $N = i'_*k_y$. Then in $D^b_c(X)$,

$$\text{Hom}^j(i_*k_x, i'_*k_y) = \text{Hom}^j(k_x, i'i'_*k_y)$$

$$= \begin{cases} k & \text{if } x = y, j = 0, \\ 0 & \text{otherwise}. \end{cases}$$
Showing that
\[ \text{Hom}_{D^b(P_X)}(k_x, k_y) = 0 \]
if \( x \neq y \) is easier, and left as an exercise. The trickier case is show that \( \text{Ext}^i_{P_X}(k_x, k_x) = 0 \) for \( i > 0 \). To do this, we will use the quiver description of \( P_X \) and Yoneda Exts. Recall that
\[ P_X \simeq \left\{ V_1 \xrightarrow{c} V_0 \ \middle| \ c \circ v + \text{id invertible} \right\}. \]
Then an element of \( \text{Ext}^1(k_x, k_y) \) has a representative of the form
\[ k_k \to F \to k_x. \]
In quiver language, such an extension is a complex
\[ k \to V_0 \to k. \]
But any such complex fits into a diagram
\[
\begin{array}{cccc}
0 & \longrightarrow & V_1 & \longrightarrow & 0 \\
\downarrow & & \downarrow \circ c & & \downarrow \\
k & \longrightarrow & V_0 & \longrightarrow & k
\end{array}
\]
The top sequence is exact, so \( V_1 = 0 \). But the bottom sequence is also exact, so \( V_1 = 0 \) implies that the bottom sequence must split. Hence our original element is zero in \( \text{Ext}^1(k_x, k_y) \), so \( \text{Ext}^1(k_x, k_y) = 0 \).

Showing that \( \text{Ext}^2(k_x, k_y) = 0 \) is more challenging. An element of \( \text{Ext}^2(k_x, k_y) \) has a representative of the form
\[ k \to V_0^1 \to V_0^2 \to k. \]
This fits into a diagram
\[
\begin{array}{cccc}
0 & \longrightarrow & V_1^1 & \longrightarrow & V_1^2 & \longrightarrow & V_1^1 & \longrightarrow & 0 \\
& & \downarrow v^1 & & \downarrow c^1 & & \downarrow c^2 & & \downarrow v^2 & & \downarrow v^1 & & \downarrow c^1 & & \downarrow c^2 & & \downarrow v^2 & \longrightarrow & 0 \\
k & \longrightarrow & V_0^1 & \longrightarrow & V_0^2 & \longrightarrow & V_0^1 & \longrightarrow & k
\end{array}
\]
We want to show that we can reduce this to an Ext supported at \( x \). But the basic issue is that there is nothing telling us that the middle terms must be supported on a point. In sheaf language, this is equivalent to the fact that the existence of a sequence
\[ i_* k_x \to \mathcal{F} \to \mathcal{G} \to i_* k_x \]
whose first and last terms are supported on a point does not imply that the middle terms \( \mathcal{F}, \mathcal{G} \) are.

There are two ways we can get around this. First, the “stupid way.” We can assume that \( c \circ v \) is nilpotent (exercise!), then we have a natural map
\[
\begin{array}{cccc}
0 & \longrightarrow & V_1^1 & \longrightarrow & V_1^2 & \longrightarrow & 0 & \longrightarrow & \text{Im} v^1 & \longrightarrow & \text{Im} v^2 & \longrightarrow & 0 \\
& & \downarrow v^1 & & \downarrow c^1 & & \downarrow c^2 & & \downarrow v^2 & & \downarrow c^1 & & \downarrow c^2 & & \downarrow v^2 & \longrightarrow & 0 \\
k & \longrightarrow & V_0^1 & \longrightarrow & V_0^2 & \longrightarrow & k & \longrightarrow & V_0^1 & \longrightarrow & V_0^2 & \longrightarrow & k
\end{array}
\]
Continuing this process, we have a map

\[
\begin{array}{ccccccccc}
0 & \rightarrow & \operatorname{Im} v^1 & \rightarrow & \operatorname{Im} v^2 & \rightarrow & 0 \\
\downarrow & & \downarrow v^1 & & \downarrow v^2 & & \downarrow & & 0 \\
k & \rightarrow & V^1_0 & \rightarrow & V^2_0 & \rightarrow & k \\
\downarrow & & \downarrow v^1 & & \downarrow v^2 & & \downarrow & & \downarrow & & \downarrow \\
k & \rightarrow & \operatorname{Im} c^1 & \rightarrow & \operatorname{Im} c^2 & \rightarrow & k \\
\end{array}
\]

Continuing in this way, we eventually obtain a top sequence of zeros, which lets us conclude that our lower sequence splits. This procedure works for all higher Ext-s.

Alternatively, we could use Beilinson’s approach using vanishing cycles, which works in greater generality (and in fact provides the skeleton of his argument in the general case). Choose a map \( f : X \rightarrow \mathbb{C} \) with zero set \( x \in X \). Let \( C \) be the complex

\[
i_* k_x \rightarrow \mathcal{F}^1 \rightarrow \cdots \rightarrow \mathcal{F}^j \rightarrow i_* k_x
\]

representing an element in \( \operatorname{Ext}^j(i_* k_x, i_* k_x) \). Then Beilinson showed that

\[
C' \simeq \phi_f(C'), \tag{19.1}
\]

where \( \phi_f : P_X \rightarrow P_{(x)} \) is the vanishing cycles functor defined in Lecture 18. The complex \( \phi_f(C') \) is supported on \( x \), so this proves that \( C' = 0 \in \operatorname{Ext}^j(i_* k_x, i_* k_x) \). To prove (19.1), we can use the exact sequences from Lecture 18:

\[
C' \rightarrow C' \oplus \Xi_f(C') \rightarrow (C' \oplus_f (C'))/j!(C') \rightarrow \phi_f(C')
\]

**Step 2:** Let \( M \) be irreducible with full support and \( N \) a skyscraper supported at \( \{x\} \). Let \( j : U = X \setminus \{x\} \hookrightarrow X \).

Recall that because the immersion \( j \) is affine, \( j_! \) and \( j_* \) are exact, preserve perverse sheaves, and fit into adjoint pairs \((j^*, j_*), (j_!, j^!)\). The adjunction maps give an exact sequence

\[
K \hookrightarrow j_! M_U \rightarrow M,
\]

where \( K \) is a perverse sheaf supported on \( \{x\} \). The corresponding long exact sequence gives the diagram

\[
\cdots \rightarrow \operatorname{Hom}^i_{P_X}(M, N) \rightarrow \operatorname{Hom}^i_{P_X}(j_! M_U, N) \rightarrow \operatorname{Hom}^i_{P_X}(K, N) \rightarrow \cdots
\]

\[
\cdots \rightarrow \operatorname{Hom}^i_{D^b(X)}(M, N) \rightarrow \operatorname{Hom}^i_{D^b(X)}(j_! M_U, N) \rightarrow \operatorname{Hom}^i_{D^b(X)}(K, N) \rightarrow \cdots
\]

Using the adjunctions, we have

\[
\operatorname{Hom}^i_{P_X}(j_! M_U, N) = \operatorname{Hom}^i_{P_U}(M_U, N_U) = 0
\]
because \( N_U = 0 \). Similarly, \( \text{Hom}^i_{\mathbb{D}^b(X)}(j_!M_U, N) = 0 \), so the middle vertical arrow is an isomorphism \( 0 \simeq 0 \). The right vertical arrow is an isomorphism by Step 1. Hence we conclude by induction that all other vertical arrows must also be isomorphisms.

**Step 3:** Let \( M \) and \( N \) be irreducible objects in \( P_X \) with full support. Then by Lemma \[9.12\] we can choose \( U \subset X \) such that \( M_U, N_U \) are (shifts of) local systems and \( U \) is \( K(\pi, 1) \). Note that the inclusion \( j : U \hookrightarrow X \) is still affine. Because \( N \) is irreducible, we have a short exact sequence

\[ N \hookrightarrow j_*j^*N = j_*N_U \twoheadrightarrow k. \]

Then by the long exact sequence in \( \text{Hom} \), we have the diagram

\[
\begin{array}{cccccc}
\cdots & \rightarrow & \text{Hom}^i_{P_X}(M, N) & \rightarrow & \text{Hom}^i_{P_X}(M, j_*N_U) & \rightarrow & \text{Hom}^i_{P_X}(M, k) & \rightarrow & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \rightarrow & \text{Hom}^i_{\mathbb{D}^b(X)}(M, N) & \rightarrow & \text{Hom}^i_{\mathbb{D}^b(X)}(M, j_*N_U) & \rightarrow & \text{Hom}^i_{\mathbb{D}^b(X)}(M, k) & \rightarrow & \cdots
\end{array}
\]

By adjunction, we have

\[ \text{Hom}^i_{P_X}(M, j_*N_U) = \text{Hom}^i(M_U, N_U). \]

Hence the middle vertical arrow is an isomorphism because \( U \) is \( K(\pi, 1) \). The right vertical arrow is an isomorphism by Step 2, and hence the left vertical arrow must also be an isomorphism. \( \Box \)

**The Moral:** If we fix a stratification, there can be complicated structure going on in \( D^b(P_X) \) which doesn’t only come from fundamental groups. However, if we’re allowed to refine our stratification as much as we want, then we can choose open strata which are \( K(\pi, 1) \), and all information in the category comes from local systems.
Recall the setting of the last few lectures: Fix $k$ to be our field of coefficients, and let $X$ be an algebraic variety over $\mathbb{C}$, with stratification

$$X = \bigsqcup_{\lambda \in \Lambda} X_\lambda.$$ 

The abelian category of $\Lambda$-constructible perverse sheaves, $\text{Perv}_\Lambda(X)$, is a subcategory of the triangulated category $D^b_\Lambda(X)$, the derived category of $\Lambda$-constructible sheaves. Moreover, there is a realization functor

$\text{real} : D^b(\text{Perv}_\Lambda(X)) \to D^b_\Lambda(X).$

Last week we saw that for a fixed stratification, $\text{real}$ is rarely an equivalence; however, if we are allowed to refine stratifications, we have Beilinson’s theorem:

**Theorem 20.1.** (Beilinson) $D^b(\text{Perv}(X)) \simeq D^b(X)$.

Today, we will show that if each strata $X_\lambda$ is an affine space, then we have such an equivalence for a fixed stratification.

**Theorem 20.2.** (Beilinson–Ginzburg–Soergel) If $\Lambda$ is a stratification of $X$ such that $X_\lambda$ is affine, then $D^b(\text{Perv}_\Lambda(X)) \simeq D^b_\Lambda(X)$.

**Remark 20.3.** Last week we saw that the failure of the strata to be $K(\pi,1)$ was the obstruction to $\text{real}$ being an equivalence. Affine spaces are contractible, so this obstruction disappears.$^{18}$

**Remark 20.4.** Serious homological algebra goes into Beilinson’s construction of $\text{real}$. However, if we allow ourselves to use the Riemann–Hilbert correspondence, we have

$$\xymatrix{ \mathcal{D} - \text{mod}^{\text{hol},r.s.}_{\Lambda\text{-const}} & \text{Perv}_\Lambda(X) \ar[l] \ar[d] \ar[r] \sim \ar[r] & D^b_\Lambda(X) \ar[l]^-{\text{R.H.}}. }$$

Under the equivalence between perverse sheaves and $\mathcal{D}$-modules given by the top arrow, the bottom arrow in this diagram is $\text{real}$. This gives a high concept (rather than high homological algebra!) construction of the realization functor.

The BGS theorem and the techniques involved in proving it will be invaluable as we approach Bezrukavnikov’s equivalence. The proof of the BGS theorem is algebraic, using what are today called **highest weight categories**.

---

$^{18}$Caution: take this explanation with a grain of salt. The proof of Beilinson’s theorem is geometric (via vanishing cycles), and the proof of the BGS theorem is algebraic (via highest weight categories), so a direct comparison doesn’t exactly work.
20.1 Highest weight categories

Definition 20.5. Let $\mathcal{A}$ be a $k$-linear category. We say that $\mathcal{A}$ is highest weight if the following six conditions hold.

1. $\mathcal{A}$ is finite length.
2. The set $\{\text{simple objects in } \mathcal{A}\}/\simeq$ is finite.
3. For any simple object $L \in \mathcal{A}$, $\text{End}(L) = k$.

Let $\Lambda$ be an indexing set for isomorphism classes of simple objects and denote by $L_\lambda \in \mathcal{A}$ the simple object corresponding to $\lambda \in \Lambda$. Assume that $\Lambda$ is a poset (this is part of the data determining a highest weight category). For any closed subset $T \subset \Lambda$ (that is, if $\lambda' \leq \lambda$ and $\lambda \in T$, then $\lambda' \in T$), denote by

$$\mathcal{A}_T = \langle L_\lambda \mid \lambda \in T \rangle_{\text{Serre}}$$

the Serre subcategory generated by the simple objects $L_\lambda$ with $\lambda \in T$. Assume moreover that for each $\lambda \in \Lambda$, there are objects $\Delta_\lambda$ (“standard” object), $\nabla_\lambda$ (“costandard” object) in $\mathcal{A}$ and maps $\Delta_\lambda \rightarrow L_\lambda$, $L_\lambda \rightarrow \nabla_\lambda$.

4. If $T \subset \Lambda$ is closed, then $\Delta_\lambda \rightarrow L_\lambda$ (resp.$L_\lambda \rightarrow \nabla_\lambda$) is a projective cover (resp. injective hull) in $\mathcal{A}_T$.

5. For $\lambda \in \Lambda$,

$$\ker(\Delta_\lambda \rightarrow L_\lambda) \in \mathcal{A}_{< \lambda}, \text{ and}$$

$$\coker(L_\lambda \rightarrow \nabla_\lambda) \in \mathcal{A}_{< \lambda}.$$

This implies that the composition series eggs of $\Delta_\lambda$ and $\nabla_\lambda$ must have the following form

$$\Delta_\lambda = \left\langle \begin{array}{c} L_\lambda \\ L_{\mu}'s \\ \text{ for } \mu < \lambda \end{array} \right. \quad \nabla_\lambda = \left\langle \begin{array}{c} L_\lambda \\ L_{\mu}'s \\ \text{ for } \mu < \lambda \end{array} \right.$$  

6. $\text{Ext}^2(\Delta_\lambda, \nabla_\lambda) = 0$ for all $\lambda, \mu \in \Lambda$.

\[^{19}\text{Note that we are not requiring } \Delta_\lambda \text{ (resp. } \nabla_\lambda \text{) to be projective (resp. injective) objects in } \mathcal{A}, \text{ just in the Serre subcategory } \mathcal{A}_T.\]

\[^{20}\text{This condition is the most mysterious, and often the hardest to show.}\]
**Theorem 20.6.** (Beilinson–Ginzburg–Soergel) Let $\mathcal{A}$ be highest weight. Then $\mathcal{A}$ has enough projective and injective objects. Moreover, the projective cover $P_\lambda$ of $L_\lambda$ has a standard filtration of the form

$$\begin{array}{c}
\Delta_\lambda \\
\Delta_{\lambda^\circ} \\
\Lambda > \lambda
\end{array}$$

Similarly, the injective hull $I_\lambda$ has a costandard filtration of the form

$$\begin{array}{c}
\nabla_{\lambda^\circ} \\
\Lambda > \lambda \\
\nabla_\lambda
\end{array}$$

**Proof.** For full details, see [BGS96, Theorem 3.2.1].

**Sketch:** Instead of proving the theorem as stated, we prove that for any closed subset $T \subseteq \Lambda$, $\mathcal{A}_T$ has enough projectives (resp. injectives), and they admit standard (resp. costandard) filtrations. We construct the projective cover $P^T_\lambda$ of $L_\lambda$ inductively on $T$:

- Let $\mu \in T$ be maximal, and $\lambda \neq \mu \in T$. Assume that the projective cover $P^T_{\lambda \setminus \{\mu\}}$ of $L_\lambda$ in $\mathcal{A}_{T \setminus \{\mu\}}$ is already constructed.

- Let $E = \text{Ext}^1(P^T_{\lambda \setminus \{\mu\}}, \nabla_\mu)$ be the ext group.

- Every element of $E$ gives rise to an extension

  $$\Delta_\mu \hookrightarrow P' \twoheadrightarrow P_\lambda.$$  

  It turns out that there exists a “universal” extension

  $$E^* \otimes \Delta_\mu \hookrightarrow \tilde{P} \twoheadrightarrow P^T_{\lambda \setminus \{\mu\}}$$

  from which all others are constructed via push-out. (Challenge: construct it!)

162
• Claim: \( \tilde{P} \) is the projective cover we are seeking.

Proof. Use long exact sequence in Hom:

\[
\begin{align*}
\text{Hom}(P^T_{\lambda \setminus \mu}, \Delta_\mu) & \longrightarrow \text{Hom}(\tilde{P}, \Delta_\mu) \longrightarrow E \otimes \text{Hom}(\Delta_\mu, \Delta_\lambda) \sim \\
\rightarrow \text{Ext}^1(P^T_{\lambda \setminus \mu}, \Delta_\mu) & \longrightarrow \text{Ext}^1(\tilde{P}, \Delta_\mu) \longrightarrow E \otimes \text{Ext}^1(\Delta_\mu, \Delta_\mu)
\end{align*}
\]

The last term is zero by axiom (4) of a highest weight category. Hence \( \text{Ext}^1(\tilde{P}, \Delta_\mu) = 0 \).

A bit more work using axiom (6) shows that \( \tilde{P} = P^T_\lambda \).

\( \square \)

Definition 20.7. In a highest weight category \( \mathcal{A} \), an object \( T \) is tilting if it has a standard and costandard filtration. The indecomposable tilting objects in \( \mathcal{A} \) are also indexed by \( \Lambda \).

Similar arguments give injective and tilting objects.

\( \square \)

Important objects in a highest weight category:

If our category also has a notion of duality compatible with the highest weight structure, then the costandard/standard and projective/injective objects are dual, as indicated by the pink arrows above.
Exercise 20.8. Let \( B \subset A \) be a Serre subcategory of an abelian category \( A \). By definition, for objects \( M, N \in B \)
\[
\Ext^1_B(M, N) \cong \Ext^1_A(M, N).
\]
Show that
\[
\Ext^2_B(M, N) \hookrightarrow \Ext^2_A(M, N).
\]
Hint: Use effaceability and the long exact sequence of Ext.

Theorem 20.9. If \( X = \bigsqcup_{\lambda \in \Lambda} X_{\lambda} \) is stratified by affine spaces, then \( \Perv_{\Lambda}(X) \) is a highest weight category.

Proof. First, note that \( j_{\lambda} : X_{\lambda} \hookrightarrow X \) is affine and hence
\[
\Delta_{\lambda} := j_{\lambda}! k_{X_{\lambda}}[\dim X_{\lambda}] \quad \text{and} \quad \nabla_{\lambda} := j_{\lambda*} k_{X_{\lambda}}[\dim X_{\lambda}]
\]
are perverse sheaves. Moreover, we have canonical maps
\[
\Delta_{\lambda} \to IC_{\lambda} \hookrightarrow \nabla_{\lambda},
\]
where \( IC_{\lambda} := j_{\lambda*} k_{X_{\lambda}} \) is the IC sheaf corresponding to the trivial local system on \( X_{\lambda} \).

1. \( \Perv_{\Lambda}(X) \) is finite-length. ✓

2. Simple objects in \( \Perv_{\Lambda}(X) \) are parameterized by pairs \( (\mathcal{L}, \lambda) \), where \( \mathcal{L} \) is a local system on \( X_{\lambda} \). Because \( X_{\lambda} \) is affine, it is contractible, and thus admits a single local system. Hence there are finitely many simple objects in \( \Perv_{\Lambda}(X) \). ✓

3. By Schur’s Lemma, \( \End(IC_{\lambda}) \) is a division algebra over \( k \).

Claim 20.10. If \( D \) is a division algebra over a field \( k \), any non-zero algebra homomorphism \( D \to k \) is an isomorphism.

Proof. Let \( \varphi : D \to k \) be a nonzero algebra homomorphism. The kernel of \( \varphi \) is an ideal in \( D \), but the division algebras have no non-trivial ideals, so \( \ker \varphi = \{0\} \). Because \( \varphi \) is a \( k \)-algebra homomorphism, \( \varphi(1) = 1 \). Hence for all \( \ell \in k \), \( \varphi(\ell \cdot 1) = \ell \varphi(1) = \ell \) and \( \im \varphi = k \).

Assume \( X_{\lambda} \subset X \) is open. Then \( IC_{\lambda}|_{X_{\lambda}} = k_{X_{\lambda}}[\dim X_{\lambda}] \). Hence the restriction map
\[
\End(IC_{\lambda}) \to \End(IC_{\lambda}|_{X_{\lambda}}) \cong k
\]
is a nonzero morphism from a division algebra to \( k \). The claim lets us conclude that \( \End(IC_{\lambda}) \cong k \).

For any \( \lambda \), the inclusion \( X_{\lambda} \hookrightarrow \overline{X}_{\lambda} \) is open because \( X_{\lambda} \) is locally closed. There is an equivalence of categories
\[
\text{pervasive sheaves supported on a closed subvariety} \quad \overset{\sim}{\longleftrightarrow} \text{Perv}(Z), \\
Z \subset X
\]
164
so
\[ \text{End}_{\text{Perv}_\Lambda(X)}(IC_{\lambda}) \cong \text{End}_{\text{Perv}_\Lambda(\overline{X}_\lambda)}(IC_{\lambda}). \]
Hence by applying the argument above to the open inclusion \( X_\lambda \hookrightarrow \overline{X}_\lambda \), we conclude that \( \text{End}(IC_{\lambda}) = k \) for all \( \lambda \). ✓

4. The maps in (20.1) give a surjection \( \Delta_\lambda \twoheadrightarrow IC_{\lambda} \) and an injection \( IC_{\lambda} \hookrightarrow \nabla_\lambda \). Because the partial order on \( \Lambda \) is given by closure of strata, for a closed subset \( \{ \leq \lambda \} \subset \Lambda \), we have
\[ \text{Perv}_\Lambda(X)_{\{ \leq \lambda \}} = \text{Perv}_\Lambda(\overline{X}_\lambda). \]
To establish axiom (4), we must show two things: (a) that \( \Delta_\lambda \) is a projective object in \( \text{Perv}_\Lambda(\overline{X}_\lambda) \), and (b) that \( \Delta_\lambda \twoheadrightarrow IC_{\lambda} \) is a projective cover.
To show that \( \Delta_\lambda \) is projective, we will show that \( \text{Hom}_{\text{Perv}_\Lambda(\overline{X}_\lambda)}(\Delta_\lambda, \cdot) \) is exact. Because \( X_\lambda \xrightarrow{j} \overline{X}_\lambda \) is open, for any \( \mathcal{F} \in \text{Perv}_\Lambda(\overline{X}_\lambda) \),
\[
\hom(j_!k_{X_\lambda}[\dim X_\lambda], \mathcal{F}) = \hom(k_{X_\lambda}[\dim X_\lambda], j_!^*\mathcal{F}) \\
= \hom(k_{X_\lambda}[\dim X_\lambda], j_!^*\mathcal{F}) \\
= \hom(k_{X_\lambda}[\dim X_\lambda], \mathcal{F}|_{X_\lambda}) \\
= \mathcal{F}|_{X_\lambda}.
\]
Restriction to an open subvariety is an exact functor, so we conclude that \( \hom(\Delta_\lambda, \cdot) \) is exact.
Because \( \text{Perv}_\Lambda(\overline{X}_\lambda) \) is a finite-length abelian category (in particular, it is Krull-Schmidt), to show that \( \Delta \twoheadrightarrow IC_{\lambda} \) is a projective cover, it suffices to show that \( \Delta_\lambda \) is indecomposable. Now, the endomorphism ring
\[
\text{End}(\Delta_\lambda) = \text{Hom}(j_!k_{X_\lambda}, j_!^*k_{X_\lambda}) = \text{Hom}(k_{X_\lambda}, j_!^*j_!^*k_{X_\lambda}) = \text{End}(k_{X_\lambda}) = k
\]
is local, so \( \Delta_\lambda \) is indecomposable.
Showing that the injection \( IC_{\lambda} \hookrightarrow \nabla_\lambda \) is an injective hull follows from a similar argument. ✓

5. The fact that \( \ker(\Delta_\lambda \twoheadrightarrow IC_{\lambda}) \), \( \text{coker}(IC_{\lambda} \hookrightarrow \nabla_\lambda) \in \text{Perv}_{<\lambda}(X) \) is clear from the composition series eggs and the definition of \( IC_{\lambda} = \text{Im}(J_{\lambda!} \to \overline{j}_{\lambda*}) \):

![Diagram](image-url)
6. To see why condition (6) holds, first observe that by Exercise 20.8,
\[ \text{Ext}^2_{\text{Perv}(X)}(\Delta_{\lambda}, \nabla_{\mu}) \hookrightarrow \text{Ext}^2_{\text{Perv}(X)}(\Delta_{\lambda}, \nabla_{\mu}). \]

Then, by Beilinson’s theorem,
\[ \text{Ext}^2_{\text{Perv}(X)}(\Delta_{\lambda}, \nabla_{\mu}) = \text{Hom}^2_{\text{D}_{bc}(X)}(\Delta_{\lambda}, \nabla_{\mu}). \]

Once we are in the derived category, we have full access\(^{21}\) to the adjoint pairs \((j^!, j^\ast), (j^*, j_\ast)\). Hence we can use adjunctions to compute
\[ \text{Hom}^2_{\text{D}_{bc}(X)}(\Delta_{\lambda}, \nabla_{\mu}) = \text{Hom}_{\text{D}_{bc}(X)}(\Delta_{\lambda}, \nabla_{\mu}). \]

Because the functor \(j^\ast\) is extension by zero, \(j^\ast j^! k_X[\dim X_\lambda] = 0\) for \(\mu \neq \lambda\). If \(\mu = \lambda\), then \(j^\ast j^! k_X[\dim X_\lambda]\) is a 1-dimensional vector space. There are no higher Exts in the category of vector spaces, so we conclude that
\[ \text{Ext}^2_{\text{Perv}_\lambda(X)}(\Delta_{\lambda}, \nabla_{\mu}) = 0. \]

Remark 20.11. It’s unusual for a category of perverse sheaves to have enough projectives. By proving that \(\text{Perv}_\Lambda(X)\) is a highest weight category, we have just algebraically produced a collection of projective perverse sheaves \(\{P_\lambda\}_{\lambda \in \Lambda}\). As far as we are aware, it is not known how to construct these perverse sheaves geometrically.

Corollary 20.12. If \(\Lambda\) is a stratification of \(X\) by affine spaces,
\[ \text{real} : D^b(\text{Perv}_\Lambda(X)) \sim \to D^b_\Lambda(X) \]
is an equivalence of categories.

Proof. Both of the sets \(\{\Delta_{\lambda}\}_{\lambda \in \Lambda}\) and \(\{\nabla_{\lambda}\}_{\lambda \in \Lambda}\) generate \(D^b(\text{Perv}_\Lambda(X))\) and \(D^b_\Lambda(X)\). By the upper triangularity of \(P_\lambda\), the set \(\{P_\lambda\}_{\lambda \in \Lambda}\) also generates each category. Hence it is enough to show
\[ \text{real} : \text{Hom}^i_{D^b(\text{Perv}_\Lambda(X))}(P_\lambda, \nabla_{\mu}) \sim \to \text{Hom}^i_{D^b_\Lambda(X)}(P_\lambda, \nabla_{\mu}). \]

In \(D^b(\text{Perv}_\Lambda(X))\),
\[ \text{Hom}^i(P_\lambda, \nabla_{\mu}) = \begin{cases} 0 & \text{if } i > 0, \\ \text{Hom}_{\text{Perv}(X)}(P_\lambda, \nabla_{\mu}) & \text{if } i = 0, \end{cases} \]
by the projectivity of \(P_\lambda\).

In \(D^b_\Lambda(X)\),
\[ \text{Hom}^i(P_\lambda, \nabla_{\mu}) = \begin{cases} 0 & \text{if } i > 0, \\ \text{Hom}_{D^b_\Lambda(X)}(P_\lambda, \nabla_{\mu}) & \text{if } i = 0, \end{cases} \]
as well. This is because \(\text{Hom}^i_{D^b_\Lambda(X)}(\Delta_\lambda, \nabla_{\mu}) = 0\) for \(i > 0\) by adjunction, so the long exact sequence in Ext and the standard filtration of \(P_\lambda\) imply that \(\text{Hom}^i(P_\lambda, \nabla_{\mu}) = 0\) for \(i > 0\). \(\square\)

\(^{21}\)What we mean by this is that the functor \(j^\ast\) is not exact if \(X_\lambda\) is not open, so it does not preserve perverse sheaves (see beginning of lecture 19).
Remark 20.13. In the proof above, the vanishing of $\text{Hom}_i$ for $i > 0$ happens for quite different reasons in each of the two categories. In $D^b(\text{Perv}_A(X))$, the reason is algebraic (projectivity of an object), whereas in $D^b(X)$, the reason is topological.

20.2 Where are we going for the next few weeks?

For the rest of this lecture, we will reconnect with the big picture of this course and describe our plan for the upcoming weeks.

Let $(X \supset R, X^\vee \supset R^\vee)$ be a root datum, and let $G, G^\vee$ be the corresponding dual groups over $\mathbb{C}$. Associated to this datum, we have a finite Weyl group $W_f$, and an affine Weyl group $W = W_f \ltimes \mathbb{Z}X^\vee$. Let $H$ be the affine Hecke algebra, and $Z$ its center. In October and November of last year, we constructed the following diagram.

$$Z \simeq (ZX^\vee)^{W_f} \xrightarrow{\sim} R_{G^\vee} = \left[\text{Coh pt}/G^\vee\right]$$

$$H \xrightarrow{\sim_{KL}} [K^{G^\vee \times \mathbb{C}^\times}(St)] \xrightarrow{\text{pull-back}}$$

The isomorphism on the bottom line is the Kazhdan–Lusztig isomorphism, which was merely stated (not yet even sufficiently explained, let alone proved!), and the injection on the left is Bernstein’s description of the center of of the affine Hecke algebra. Our goal for the rest of the course is to categorify this picture. This is done via Bezrukavnikov’s equivalence, which very roughly is an equivalence of the form

$$\left(\begin{array}{c}
\text{constructible} \\
\text{affine Hecke category, *}
\end{array}\right) \xrightarrow{\sim_B} \left(\begin{array}{c}
\text{coherent} \\
\text{affine Hecke category, *}
\end{array}\right).$$

The constructible affine Hecke category on the LHS should be (a variant of) a category of constructible sheaves on the affine flag variety of $G$, and the coherent affine Hecke category on the RHS should be (a variant of) a category of $G \times \mathbb{C}^\times$-equivariant coherent sheaves on the Steinberg variety. When we take Grothendieck groups, we should recover the first diagram.

**Philosophy for now:** Before we can understand this story on the level of categories, we need to better understand the Kazhdan–Lusztig isomorphism.

**General strategy for understanding $KL$:**

1. On the Bernstein generators $T_i, \mathcal{O}_\lambda$, define
   $$T_i \mapsto Q_i$$
   $$\mathcal{O}_\lambda \mapsto \mathcal{O}_\lambda$$ (pull-back of $\mathcal{O}(\lambda)$ on $G^\vee/B^\vee$ to $T^*G^\vee/B^\vee \xrightarrow{\text{diagonal}} \text{St}$)

**Remark 20.14.** It is very challenging to verify the relations directly! (See Leonardo Maltoni’s May 24, 2019 talk in the Informal Friday Seminar.)
2. The affine Hecke algebra $H$ has two important modules, defined as follows. Let
\[
\text{triv} : H_f \to \mathbb{Z}[q^{\pm 1}], T_i \mapsto q \\
\text{sgn} : H_f \to \mathbb{Z}[q^{\pm 1}], T_i \mapsto -1
\]
be the (quantized versions of) the trivial and sign representation of the finite Hecke algebra $H_f$. Define two $H$-modules
\[
M := H \otimes_{H_f} \text{triv}, \quad N := H \otimes_{H_f} \text{sgn}
\]
by left multiplication on the first tensor factor. These are, respectively, the \textbf{spherical module} and \textbf{antispherical module} of the Hecke algebra corresponding to the parabolic subgroup $W_f \subset W$.

\textbf{Remark 20.15.} By the Bernstein presentation,
\[
H = \mathbb{Z}[q^{\pm 1}][X^\vee] \otimes H_f.
\]
Hence, as $\mathbb{Z}[q^{\pm 1}]$-modules,
\[
M \cong N \cong \mathbb{Z}[q^{\pm 1}][X^\vee].
\]
Thus, as modules over $\mathbb{Z}[q^{\pm 1}][X^\vee]$, both the spherical and anti-spherical modules are free of rank 1.

3. By convolution formalism, both $K^{G \times C^\times} (G^\vee/B^\vee)$ and $K^{G \times C^\times} (T^* G^\vee/B^\vee)$ are $K^{G \times C^\times} (St)$-modules.

\textbf{Remark 20.16.} Note that
\[
\mathbb{Z}[q^{\pm 1}][X^\vee] = K^{B^\vee \times C^\times} (\text{pt}) \cong K^{G^\vee \times C^\times} (G^\vee/B^\vee) \xrightarrow{\sim} K^{G^\vee \times C^\times} (T^* G^\vee/B^\vee).
\]

4. Compute actions of generators in $M$ (resp. $N$) and match them with actions in $K^{G^\vee \times C^\times} (G^\vee/B^\vee)$ (resp. $K^{G^\vee \times C^\times} (T^* G^\vee/B^\vee)$ under (a choice of) the above isomorphisms. Because all of these modules are faithful, this implies the Kazhdan–Lusztig isomorphism.

\textbf{Remark 20.17.} We really only need to do this computation for either $M$ or $N$ to use this argument to deduce the Kazhdan–Lusztig isomorphism.

\textbf{Next week:} We implement 1-4.

\textbf{Following week:} We take the first step toward Bezrukavnikov’s equivalence by explaining the Arkhipov–Bezrukavnikov’s theorem that
\[
\mathcal{AS} \xrightarrow{\sim} D^b \left( \text{Coh}^{G^\vee \times C^\times} (T^* G^\vee/B^\vee) \right),
\]
where \(\mathcal{AS}\) is the categorical antispherical module.
21 Lecture 21 (April 10, 2020): Equivariant $K$-theory of the Steinberg variety and the antispherical module

Our goal for the next few lectures is to prove the Kazhdan–Lusztig isomorphism:

$$H_{\text{affine}} \simeq K_{G \times \mathbb{C}^\times}(\text{Steinberg}).$$

This is an isomorphism of the affine Hecke algebra with the $G \times \mathbb{C}^\times$-equivariant $K$-theory of the Steinberg variety. Recall from the end of last lecture that our general strategy for proving this isomorphism is to find a vector space on which each algebra acts faithfully by the same operators.

**Remark 21.1.** The reader might have the (correct) impression that this is a rather indirect way of seeing that two algebras are isomorphic. However, there are several instances of very indirect techniques to obtain isomorphisms, equivalences, or correspondences in the Langlands program. Another example of this is Soergel’s functor, which proves an equivalence of two categories (one geometric and one representation theoretic) by matching their images in a third world of algebra (so-called Soergel bimodules).

References for this lecture are:

- Kazhdan–Lusztig, Proof of the Deligne–Langlands conjecture for Hecke algebras, [KL87],
- Chriss-Ginzburg, Representation theory and complex geometry, Chapters 6 & 7, [CG09],
- Henderson, Notes on affine Hecke algebras and $K$-theory.

21.1 Equivariant $K$-theory

Let $X$ be a scheme with an action by a group $G$. Associated to $X$ are the $G$-equivariant $K$-groups for $i \in \mathbb{Z}_{\geq 0}$:

$$G \cap X \sim K_i^G(X).$$

When $i = 0$, this is

$$K_0^G(X) = \text{Grothendieck group of the exact category of } G\text{-equivariant perfect complexes on } X \text{ (i.e. bounded complexes of vector bundles)}.$$

If $X$ is smooth, then every $G$-equivariant coherent sheaf has a resolution by $G$-equivariant vector bundles and thus

$$K_0^G(X) = \text{Grothendieck group of the category of } G\text{-equivariant coherent sheaves on } X.$$

169
Remark 21.2. At some future point we should expand on higher $K$-groups, but that time is not today. For those who are interested, Quillen’s work and the groundbreaking paper [TT90] of Thomason-Trobaugh are highly recommended. In [TT90], they show that if $U \subset X$ is open, we have a sequence \[ \cdots \rightarrow K_i(X \text{ on } Y) \rightarrow K_i(X) \rightarrow K_{i-1}(U) \rightarrow K_{i-1}(X \text{ on } Y) \rightarrow \cdots \] which is almost exact, except that $K_0(X) \rightarrow K_0(U)$ might not be onto for singular $X$. (This result was already proved by Quillen for smooth $X$.)

In the arguments to come, we only care about $K^G_0$, and at certain points we will simply assert that certain boundary maps vanish; e.g., we have a short exact sequence \[ K^G_0(X \text{ on } Y) \hookrightarrow K^G_0(X) \twoheadrightarrow K^G_0(U). \] We set $K^G(X) := K^G_0(X)$.

Examples

1. $K^G(\text{pt}) = R_G = \text{Grothendieck group of finite-dimensional algebraic representations of } G$

2. We claim that $K(\mathbb{P}^1) = \mathbb{Z}[x^{\pm 1}]/(x - 1)^2$. How can we see that this is true? To start, every vector bundle on $\mathbb{P}^1$ is a sum of line bundles. Hence there is a surjection \[ \mathbb{Z}[x^{\pm 1}] \rightarrow K(\mathbb{P}^1) \]
\[ x^m \mapsto \mathcal{O}(m). \]

The tautological exact sequence of vector bundles \[ \mathcal{O}(-1) \hookrightarrow \mathcal{O}_{\mathbb{P}^1} \twoheadrightarrow \mathcal{O}(1) \] shows that under the surjection above,
\[ x^{-1} - 2 + x \mapsto 0. \]

Hence $(x - 1)^2 \mapsto 0$. This shows us that we have a map $\phi : \mathbb{Z}[x^{\pm 1}]/(x - 1)^2 \rightarrow K(\mathbb{P}^1)$.

Claim: $K(\mathbb{P}^1) = \mathbb{Z}[\mathcal{O}] \oplus \mathbb{Z}[\mathcal{O}(1)]$.

The arguments above imply that $[\mathcal{O}]$ and $[\mathcal{O}(1)]$ span $K(\mathbb{P}^1)$. It remains to show that they are linearly independent.

Proof 1: For $X$ proper, $K(X)$ carries an intersection form:
\[ \langle \mathcal{F}, \mathcal{G} \rangle := \chi(\mathcal{F} \otimes \mathcal{G}), \]

\[22\text{We can think of this like the long exact sequence in cohomology, but unlike cohomology, where the long exact sequence came almost simultaneously with its definition, this took twenty years after the initial definition of } K\text{-theory to prove.}\]
where \( \chi \) is the Euler characteristic. Computing the pairings with respect to this form, we get the following table.

\[
\begin{array}{c|cc}
& \mathcal{O} & \mathcal{O}(1) \\
\hline
\mathcal{O} & 1 & 2 \\
\mathcal{O}(1) & 2 & 3 \\
\end{array}
\]

We can see that the determinant is \(-1\), so \( \mathcal{O} \) and \( \mathcal{O}(1) \) are linearly independent. \( \square \)

**Proof 2:** We have seen in Tom’s course that

\[
D^b(\text{Coh } \mathbb{P}^1) \simeq D^b(\text{Rep}(\bullet \rightarrow \bullet))
\]

\[
\mathcal{O} \mapsto L_0 := k \mapsto 0 \\
\mathcal{O}(1) \mapsto L_1 := 0 \mapsto k
\]

The \( K \)-group of any finite length abelian category has a basis given by the classes of simple objects. In the case of \( \text{Rep}(\bullet \rightarrow \bullet) \), the two simple objects are \( L_0 \) and \( L_0 \). Hence we have

\[
K(\mathbb{P}^1) = K(D^b(\text{Coh}(\mathbb{P}^1))) = K(D^b(\text{Rep}(\bullet \rightarrow \bullet))) = \mathbb{Z}[L_0] \oplus \mathbb{Z}[L_1]. \quad \square
\]

**Remark 21.3.** The second proof illustrates a common phenomenon: derived equivalences can have interesting consequences for \( K \)-theory.

**Fact:** Proper maps \( f : X \to Y \) induce maps in \( K \)-theory:

\[
p_\ast : K^G(X) \to K^G(Y)
\]

The map \( p_\ast \) is given by \( p_\ast(F) = \sum (-1)^i R^i f_\ast(F) \).

**Example 21.4.** 1. Projection to a point, \( p : \mathbb{P}^1 \to \text{pt} \), induces the following map on (non-equivariant) \( K \)-theory:

\[
p_\ast : K(\mathbb{P}^1) \cong \mathbb{Z}[x^\pm 1]/(x - 1)^2 \to K(\text{pt}) \cong \mathbb{Z} \\
x^m \mapsto \chi(\mathcal{O}(m)) = m + 1
\]

2. Let \( B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subset SL_2 \) act on \( \mathbb{P}^1 \) in the standard way. Then the map that \( p \) induces on \( B \)-equivariant \( K \)-theory is given by the Weyl character formula. Indeed, we can identify

\[
K^G(\mathbb{P}^1) = K^B(\text{pt}) = \mathbb{Z}[X(B)] = \mathbb{Z}[x^\pm 1].
\]

Then under the composition

\[
K^G(\mathbb{P}^1) \to K^G(\text{pt}) \to K^B(\text{pt}) = \mathbb{Z}[x^\pm 1].
\]

the element \( x^m \in K^B(\mathbb{P}^1) \cong \mathbb{Z}[x^\pm 1] \) maps to \( \frac{x^m - x^{-m - 2}}{1 - x^{-2}} \in K^B(\text{pt}) \cong \mathbb{Z}[x^\pm 1] \).
21.2 Equivariant $K$-theory of the Steinberg variety

Let
\[ G \supset B \supset T \]
be a complex reductive group containing a Borel subgroup containing a maximal torus. Let \( X = X(T) \) be the character lattice, \( W_f \) the finite Weyl group, and \( W = W_f \ltimes \mathbb{Z}X \) the affine Weyl group of the dual\(^{23}\) root system. Let
\[ \mathcal{N} \subset g \]
be the nilpotent cone in the Lie algebra of \( G \), and
\[ \tilde{\mathcal{N}} = \{(x, b) \in \mathcal{N} \times B \mid x \in b\} = T^*B \rightarrow \mathcal{N} \]
be the Springer resolution. Recall that the Steinberg variety is defined to be
\[ St := \tilde{\mathcal{N}} \times_{\mathcal{N}} \tilde{\mathcal{N}} = \{(x, b, b') \mid x \in b, x \in b'\}. \]

We also explained in Lecture 13 how this could be realized as the conormal space to the space \( B \times B \) with the stratification by \( G \)-orbits (which are parameterized by \( W \)).

Example 21.5. Let \( G = SL_2 \). Then \( B = \mathbb{P}^1 \), and the \( G \)-orbit stratification on \( B \times B \) is given by
\[ B \times B = \Delta \sqcup Y, \]
where \( Y := (\mathbb{P}^1 \times \mathbb{P}^1) \setminus \Delta \). An illustration:

Then the Steinberg variety is
\[ T^*_\Delta(\mathbb{P}^1 \times \mathbb{P}^1) \sqcup T^*_Y(\mathbb{P}^1 \times \mathbb{P}^1) = T^*\mathbb{P}^1 \sqcup Y. \]

\(^{23}\)This convention is introduced to avoid including many checks (to indicate Langlands dual groups) in the rest of this lecture and the next.
An illustration:

In the “easy part,” projection onto each component of $B \times B$ is an isomorphism. In the “tricky part,” projection onto each component hits the zero section in $T^*\mathbb{P}^1$.

The group $G \times \mathbb{C}^\times$ acts on $St$ via
\[
(g, z) \cdot (z, b, b') = (z^2 gx, gb, gb').
\] (21.1)

**Algebra structure on $K^{G \times \mathbb{C}^\times}(St)$:**

Recall that $K^{G \times \mathbb{C}^\times}(St)$ has an algebra structure given by convolution in $D^b(\text{Coh})$ (see Lectures 14 and 15 for a refresher):
\[
\mathcal{F} \ast \mathcal{G} := p_{13}^*(p_{12}^* \mathcal{F} \otimes p_{23}^* \mathcal{G}),
\]
where $p_{ij}$ are the canonical projections

\[
\begin{array}{ccc}
\tilde{N} & \times_N & \tilde{N} \\
\downarrow p_{12} & & \downarrow p_{13} \\
St & \leftarrow & St \\
\end{array}
\begin{array}{ccc}
\tilde{N} & \times_N & \tilde{N} \\
\downarrow p_{23} & & \downarrow p_{23} \\
St & \rightarrow & St \\
\end{array}
\]

**Module structure on $K^{G \times \mathbb{C}^\times}(\tilde{N})$:**

Similarly, convolution also gives $K^{G \times \mathbb{C}^\times}(\tilde{N})$ the structure of a module for $K^{G \times \mathbb{C}^\times}(St)$:
\[
\mathcal{F} \ast \mathcal{G} := p_{1*}(\mathcal{F} \times p_2^* \mathcal{G}),
\]
where

\[
\begin{array}{ccc}
\tilde{N} & \times_N & \tilde{N} \\
\downarrow p_1 & & \downarrow p_2 \\
\tilde{N} & \leftarrow & \tilde{N} \\
\end{array}
\]

Recall that our goal is to prove that
\[
K^{G \times \mathbb{C}^\times}(St) \cong H.
\]
We will accomplish that through a subgoal, which is to show that
\[ K^{G \times C^x} (\widetilde{N}) \cong \text{anti-spherical module}. \]

We can work toward the subgoal by examining the vector space structure of \( K^{G \times C^x} (\widetilde{N}) \) more closely.

First, note that we have a map
\[ (K^{G \times C^x} (\widetilde{N})) \xrightarrow{\text{pull back}} K^{G \times C^x} (B) = K^{B \times C^x} (\text{pt}) = \mathbb{Z}[v^{\pm 1}][X]. \]

Because \( \widetilde{N} \) is a vector bundle over \( B \), pull-back is an isomorphism. Hence
\[ K^{G \times C^x} (\widetilde{N}) = \mathbb{Z}[v^{\pm 1}][X]. \]

Now we turn to the vector space structure on \( K^{G \times C^x} (St) \). The space \( B \times B \) has a filtration via closures of \( G \)-orbits:
\[ \emptyset = Z_{-1} \subset Z_0 \subset \cdots \subset Z_m = B \times B, \]
with \( Z_i \setminus Z_{i+1} \cong G \cdot (x_i B, B) \cong G 	imes_B X_i \), where \( X_i = Bx_i B / B \) is a Bruhat cell. This induces a filtration of the Steinberg variety:
\[ \emptyset = \widetilde{Z}_{-1} \subset \widetilde{Z}_0 \subset \cdots \subset \widetilde{Z}_m = St, \]
with \( \widetilde{Z}_i \setminus \widetilde{Z}_{i+1} \cong T^*_x (B \times B) =: T^*_x. \) We have
\[ K^{G \times C^x} (T^*_x) = K^{G \times C^x} (X_i) = K^{B \times C^x} (X_i) = K^{B \times C^x} (\text{pt}). \]

All boundary maps vanish when we apply \( K^{G \times C^x} \) to the above filtration, and a little work (see [CG09]) yields:
\[ K^{G \times C^x} (St) = \bigoplus_{x \in W_f} \mathbb{Z}[v^{\pm 1}][X][O_{T^*_x}]. \]

Remark 21.6. Compare this to the decomposition
\[ H = \bigoplus_{x \in W_f} \mathbb{Z}[v^{\pm 1}][X]T_x. \]

21.3 The spherical and anti-spherical modules

Recall Bernstein’s presentation of the affine Hecke algebra (Theorem 12.5): \( H \) is an algebra over \( \mathbb{Z}[v^{\pm 1}] \) with generators
\[ \{ H_s \mid s \in S_f \} \quad \text{(finite part)} \quad \text{and} \quad \{ \theta_\lambda \mid \lambda \in X \} \quad \text{(lattice part)}. \]

The generators \( \{ H_s \mid s \in S_f \} \) generate a copy of the finite Hecke algebra \( H_f \) and the generators \( \{ \theta_\lambda \mid \lambda \in X \} \) generate \( \mathbb{Z}[v^{\pm 1}][X] \). The relations are:
1. $H_s^2 = (v^{-1} - v)H_1 + 1$ for all $s \in S$ + braid relations (finite part),
2. $\theta_{\lambda\gamma} = \theta_{\lambda + \gamma}$ for all $\lambda, \gamma \in X$ (lattice part), and
3. **the most important relation:** For a simple reflection $s = s_\alpha \in S$ and $\lambda \in X$,

$$H_s \theta_{s\lambda} - \theta_\lambda H_s = (v - v^{-1}) \left( \frac{\theta_\lambda - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right).$$

The first relation can be rewritten as

$$(H_s + v)(H_s - v^{-1}) = 0,$$

which implies that $H_f$ has two natural rank 1 modules:

$$\text{triv} : H_s \mapsto v^{-1},$$
$$\text{sgn} : H_s \mapsto -v.$$

From these we construct two induced $H$-modules:

$$M = H \otimes_{H_f} \text{triv}, \text{ “spherical module”}$$
$$N = H \otimes_{H_f} \text{sgn}, \text{ “anti-spherical module”}$$

As modules over the lattice part, each is isomorphic to $\mathbb{Z}[v^\pm 1][X]$.

**Remark 21.7.** In what follows, we will abuse notation and write $\theta_\lambda := \theta_\lambda \otimes 1 \in N$.

Using the third relation in the affine Hecke algebra, we can compute the action of the generator $\theta_s \in H$ on $\theta_{s\lambda} \in N$ in the anti-spherical module:

$$H_s \cdot \theta_{s\lambda} = (v - v^{-1}) \left( \frac{\theta_\lambda - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right) + \theta_\lambda H_s$$

$$= v \left( \frac{\theta_\lambda - \theta_{s\lambda} - \theta_\lambda + \theta_{\lambda - \alpha}}{1 - \theta_{-\alpha}} \right) - v^{-1} \left( \frac{\theta_\lambda - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right)$$

$$= v \left( \frac{\theta_{\lambda - \alpha} - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right) - v^{-1} \left( \frac{\theta_\lambda - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right).$$

This formula looks nicer if we instead compute the action in terms of the Kazhdan–Lusztig generator $b_s := H_s + v$:

$$b_s \cdot \theta_{s\lambda} = v \left( \frac{\theta_{\lambda - \alpha} - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right) - v^{-1} \left( \frac{\theta_\lambda - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right) + v \theta_{s\lambda}$$

$$= v \left( \frac{\theta_{\lambda - \alpha} - \theta_{s\lambda - \alpha}}{1 - \theta_{-\alpha}} \right) - v^{-1} \left( \frac{\theta_\lambda - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right)$$

$$= (v \theta_{-\alpha} - v^{-1}) \left( \frac{\theta_\lambda - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right).$$

In other words,

$$b_s \cdot \theta_\lambda = (v^{-1} - v \theta_{-\alpha}) \left( \frac{\theta_\lambda - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right).$$

(21.2)

We’ll pick up here next week with a very similar looking computation in $K$-theory.
22 Lecture 22 (April 17, 2020): Proof of the Kazhdan–Lusztig isomorphism

In today’s lecture we will complete the proof of the Kazhdan–Lusztig isomorphism. First, we establish and streamline notation.

22.1 Notation and set-up

Let

\[ G \supset B \supset T \]

be a complex reductive group, Borel subgroup, and maximal torus. Let \( X \) be the character lattice, and \( W_f \subset W \) the finite and affine Weyl groups with simple reflections \( S_f \subset W_f \) and \( S \subset W \). We denote by \( B \) the flag variety, which we realize as the variety of Borel subalgebras of \( \mathfrak{g} = \text{Lie} \, G \). The group \( G \) acts on the product \( B \times B \), and the orbits give a stratification with strata parameterized by \( W_f \):

\[ G \circlearrowright B \times B = \bigsqcup_{x \in W_f} \mathcal{O}_x. \]

The orbit \( \mathcal{O}_x \) consists of pairs of flags/Borel subalgebras in relative position \( x \). For example, \( \mathcal{O}_{\text{id}} = \Delta \) (the diagonal in \( B \times B \)), and \( \mathcal{O}_{w_0} \) (where \( w_0 \in W_f \) is the longest element) is open in \( B \times B \).

Let

\[ \widetilde{N} = T^* B \to N \subset \mathfrak{g} \]

be the Springer resolution. The Steinberg variety is

\[ St = \widetilde{N} \times_N \widetilde{N} = \bigsqcup_{x \in W_f} T^*_{\mathcal{O}_x} (B \times B) = \bigsqcup_{w \in W_f} \Lambda_x, \]

where \( T^*_{\mathcal{O}_x} (B \times B) \) is the conormal bundle of the \( G \)-orbit \( \mathcal{O}_x \), whose closure \( \Lambda_x := \overline{T^*_{\mathcal{O}_x} (B \times B)} \) is an irreducible component of \( St \).

Last week we discussed the following example.

Example 22.1. Let \( G = SL_2 \), so \( B = \mathbb{P}^1 \). The \( G \)-orbit stratification of \( B \times B \) is:

![Diagram of orbit stratification](image)
The corresponding stratification of the Steinberg variety is

\[ St = T_{0_{id}}^*(\mathcal{B} \times \mathcal{B}) \sqcup T_{0_{s}}^*(\mathcal{B} \times \mathcal{B}). \]

The closures of the strata give the irreducible components \( \Lambda_x, x \in W_f \) of \( St \), which are glued together as follows:

\[ \Lambda_{id} \simeq \tilde{\mathcal{N}} \simeq T^* \mathbb{P}^1 \]

\[ \Lambda_s \simeq \mathbb{P}^1 \times \mathbb{P}^1 \]

**Remark 22.2.** In general, the components range from \( \Lambda_{id} \simeq \tilde{\mathcal{N}} \) to \( \Lambda_{w_0} = \mathcal{B} \times \mathcal{B} \). They are not smooth in general, and their intersection pattern is extremely complicated. For example, it is not known in general when two \( \Lambda_x \) and \( \Lambda_y \) intersect in codimension 1.

Last week we introduced the anti-spherical module

\[ N = H \otimes_{H_f} \text{sgn} \simeq \mathbb{Z}[v^\pm][X] \]

\[ \theta_\lambda := \theta_\lambda \otimes 1 \leftarrow e^\lambda \]

for the affine Hecke algebra \( H \) and established the **Demazure–Lusztig formula**

\[ b_s \cdot \theta_\lambda = (v^{-1} - v\theta_\alpha) \left( \frac{\theta_\lambda - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right), \]

(22.1)

Here \( H_f = \langle H_s \rangle_{s \in S_f} \) is the finite Hecke algebra and \( b_s := H_s + v \) is the Kazhdan–Lusztig generator corresponding to the simple reflection \( s = s_\alpha \in S_f \).

**Remark 22.3.** It is not immediately obvious that the formula \( \left( \frac{\theta_\lambda - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right) \) gives an element in the lattice part of \( H \). However, by rewriting

\[ \left( \frac{\theta_\lambda - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right) = (\theta_\lambda + \theta_{\lambda - \alpha} + \cdots + \theta_{s\lambda + \alpha}), \]

we see that \( b_s \cdot \theta_\lambda \in \mathbb{Z}[v^\pm][X] \). (Here we assume \( \langle \lambda, \alpha^\vee \rangle \geq 0 \).)

We want to show that a similar formula holds for the \( K^{G \times \mathbb{C}^\times} (St) \)-action on \( K^{G \times \mathbb{C}^\times} (\tilde{\mathcal{N}}) \). We will first do so in the special case of \( G = SL_2 \), then move on to the general formulation.
22.2 The case of SL₂

We start with a baby version of the calculation. We identify $K^G(\mathbb{P}^1)$ with $\mathbb{Z}[x^{\pm 1}]$ via the chain of isomorphisms

$$K^G(\mathbb{P}^1) \simeq K^G(G/B) \simeq K^B(\text{pt}) \simeq \mathbb{Z}[x^{\pm 1}]$$

Under this identification, $\mathcal{O}(m) \mapsto x^m$. We have a Cartesian square

$$\begin{array}{ccc} \mathbb{P}^1 \times \mathbb{P}^1 & \xrightarrow{p_1} & \mathbb{P}^1 \\ \downarrow^{p_1} & & \downarrow^{\text{pt}} \\ \mathbb{P}^1 & \xrightarrow{p_2} & \text{pt} \end{array}$$

Claim 1: The map $p_1*p_2^*: K^G(\mathbb{P}^1) \to K^G(\mathbb{P}^1)$ is given by $x^m \mapsto \frac{x^{m-x^{-m-2}}}{1-x^{-2}}$.

Proof. By smooth base change, $p_1*p_2^* = p_2^*p_1^*$. Then the claim follows from Weyl’s character formula.

Claim 2: $p_1*(\mathcal{O}(-2,0) \otimes p_2^*(-)) : K^G(\mathbb{P}^1) \to K^G(\mathbb{P}^1)$ is given by $x^m \mapsto x^{-2}\left(\frac{x^{m-x^{-m-2}}}{1-x^{-2}}\right)$.

Proof. The notation $\mathcal{O}(m, n)$ refers to $p_1^*\mathcal{O}(m) \otimes p_2^*\mathcal{O}(n)$. By the projection formula, $p_1*(p_1^*(-2) \otimes p_2^*(-)) = \mathcal{O}(-2) \otimes p_1*p_2^*(-)$. The claim then follows from Claim 1.

Now we move up to $\tilde{N}$. Recall that the pull-back $q^*$ of the projection $\tilde{N} = T^*\mathbb{P}^1 \to \mathbb{P}^1$ gives an isomorphism

$$K^{G \times \mathbb{C}^\times}(\tilde{N}) \leftarrow q^* K^{G \times \mathbb{C}^\times}(\mathbb{P}^1) = \mathbb{Z}[v^{\pm 1}][X].$$

Recall that $\mathbb{C}^\times$ acts on $\tilde{N}$ via scaling by $z^2$ (equation (21.1)). For the rest of this section, set $\mathcal{O} := \mathcal{O}_{\tilde{N}}$.

We have projections

\[ \begin{array}{ccc} \tilde{N} & \xrightarrow{q^*} & K^{G \times \mathbb{C}^\times}(\mathbb{P}^1) \\ \downarrow^{p_1} & & \downarrow^{p_1} \\ \tilde{N} & \xrightarrow{p_1} & \mathbb{P}^1 \\ \downarrow^{p_1} & & \downarrow^{p_1} \\ \tilde{N} & \xrightarrow{p_1} & \mathbb{P}^1 \end{array} \]
Set

\[ Q_s := \mathcal{O}_{\mathbb{P}^1 \times \mathbb{P}^1}(-2, 0) \]

on \( \Lambda_s \simeq \mathbb{P}^1 \times \mathbb{P}^1 \subset \text{St} \). We will see that (up to some simple scalar factors), \( Q_s \) acts via convolution on \( K^{G \times \mathbb{C}^e}(\text{St}) \) in the same way that \( b_s \) acts on \( N \). To do so, we want to calculate

\[ p_{1*}(Q_s \otimes p_2^* \mathcal{O}(m)) \in K^{G \times \mathbb{C}^e}(\tilde{N}). \]

**Claim 3:** Let \( \mathbb{P}^1 \rightarrow \tilde{N} \). Then \( p_{1*}(Q_s \otimes p_2^* \mathcal{O}(m)) = \left( \frac{z^m - x - m - 2}{1 - x - z} \right) [i_* \mathcal{O}_{\mathbb{P}^1}(-2)] \).

**Exercise 22.4.**

1. Suppose \( \pi : E \rightarrow Y \) is a vector bundle, \( \mathcal{F} \) a quasi-coherent sheaf on \( Y \), \( \mathcal{G} \) a locally free sheaf on \( Y \), and \( i : Y \hookrightarrow E \) the zero section. Show that

\[ i_* \mathcal{F} \otimes \pi^* \mathcal{G} = i_* (\mathcal{F} \otimes \mathcal{G}). \]

2. Use 1. applied to \( \tilde{N} \times \tilde{N} \rightarrow \mathbb{P}^1 \times \mathbb{P}^1 \) to deduce Claim 3.

It remains to express \([i_* \mathcal{O}_{\mathbb{P}^1}(-2)]\) in terms of our basis of \( K^{G \times \mathbb{C}^e}(\tilde{N}) \); that is, to understand \( i_* \mathcal{O}_{\mathbb{P}^1}(-2) \) in terms of vector bundles.

**Useful basic technique:** Given a vector bundle \( q : V \rightarrow Y \), there is a bijection

\[ \left\{ \begin{array}{c}
\text{quasi-coherent sheaves} \\
\text{on the total space of } V
\end{array} \right\} \simeq \left\{ \begin{array}{c}
\text{quasicoherent sheaves of} \\
\text{modules over } q_* \mathcal{O}_V \simeq \text{Sym}^e(V^*)
\end{array} \right\}. \]

(More generally, this holds for any affine morphism, see Hartshorne.)

In our case, the projection

\[ \tilde{N} = T^* \mathbb{P}^1 \rightarrow \mathbb{P}^1 \]

is the line bundle associated to \( \mathcal{O}(-2) \), and

\[ q_* \mathcal{O} \simeq \text{Sym}^e(\mathcal{O}_{\mathbb{P}^1}(2)) = \mathcal{O}_{\mathbb{P}^1} \oplus \mathcal{O}_{\mathbb{P}^1}(2) \oplus \mathcal{O}_{\mathbb{P}^1}(4) \oplus \cdots . \]

Additionally, \( \mathbb{C}^e \) acts on \( T^* \mathbb{P}^1 \rightarrow \mathbb{P}^1 \) as multiplication by \( z^2 \) along the fibres, which corresponds to multiplication by \( z^{-2} \) in the second factor in the direct sum decomposition above. Hence we have an exact sequence

\[ z^{-2} \mathcal{O}(2) \hookrightarrow \mathcal{O} \twoheadrightarrow i_* \mathcal{O}_{\mathbb{P}^1}. \]

**Remark 22.5.** Locally, this is the short exact sequence

\[ k[x] \xrightarrow{x^e} k[x] \rightarrow k, \]

but globally, we have some twisting. This is a special example of the Koszul resolution of the zero section of a vector bundle.
Hence in $K^{G \times \mathbb{C}^x} (\mathcal{N})$, we have
\[ [i_* \mathcal{O}_{\mathbb{P}^1}] = [\mathcal{O}] - v^{-2} [\mathcal{O}(2)]. \]

By tensoring with $\mathcal{O}(-2)$ we obtain
\[ [i_* \mathcal{O}_{\mathbb{P}^1}(-2)] = [\mathcal{O}(-2)] - v^{-2} [\mathcal{O}]. \]

Putting it all together, we see that
\[ x_m \overset{[Q_s]^*}{\rightarrow} (x^{-2} - v^{-2}) \left( \frac{x^m - x^{-m-2}}{1 - x^{-2}} \right). \]

Hence
\[ x_m \overset{[-vQ_s]^*}{\rightarrow} (v^{-1} - vx^{-2}) \left( \frac{x^m - x^{-m-2}}{1 - x^{-2}} \right). \]

We only need two last pieces of information to establish the Kazhdan–Lusztig isomorphism for $SL_2$, which we leave as exercises.

**Exercise 22.6.** The map $\theta_m \mapsto x^{m-1}$ intertwines the actions of $b_s$ and $-[vQ_s]^*$.

**Exercise 22.7.** Both the representation $N$ of $H$ and the representation $K^{G \times \mathbb{C}^x} (\mathcal{N})$ of $K^{G \times \mathbb{C}^x} (St)$ are faithful.

### 22.3 The general case

Roughly speaking, in the $SL_2$ example, we have seen the meaning in $K$-theory of the Demazure–Lusztig formula
\[ b_s \cdot \theta_\lambda = (v^{-1} - v\theta_{-\alpha}) \left( \frac{\theta_\lambda - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right). \]

The first factor $(v^{-1} - v\theta_{-\alpha})$ comes from the “Koszul resolution,” and the second factor $\left( \frac{\theta_\lambda - \theta_{s\lambda}}{1 - \theta_{-\alpha}} \right)$ from the “push-pull for $\mathbb{P}^1$.” We will now explain that the same philosophy works in general.

**Relative cotangent bundle:** Let
\[ Z \xrightarrow{f} Y \]
be a smooth map. (Think submersion = fibration.)
The relative tangent bundle is
\[ T_{Z/Y} := \ker(df : TZ \to TY). \]
We have a short exact sequence
\[ T_{Z/Y} \hookrightarrow T_Z \to f^*T_Y. \]
Dually,
\[ f^*T_Y^* \hookrightarrow T_Z^* \to T_{Z/Y}^*. \]

A caricature:

In our setting, we have a \( \mathbb{P}^1 \) fibration
\[ \mathcal{B} \xrightarrow{\pi_s} \mathcal{B}_s, \]
where \( \mathcal{B}_s \) is the variety of parabolic subalgebras of type \( s \).

Fundamental Cartesian diagram:
\[ \mathcal{O}_s \xrightarrow{p_1} \mathcal{B} \xrightarrow{p_2} \mathcal{B}_s \]
\[ \pi_s \downarrow \quad \pi_s \downarrow \]
\[ \mathcal{B} \xrightarrow{\pi_s} \mathcal{B}_s \]

Here \( \mathcal{O}_s \subset \mathcal{B} \times \mathcal{B} \) is the \( G \)-orbit consisting of pairs of flags in relative position \( s \). All maps in this diagram are \( \mathbb{P}^1 \)-fibrations. We identify \( K^G(\mathcal{B}) \simeq \mathbb{Z}[X] \) via \( \mathcal{O}_B(\lambda) \mapsto e^{\lambda} \).

Claim 4: \( \pi_s \pi_s^* : K^G(\mathcal{B}) \to K \) maps \( e^{\lambda} \mapsto \frac{e^{\lambda} - e^{s(\lambda)} - \alpha}{1 - e^{-\alpha}} \).
Proof. Again, this is simply an instance of the Weyl character formula for \( \mathbb{P}^1 \).

We claim that the corresponding Cartesian diagram “upstairs” is

\[
\begin{array}{ccc}
\Lambda_s & \longrightarrow & \tilde{N}_s \\
\downarrow & & \downarrow \\
\tilde{N}_s & \longrightarrow & T^*B_s
\end{array}
\]

To see that this is the correct lift of the first Cartesian square, we start with the lower right corner

\[ T^*B_s = \{(p, x) \mid x \in \text{nilrad}(\pi_s(b)) \}, \]

which implies that the upper right and lower left corners are

\[ \tilde{N}_s = \pi_s^*T^*_B/B_s = \{(b, x) \mid x \in \text{nilrad}(\pi_s(b)) \} \subset \tilde{N}. \]

Hence the fibre product completing the diagram in the upper left corner is given by

\[ \left\{ (b, b', x) \mid b, b' \text{ in relative position } s, \text{ and } x \in \text{nilrad}(\pi_s(b)) = \text{nilrad}(\pi_s(b')) \right\} = \Lambda_s. \]

Together, these two Cartesian squares form a “Cartesian cube:”

\[
\begin{array}{ccc}
\Lambda_s & \longrightarrow & \tilde{N}_s \\
\downarrow & & \downarrow \\
\tilde{N}_s & \longrightarrow & T^*B_s \\
\downarrow & & \downarrow \\
\tilde{B}_s & \longrightarrow & B
\end{array}
\]

Define

\[ Q_s := q^*\Omega_{\tilde{B}_s/B} \]

to be the relative 1-forms with respect to the second projection. As earlier, Claim 4 gives

\[ p_1^*(Q_s \otimes p_2^*\mathcal{O}(\lambda)) = \left( \frac{e^\lambda - e^{s(\lambda)-\alpha}}{1 - e^{-\alpha}} \right) [i_*\mathcal{O}_{\tilde{N}_s}(-\alpha)], \]

where \( \tilde{N}_s \hookrightarrow \tilde{N} \) is the inclusion.

What remains is to express \( [i_*\mathcal{O}_{\tilde{N}_s}(-\alpha)] \in K^{G \times \mathbb{C}^\times}(\tilde{N}) \) in the basis of line bundles. Again, we can do so using a Koszul-type resolution. There is a short exact sequence of \( B \)-modules

\[ p_s/b \hookrightarrow g/b \twoheadrightarrow g/p_s. \]
The corresponding exact sequence of vector bundles on $B = G/B$ is

$$L_\alpha \hookrightarrow T_B \twoheadrightarrow \pi_s^*T_{B_s};$$

where $L_\alpha$ is the line bundle on $B$ associated to $\alpha \in X$. Passing to symmetric algebras, we obtain the Koszul resolution

$$z^{-2}\text{Sym}^\bullet(T_B)(\alpha) \hookrightarrow \text{Sym}^\bullet(T_B) \twoheadrightarrow \text{Sym}^\bullet(\pi_s^*T_B).$$

**Remark 22.8.** This should be thought of as the vector bundle version of the short exact sequence

$$k[x_1,\ldots,x_n] \xrightarrow{x_n} k[x_1,\ldots,x_n] \rightarrow k[x_1,\ldots,x_{n-1}].$$

The $z^{-2}$ comes from the $\mathbb{C}^\times$-action.

In other words,

$$z^{-2}\mathcal{O}_{\tilde{N}}(\alpha) \hookrightarrow \mathcal{O}_{\tilde{N}} \twoheadrightarrow i_*\mathcal{O}_{\tilde{N}_s}.$$

**The result:**

$$[i_*\mathcal{O}_{\tilde{N}_s}(-\alpha)] = [\mathcal{O}_{\tilde{N}}(-\alpha)] - z^{-2}[\mathcal{O}_{\tilde{N}}].$$

From here, the proof follows from two exercises analogous to those in the previous section.

**Exercise 22.9.** Check that $\theta_\lambda \mapsto e^{\lambda\pm\rho}$ intertwines $b_s^\ast$ and $-[vQ_s]^\ast$.

**Exercise 22.10.** Complete the proof by showing that $N$ (resp. $K^G\times\mathbb{C}^\times(\tilde{N})$) are faithful modules over $H$ (resp. $K^G\times\mathbb{C}^\times(\tilde{N})$).

**Remark 22.11.** Geordie isn’t quite sure about whether we should have $\alpha$ or $-\alpha$ above, so the reader should take the final arguments with a grain of salt.
References


