Galois Representations

Tim Dokchitser
Course notes by Emma Bailey

Oct 13 - Dec 1, 2016

1 Riemann ζ-function

Definition. *Recall that we define Riemann's zeta function via*

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1}.$$

Riemann proved that ζ can be extended meromorphically to $\mathbb{C}$.

Theorem 1.1. *We have that $\zeta(s)$ has meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1$ of residue 1. The completed function has the form*

$$\hat{\zeta}(s) = \frac{1}{\pi^{s/2}} \Gamma\left(\frac{s}{2}\right) \zeta(s),$$

and it satisfies the functional equation

$$\hat{\zeta}(s) = \hat{\zeta}(1 - s).$$

Proof. This is proved using the Poisson summation formula and is a standard proof. □

Definition (L-function)**.** *We define an L-function as a Dirichlet series of the form*

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where $a_n \in \mathbb{C}$, and $a_n = O(n^r)$ for some r. Then the series 'makes sense' since it will converge on the half plane for $\mathrm{Re}(s) > r + 1$. *It* has an Euler product and has degree d *if can be written as a product*

$$L(s) = \prod_p \frac{1}{F_p(p^{-s})}$$

with $F_p(t) \in \mathbb{C}[t]$ polynomials of degree $\leq d$, and $= d$ for almost all primes. The terms are called local factors and $F_p(T)$ the local polynomials.

Example 1.1. *The Riemann zeta function has Euler product and degree 1.*

All L-fns we will see will satisfy this, and are conjectured to

(a) have meromorphic continuation to $\mathbb{C}$ with finitely many poles (usually none)

(b) Function equation: $\exists$ weight k, a sign w, conductor N and a Γ-factor

$$\gamma(s) = \Gamma\left(\frac{s+\lambda_1}{2}\right)\cdots\Gamma\left(\frac{s+\lambda_d}{2}\right)$$

such that

$$\hat{L}(s) = \left(\frac{N}{\pi^d}\right)^{s/2}\gamma(s)L(s)$$

satisfies

$$\hat{L}(s) = w\cdot\overline{\hat{L}}(k-s).$$

(c) Riemann hypothesis: all non-trivial zeros lie on the line $\mathrm{Re}(s) = k/2$.

Remarks.

- *If $L(s)$ satisfies (a) and (b) then as in the proof of theorem 1.1 (here this theta function is not the Jacobi one)*

$$\hat{L}(s) = \int_1^\infty (x^{s/2} + w\cdot x^{(k-s)/2})\Theta(\sqrt{N}\cdot x)\frac{dx}{x}$$

where $\Theta(x) = \sum_{n=1}^\infty a_n\phi_{n,\gamma}(x)$ where the ϕ function depends only on $\gamma(s)$ and decays exponentially with n. In fact, (b) is equivalent to

$$\Theta\left(\frac{1}{Nx}\right) = w\cdot\overline{\Theta}(x). \qquad (\star)$$

This gives a way to compute L-functions numerically (with $\sim\sqrt{N}$ terms). This gives an idea of measure of arithmetic complexity of an L-function by looking at how bit the square root of the conductor is (larger means harder).

- *There are functions called modular forms f (technically, newforms of weight k, level N and w-eigenform for the Atkin-Lehner involution)*

$$f : \{z\in\mathbb{C} : \mathrm{Im}(z) > 0\} \to \mathbb{C}$$

such that $\Theta(x) = f(ix)$ satisfies ($\star$) by definition. Thus, their L-functions satisfy (a) and (b), again pretty much by definition.

- *2 categories of L-fns $L(s) = \sum_{n=1}^\infty \frac{a_n}{n^s}$:*
  - *(i) With a direct formula for the a_n. Generally, we know how to prove (a) and (b) for these.*
  - *(ii) Only defined by an Euler product, for example $L(\rho, s)$ Artin, $L(E, s)$ elliptic curves, other varieties... We never know how to prove (a) and (b) for these except by reducing to (i).*

Function	a_n
$\zeta(s)$	1
$L(\chi, s)$	$\chi(n)$
$\zeta_K(s)$	# ideals of norm n in $\mathcal{O}_K$

2 Dedekind ζ-functions

Definition. *Let K be a number field, with $[K : \mathbb{Q}] = d$ so $K \cong \mathbb{Q}^d$ as a $\mathbb{Q}$-vector space. Then let $\mathcal{O} = \mathcal{O}_K$ be the ring of integers, so $\mathcal{O} \cong \mathbb{Z}^d$ as abelian group. Take $I \subset \mathcal{O}_K$ a non-zero ideal. Define the norm*

$$NI = (\mathcal{O}_K : I).$$

It is finite, and satisfies nice properties like being multiplicative:

$$N(IJ) = NI \cdot NJ,$$

and I can be written as a unique product of prime ideals,

$$I = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}$$

where $\mathcal{O}/\mathfrak{p}_i$ is a finite integral domain, which implies it is a field $\mathbb{F}_{p^r}$ and hence $\mathfrak{p}_i \subset (p_i)$ for some primes $p_i \in \mathbb{Z}$.

In particular, if we take an ideal $I = (p)$ where $p \in \mathbb{Z}$ and factor it

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

we call the ideals $\mathfrak{p}_i$ primes above p, and the e_i's are ramification indices (theese are usually equal to 1 for all but finitely many p, namely $p \nmid \Delta_k$ called unramified primes p). Finally, we say that

$$f_i = [\mathcal{O}/\mathfrak{p}_i : \mathbb{F}_p]$$

are the residue degrees. Thus $\mathcal{O}/\mathfrak{p}_i \cong \mathbb{F}_{p^f}$.

Then $N(p) = (\mathcal{O} : p\mathcal{O}) = p^d$ since $\mathcal{O} \cong \mathbb{Z}^d$ and $p\mathcal{O} \cong p \cdot \mathbb{Z}^d$. This implies that

$$d = \sum_{i=1}^{r} e_i f_i$$

in general, and $d = \sum_{i=1}^{r} f_i$ for unramified primes.

Note that if the extension $K/\mathbb{Q}$ is Galois then $e_1 = \cdots = e_d, f_1 = \cdots = f_d$ since Gal($K/\mathbb{Q}$) permutes $\mathfrak{p}_i$ transitively. Hence in this case $d = efr$.

In practice,

Theorem 2.1 (Kummer-Dedekind)**.** *Let* $K = \frac{\mathbb{Q}[x]}{(g(X))}$ *where* $g(X) \in \mathbb{Z}[X]$ *monic. Then* $\Delta_K | \Delta_g$, *and for all primes* $p \nmid \Delta_g$,

$$p = \prod_{i=1}^{r} \mathfrak{p}_i$$

is unramified, and we have

$$g(X) = g_1 \dots g_r \mod p$$

with $\deg g_i = f_i$.

Definition (Dedekind ζ-function of K)**.** *Let*

$$\zeta_K(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$$

where $a_n = \{\#$ *of ideas of norm n in* $\mathcal{O}_K\}$. *Alternatively, we can write*

$$\begin{aligned}
\zeta_K(s) &= \sum_{\substack{I \subset \mathcal{O}_K \textit{ideal} \\ I \neq 0}} \frac{1}{NI^s} \\
&= \prod_{\mathfrak{p} \textit{ prime ideal } \neq 0} \frac{1}{1 - N\mathfrak{p}^{-s}} \\
&= \prod_{p \textit{ prime of } \mathbb{Z}} \frac{1}{F_p(p^{-s})} \qquad \textit{This follows from KD}
\end{aligned}$$

Here $F_p \in \mathbb{Z}[x]$ *is of degree* d *for* $p \nmid \Delta_K$ *and of degree* $< d$ *for* $p | \Delta_K$. *These are degree* d *L-functions.*

Example 2.1. *Take* $K = \mathbb{Q}(i)$, $\mathcal{O} = \mathbb{Z}[i]$ *Gaussian integers, and* $\mathcal{O}^\times = \{\pm 1, \pm i\}$ *units.*

As for Riemann ζ,

$$\begin{aligned}
\zeta_K(s) &= \sum_{\substack{I \subset \mathbb{Z}[i] \\ I \neq 0}} \frac{1}{NI^s} \\
&= \sum_{\substack{0 \neq \alpha \in \mathbb{Z}[i] \\ \bmod \mathbb{Z}[i]^\times}} \frac{1}{(\alpha\overline{\alpha})^s} \qquad \text{Since } \mathbb{Z}[i] \text{ is a PID} \\
&= \frac{1}{4} \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{0\}} \frac{1}{(m^2 + n^2)^s}.
\end{aligned}$$

The same computation as before (for RZF) gives that

$$\frac{2^s}{\pi^s} \Gamma(s) \zeta_K(s) = \text{Mellin transform of } \frac{\Theta(x) - 1}{4}$$

and

$$\begin{aligned}\Theta(x) &= \sum_{m,n\in\mathbb{Z}} e^{-\pi(m^2+n^2)x} \\ &= \sum_m e^{-\pi m^2 x} \sum_n e^{-\pi n^2 x} \\ &= \frac{1}{\sqrt{x}}\frac{1}{\sqrt{x}}\Theta\left(\frac{1}{x}\right).\end{aligned}$$

This trick as before gives a functional equation for $\zeta_{\mathbb{Q}(i)}(s)$. For general number fields, the extra statement we need is a generalised Poisson summation formula:

Let $V = \mathbb{R}^d$, $f : V \to \mathbb{C}$ decaying fast. Take V^* the dual vector space, and define the Fourier transform $\mathcal{F}f : V^* \to \mathbb{C}$ by

$$(\mathcal{F}f)(\underline{m}) = \int_V e^{-2\pi i\langle m,n\rangle} f(\underline{n})d\underline{n}.$$

Take $\Gamma \subset V$ a rank d lattice. Then

$$\sum_{\underline{n}\in\Gamma} f(\underline{n}) = \frac{1}{\mathrm{vol}(V/\Gamma)} \sum_{\underline{m}\in\Gamma^*} (\mathcal{F}\hat{f})(\underline{m}).$$

Use this to compare $\sum_{I\neq 0} \frac{1}{NI^s}$ to $\sum_{\substack{\alpha\in\mathcal{O}\\ \alpha\neq 0}} \frac{1}{N\alpha^s}$. This will involve

- the class number, $h = \#\{\text{ideals}/\text{principal ideals}\}$ and
- units, roots of unity,

If we have K a number field of degree $[K : \mathbb{Q}] = d = r_1 + 2r_2$, then

- $r_1 = \#$real embeddings $K \hookrightarrow \mathbb{R}$
- $r_2 = \#$pairs of non-real embeddings $K \hookrightarrow \mathbb{C}$.

Then $\mathcal{O} \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^d$ is a lattice.

After these considerations, we find that Poisson summation gives that

Theorem 2.2. *We have that $\zeta_K(s)$ is meromorphic on $\mathbb{C}$, it has a simple pole at $s = 1$, a residue at $s = 1$ of value*

$$\frac{2^{r_1}(2\pi)^{r_2}hR}{\#\text{roots of unity in } K \cdot \sqrt{|\Delta_K|}}.$$

The above expression for the value of the residue is called the class number formula, where h is again the class number, and R is the regulator (of units). Further, $\zeta_K(s)$ satisfies the functional equation,

$$\hat{\zeta}_K(1-s) = \hat{\zeta}_K(s).$$

Exercise 2.1 (Answer on MO 218759)**.** *If $[K : \mathbb{Q}] = d$, and K is Galois, then there exists infinitely many primes that 'split completely in K' (i.e. they have the maximal possible number of primes above them, and $e = f = 1$), and have density $\frac{1}{d}$.*

3 Dirichlet L-functions

Within this section, we will show that we can relate Dirichlet L-functions and the Dedekind zeta function over a cyclotomic field. First we begin with some standard definitions.

Definition. *Let $n \geq 2$. Then a (mod n) Dirichlet character is a group homomorphism*

$$\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times,$$

and they form a group $\widehat{(\mathbb{Z}/n\mathbb{Z})}^\times$. The two main invariants of a character are:

- ***Order of** χ: the smallest such d such that $\chi^d = 1$, so χ maps to the d^{th} roots of unity. Those characters where $d = 2$ are called quadratic.*
- ***Modulus of** χ: the smallest $m|n$ such that $\exists \chi_0 : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ such that $\chi(a) = \chi_0(a)$ for all a such that $(a, n) = 1$. We extend $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ to*

  $$\chi : \mathbb{Z} \to \mathbb{C}$$

  by

  $$\chi(a) = \begin{cases} \chi_0(a) & (a, m) = 1 \\ 0 & \textit{o.w.} \end{cases}$$

  Then χ is almost a homomorphism (it is except on 'bad' primes) - but it is totally multiplicative.

Example 3.1. *For $n = 1$, $\chi(a) = 1$ for all $a \in \mathbb{Z}$, which we call the trivial character. It has order 1 and modulus 1. We write $\mathbb{1}$ for the trivial character.*

Example 3.2. *For $n = 3$, then $\chi : (\mathbb{Z}/3\mathbb{Z})^\times \to \mathbb{C}^\times$ and $(\mathbb{Z}/3\mathbb{Z})^\times \cong C_2$ so there are 2 characters. The first is the trivial character $\mathbb{1}$, and the second is*

$$\chi_3(n) = \begin{cases} 1 & a \equiv 1 \mod 3 \\ -1 & a \equiv 2 \mod 3 \\ 0 & a \equiv 0 \mod 3 \end{cases}.$$

Then χ_3 has modulus 3 and order 2.

For $n = 4$, there are also 2 characters, with the non-trivial being

$$\chi_4(a) = \begin{cases} 1 & a \equiv 1 \mod 4 \\ -1 & a \equiv 3 \mod 4 \\ 0 & a \textit{ even.} \end{cases}$$

Then χ_4 has order 2 and modulus 4.

Example 3.3. *When $n = 5$ then the domain is isomorphic to C_4 so*

$$\chi_5 : C_4 \to \mathbb{C}^\times,$$

so we could send $2 \mapsto i$ then χ_5^2, $\bar{\chi_5} = \chi_5^3$ and $\chi_5^4 = \mathbb{1}$ are the possible characters.

	1	5	7	11
$\mathbb{1}$	1	1	1	1
χ_3	1	-1	1	-1
χ_4	1	1	-1	-1
$\chi_3\chi_4$	1	-1	-1	1

Example 3.4. *$n = 12$ then there are 4 characters (isom to $C_2 \times C_2$), and*

Note that χ_3 looks like $\left(\frac{-3}{\cdot}\right)$ and has modulus 3, order 2; χ_4 is $\left(\frac{-1}{\cdot}\right)$ and has modulus 4, order 2; $\chi_3\chi_4$ is $\left(\frac{3}{\cdot}\right)$ and has modulus 12 order 2.

Recall that in the particular case $q = 2$, we have

$$\left(\frac{n}{2}\right) = \begin{cases} 0 & n \not\equiv 1 \mod 4 \\ 1 & n \equiv 1 \mod 8 \\ -1 & n \equiv 5 \mod 8 \end{cases}$$

$$= \begin{cases} 0 & 2 \text{ ramifies in } \mathbb{Q}(\sqrt{n}) \\ 1 & 2 \text{ splits in } \mathbb{Q}(\sqrt{n}) \\ -1 & 2 \text{ inert in } \mathbb{Q}(\sqrt{n}). \end{cases}$$

Definition. *We define the Dirichlet L-function modulus m to be, for a Dirichlet character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$,*

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}}.$$

These are local polynomials: 1 if $p|m$ and $1 - \chi(p)T$ if $p \nmid m$.

Further $|\chi(n)| \le 1$ thus they are absolutely convergent on $\mathrm{Re}(s) > 1$. In fact, for $\chi \neq \mathbb{1}$, using some yoga called Abel summation and the fact that

$$\left| \sum_{n=A}^{B} \chi(n) \right| \le m$$

for all A, B, the L-series converges (not absolutely) on $\mathrm{Re}(s) > 0$.

Theorem 3.1. *$L(\chi, s)$ is entire for χ not the trivial character. The completed form is*

$$\hat{L}(\chi, s) = \left(\frac{m}{\pi}\right)^{s/2} \Gamma\left(\frac{s + \lambda}{2}\right) L(\chi, s),$$

and it satisfies the functional equation

$$\hat{L}(\chi, 1 - s) = w \cdot L(\bar{\chi}, s)$$

where bar is complex conj, with

$$\lambda = \begin{cases} 0 & \chi(-1) = 1, \chi \text{ even} \\ 1 & \chi(-1) = -1, \chi \text{ odd}. \end{cases}.$$

Note that $w = 1$ for Riemann zeta but in this case is defined as

$$w = \frac{1}{\sqrt{m}} \sum_{a=0}^{m-1} \chi(a) \zeta_m^a,$$

the $\zeta_m = e^{\frac{2\pi i}{m}}$ are primitive m^{th} roots of unity. Note that this is the Gauss sum and $w \in \mathbb{C}^\times$ with $|w| = 1$.

Proof. The outline of the proof uses Poisson summation with

$$\begin{aligned} e^{-\pi(mx+a)^2 t} &\quad \text{even } \chi \\ e^{-\pi x^2 t} &\quad \text{odd } \chi. \end{aligned}$$

□

We now want to show that the Dedekind zeta satisfies

$$\zeta_{\mathbb{Q}(\zeta_m)}(s) = \prod L(\chi, s),$$

where the χ vary all over $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$.

Note that a corollary of this is that $L(\chi, 1) \neq 0$ for all non-trivial characters: from the Dedekind zeta product form above, there is a simple pole in LHS at $s = 1$ and on the right we have $L(\mathbb{1}, s) = \zeta(s)$ (which has the pole) and all the other characters give analytic L-functions at $s = 1$. This proves Dirichlet's theorem on primes in arithmetic progressions:

Take

$$\underline{p} = \{\text{primes } p \equiv a \mod m\} \quad \text{for } (a, m) = 1,$$

then consider

$$\sum_{p \in \underline{p}} \frac{1}{p^s}.$$

Since we can consider

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + \{\text{terms analytic at } s = 1\},$$

we can say

$$\sum_{p \in \underline{p}} \frac{1}{p^s} = \frac{1}{\varphi(m)} \sum_\chi \overline{\chi(a)} \log L(\chi, s) + \{\text{analytic at } s = 1\}.$$

Note that all the functions are analytic except when we are considering Riemann zeta which contributes a pole.

The LHS diverges for $s = 1$ because of the contribution from $L(\mathbb{1}, s)$ on the right which then gives a growth independent of the choice of a. Thus $\underline{p}$ is infinite and has density $\frac{1}{\varphi(m)}$.

4 Cyclotomic Fields

Fix $m \geq 1$ and assume that m is not twice an odd number. Then $K = \mathbb{Q}(\zeta_m)$ is the field of interest, and is called the m^{th} cyclotomic field, where $\zeta_m = e^{\frac{2\pi i}{m}}$ and the degree of K over $\mathbb{Q}$ is $\varphi(m)$:

Clearly $K = \mathbb{Q}(\text{roots of } x^m - 1) = \mathbb{Q}(\text{roots of } \Phi_m)$ where Φ_m is the m^{th} cyclotomic polynomial, $\Phi_1(x) = x - 1$,

$$x^m - 1 = \prod_{d|m} \Phi(d)$$

so $\deg \Phi_m = \varphi(m) = (\mathbb{Z}/m\mathbb{Z})^\times$.

Note that K is Galois over $\mathbb{Q}$.

Further, when $m = q^k$ then it is easy to verify that

- $\Phi_m(x+1) = x^{\varphi(m)} + \cdots + q$, and it is Eisenstein and hence irreducible. This in particular shows that $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$.
- $(q) = (1 - \zeta_m)^{\phi(m)}$ so we have equality as ideals in $\mathcal{O}_K$. Thus q is totally ramified in $K/\mathbb{Q}$.
- All other primes are $p \nmid \Delta_{x^m - 1} \implies$ are unramified in $K/\mathbb{Q}$ with residue degree

$$f = \text{order of } p \text{ in } (\mathbb{Z}/m\mathbb{Z})^\times.$$

Proof. We have that $p \equiv 1 \mod m$ iff m^{th} roots of unity are all contained in $\mathbb{F}_p^\times$. Equivalently, $\Phi_m = \frac{x^{q^k} - 1}{x^{q^{k-1}} - 1}$ splits completely over $\mathbb{F}_p$. Similarly, if $p^r \equiv 1 \mod m$ for some r, this is equivalent as above (except with $\mathbb{F}_{p^r}^\times$) and Φ_m has irreducible factors of degree dividing r over $\mathbb{F}_p$. Thus, since the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$ is the smallest such r, then $f = r$ by KD. $\square$

Now, in the general case, $m = q_1^{k_1} \ldots q_j^{k_j}$, the field that we consider $K = \mathbb{Q}(\zeta_m)$ is the compositum of $\mathbb{Q}(\zeta_{q_1}^{k_1}), \ldots, \mathbb{Q}(\zeta_{q_j}^{k_j})$, and in particular, if we look at ramification of primes, we see that these fields have no common overlap so

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \prod \varphi(q_i^{k_i}) = \varphi(m),$$

which proves that all Φ_m are irreducible.

Then if $p \nmid m$ then p is unramified in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ with residue degree $f_p = \text{order of } p \text{ in } (\mathbb{Z}/m\mathbb{Z})^\times$.

If otherwise $p|m$ so $m = p^k m_0$ so p ramifies in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ with ramification degree $e_p = [\mathbb{Q}(\zeta_{p^k}) : \mathbb{Q}] = p^{k=1}(p-1)$ and has residue degree $f_p = \text{order } p \mod m_0$.

4.1 ζ-function of $\mathbb{Q}(\zeta_m)$

Recall that

$$\zeta_K(s) = \prod_p F_p(p^{-s}).$$

Then

$$F_p(T) = (1 - T^{f_p})^{\frac{\varphi(m)}{e_p f_p}}$$

and recall that $1 - N\mathfrak{p}^{-s} = 1 - p^{-f_p s} = 1 - T^{f_p}$, and $\frac{\varphi(m)}{e_p f_p}$ is the number of primes above p. The degree of F_p is usually $\varphi(m)$ since most primes are unramified, and in general $\deg F_p = \varphi(m_0)$.

We can hence observe,

$$F_p(T) = \prod_{a \in (\mathbb{Z}/f_p\mathbb{Z})^\times} (1 - \zeta_{f_p}^a T)^{\frac{\varphi(m_0)}{f_p}} = \prod_{\chi:(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times} (1 - \chi(p)T).$$

Combining over all primes, we have shown that

$$\zeta_{\mathbb{Q}(\zeta_m)}(s) = \prod_{\chi:(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times} L(\chi, s).$$

Example 4.1. *Let $m = 12$, $K = \mathbb{Q}(\zeta_{12}) = \mathbb{Q}(i, \sqrt{-3})$, a biquadratic extension. It is also the splitting filed of $x^{12} - 1 = \Phi_{12}(x)$. Recall that we can write*

$$\begin{aligned} \Phi_{12}(x) &= \Phi_1\Phi_2\Phi_3\Phi_4\Phi_6\Phi_{12} \\ &= (x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1). \end{aligned}$$

Here are some local factors for $\zeta_{\mathbb{Q}(\zeta_{12})}(s)$:

		$F_2(T)$	$F_3(T)$	$F_5(T)$	$\dots$	$F_{13}(T)$
	$\zeta(s) = L(\mathbb{1}, s)$	$1-T$	$1-T$	$1-T$	$\dots$	$1-T$
$\times$	$L(\chi_3, s)$	$1+T$	1	$1+T$	$\dots$	$1-T$
$\times$	$L(\chi_4, s)$	1	$1+T$	$1-T$	$\dots$	$1-T$
$\times$	$L(\chi_{12}, s)$	1	1	$1+T$	$\dots$	$1-T$
$=$	$\zeta_{\mathbb{Q}(\zeta_{12})}(s)$	$1-T^2$	$1-T^2$	$(1-T^2)^2$	$\dots$	$(1-T)^4$

The prime decomposition is

$(2) = \mathfrak{p}_2^2$	$N\mathfrak{p}_2 = 4$	$e = 2, f = 2$	***ramified***
$(3) = \mathfrak{p}_3^2$	$N\mathfrak{p}_3 = 9$	$e = 2, f = 2$	***ramified***
$(5) = \mathfrak{p}_{5A}\mathfrak{p}_{5B}$		$e = 1, f = 2$	***partially split***[1]
$(13) = \mathfrak{p}_{13A}\mathfrak{p}_{13B}\mathfrak{p}_{13C}\mathfrak{p}_{13D}$			***totally split***[2].

[1] c.f. $x^4 - x^2 + 1 = (x^2 + 2x - 1)(x^2 - 2x - 1) \mod 5$

[2] c.f. $x^4 - x^2 + 1 = (x-2)(x-6)(x-7)(x-11) \mod 13$

4.2 Abelian extensions of $\mathbb{Q}$

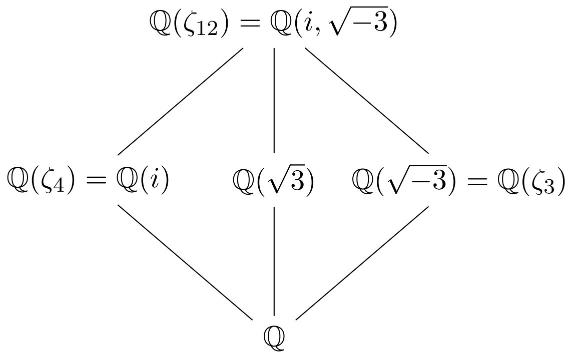


Figure 1: Extension map

We have the extension map figure 1. Note that we have the following decompositions,

$$\begin{aligned}
\zeta_{\mathbb{Q}(\zeta_{12})} &= \zeta \cdot L(\chi_3)L(\chi_4)L(\chi_{12}) \\
\zeta_{\mathbb{Q}(\zeta_4)} &= \zeta \cdot L(\chi_4) \\
\zeta_{\mathbb{Q}(\zeta_3)} &= \zeta \cdot L(\chi_3) \\
\zeta_{\mathbb{Q}(\sqrt{3})} &= \zeta \cdot L(\chi_{12}) = \zeta \cdot L(\left(\frac{3}{\cdot}\right)).
\end{aligned}$$

Theorem 4.1 (Kronecker-Weber)**.** *We say that $K/\mathbb{Q}$ is abelian if it is Galois with Gal($K/\mathbb{Q}$) abelian. Then*

$$K/\mathbb{Q} \text{ is abelian } \iff K \subset \mathbb{Q}(\zeta_m) \quad \text{for some } m$$

In fact, from representation theory (justified more later),

$$\iff \zeta_K(s) = \prod_{i=1}^{[K:\mathbb{Q}]} \text{Dirichlet } L\text{-fns}.$$

Generalisation

Due to Hecke: can we do the same type of procedure over a number field F in place of $\mathbb{Q}$? So we would fix a non-zero ideal $\mathfrak{m} \subset \mathcal{O}_F$ called a 'modulus'. Then we would define

$$L(\chi, s) = \sum_{\substack{I \subset \mathcal{O}_F \\ \text{ideal} \neq 0}} \chi(I) N I^{-s} = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p})(N\mathfrak{p})^{-s}},$$

with $\chi : I_{\mathfrak{m}} = \{\text{fractional ideals of } F \text{ prime to } \mathfrak{m}\} \to \mathbb{C}^\times$ of finite order,

$$\chi(I) = 1 \text{ on } P_{\mathfrak{m}} = \{\text{principal ideals } (\alpha) \text{ such that } \alpha \equiv 1 \mod \mathfrak{m}\}.$$

Then extend to all other ideals, by mapping them to 0.

$\mathbb{R}^\times \to \mathbb{C}^\times$	$x \mapsto \text{sgn}(x)^u \lvert x\rvert^{v+iw}$	$u \in \{0,1\}$
$\mathbb{C}^\times \to \mathbb{C}^\times$	$x \mapsto \left(\frac{x}{\lvert x\rvert}\right)^u \lvert x\rvert^{v+iw}$	$u \in \mathbb{Z}$.

Table 1: Possibilities for φ.

Example 4.2. $L(\mathbb{1}, s) = \zeta_F(s)$.

Hecke showed analytic continuation and a functional equation for these L-functions. Thus these are truly analogues to Dirichlet L-functions, but over F. There is a further slight generalisation, called Hecke characters and/or Grössencharakters. These allow $\chi|_{P_m} : \alpha \mapsto \mathbb{C}^\times$ instead of 1, to agree with

$$F^\times \hookrightarrow (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \to \mathbb{C}^\times$$

via some continuous homomorphism φ, cally 'infinity type'.

At real places, possibilities for φ (see Table 1) are just shifts.

Example 4.3.

$$\zeta(s-1) = \prod_p \frac{1}{1 - p \cdot p^{1-s}} = L(\chi, s),$$

with $\chi(p) = p$ the cyclotomic character.

This is a Hecke character with infinite typy $\mathbb{R}^\times \to \mathbb{C}^\times$, $z \mapsto |z|$. That is, takes generator $\pm n$ of an ideal (n) and maps it to n. The modern formulation is:

Hecke characters on F = continuous group homomorphisms,

$$\mathbb{A}_F^\times \to \mathbb{C}^\times \quad \text{with } F^\times \text{ in the kernel.}$$

Tate's thesis gives an alternative proof of meromorphic continuation and functional equation for Hecke characters using Fourier analysis on adeles.

5 Decomposition, inertia, Frobenius

Let K be a number field, $\mathfrak{p} \subset \mathcal{O}_K$ a prime (e.g. $\mathbb{Q}, (p)$). Then assume F/K is a finite Galois extension, $G = \text{Gal}(F/K)$, $|G| = [F : K] = d$.

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the primes above $\mathfrak{p}$ in F. Recall that if e is the ramification degree, f the residue degree, then here $efr = d$.

Remark (Fact 1). *G permutes the $\mathfrak{p}_i$ transitively.*

Definition. *We define the* ***decomposition group*** *of the primes $\mathfrak{p}_i$ as the stabiliser of $\mathfrak{p}_i$ in G. We write it as $D_{\mathfrak{p}_i}$, so*

$$D_{\mathfrak{p}_i} = \{\sigma \in \text{Gal}(F/K) : \sigma(\mathfrak{p}_i) = \mathfrak{p}_i\},$$

and has index r in G.

Then $D_{\mathfrak{p}_i}$ acts on the residue fields $\mathcal{O}_F/\mathfrak{p}_i \cong \mathbb{F}_{q^f}$ so we get

$$D_{\mathfrak{p}_i} \xrightarrow[\sigma \mapsto \bar{\sigma}]{\text{mod } \mathfrak{p}_i} \mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q) \cong C_f \quad \textit{cyclic, gen. by } x \mapsto x^q$$

with the map being the reduction map on automorphisms.

Remark (Fact 2). *This map is onto.*

Definition. *The kernel of $\sigma \mapsto \bar{\sigma}$ is the **inertia group** of $\mathfrak{p}_i$. Then*

$$I_{\mathfrak{p}_i} = \{\sigma \in D_{\mathfrak{p}_i} | \bar{\sigma} = id\}$$

that is they are the elements of G that map $\mathfrak{p}_i \to \mathfrak{p}_i$ that are invisible on $\mathcal{O}_F/\mathfrak{p}_i$. Then $I_{\mathfrak{p}_i} \overset{f}{\triangleleft} D_{\mathfrak{p}_i}$, and $|I_{\mathfrak{p}_i}| = e$.

Definition. *A **Frobenius element** at $\mathfrak{p}_i$,*

$$\mathrm{Frob}_{\mathfrak{p}_i} = \textit{any element of } D_{\mathfrak{p}_i} \textit{ that acts as } x \mapsto x^q \textit{ on } \mathcal{O}_F/\mathfrak{p}_i.$$

So G has a subgroup of index r, $D_{\mathfrak{p}_i}$. Inside $D_{\mathfrak{p}_i}$ there is a normal subgroup of index f, $I_{\mathfrak{p}_i}$. Inside $I_{\mathfrak{p}_i}$ there is the trivial normal subgroup of index e:

$$G \overset{r}{>} D_{\mathfrak{p}_i} \overset{f}{\triangleright} I_{\mathfrak{p}_i} \overset{e}{\triangleright} \{1\}.$$

By Galois theory, this corresponds to

$$K \frac{\mathfrak{p}\text{ split}}{r} K_1 \frac{\tilde{\mathfrak{p}}_i \text{ totally inert}}{f} K_2 \frac{\tilde{\mathfrak{p}}_i \text{ totally ramified}}{e} F.$$

Remark. *For $\tau \in G$,*

$$\begin{aligned} D_{\tau(\mathfrak{p}_i)} &= \{\sigma \in G | \sigma(\tau(\mathfrak{p}_i)) = \tau(\mathfrak{p}_i)\} \\ &= \{\tau\sigma\tau^{-1} | \sigma(\mathfrak{p}_i) = \mathfrak{p}_i\} \\ &= \tau D_{\mathfrak{p}_i} \tau^{-1}. \end{aligned}$$

Thus $D_{\mathfrak{p}_1}, \ldots, D_{\mathfrak{p}_r}$ are conjugate in G. It is then convenient to descend to K:

Definition. *Let F/K be Galois, $\mathfrak{p}$ prime of K. Then*

- $D_{\mathfrak{p}}$:= *decomposition group of some prime $\mathfrak{p}_i | \mathfrak{p}$. Therefore, this is defined up to conjugacy.*
- $I_{\mathfrak{p}}$:= *intertia group of some $\mathfrak{p}_i | \mathfrak{p}$, also defined up to conjugacy.*
- $\mathrm{Frob}_{\mathfrak{p}}$:= *Frob. element of $D_{\mathfrak{p}_i}$. This is defined up to conjugacy and modulo inertia.*

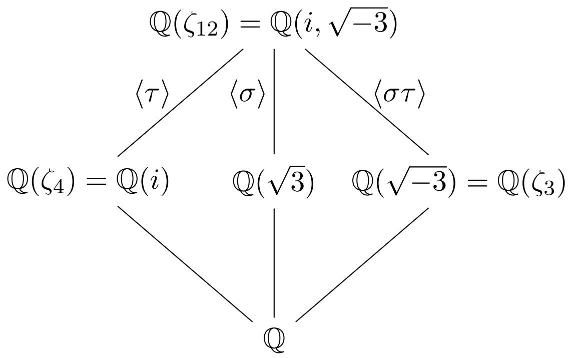


Figure 2: Extension map

Example 5.1. *Take $F = \mathbb{Q}(\sqrt{3}, i)$, the biquadratic extension, structure given in Figure 2, and $K = \mathbb{Q}$. Then the Galois group is isomorphic to $C_2 \times C_2$ generated by*

$$\sigma(i) = -i \qquad \sigma(\sqrt{3}) = \sqrt{3}$$
$$\tau(i) = i \qquad \tau(\sqrt{3}) = -\sqrt{3}.$$

We look at (2) in F/K. Then (2) is inert in $\mathbb{Q}(\sqrt{-3})$ so its inertia degree is 2 so $2|f$. Similarly it ramifies in $\mathbb{Q}(i)$ so $2|e$. (This is expanded in HW3). Thus $e = f = 2$ and $r = 1$ (since $F/K = 4$ and $(2) = \mathfrak{p}_2^2$ whose norm is 4. Hence, we have that

$$K \xrightarrow[r]{\mathfrak{p}\text{ split}} K_1 \xrightarrow[f]{\tilde{\mathfrak{p}}_i\text{ totally inert}} K_2 \xrightarrow[e]{\tilde{\mathfrak{p}}_i\text{ totally ramified}} F$$
$$\mathbb{Q} \overset{\text{no splitting}}{=} \mathbb{Q} \xrightarrow{\text{2 inert}} \mathbb{Q}(\sqrt{-3}) \xrightarrow{\text{2 ramifies}} F.$$

Then

$$D_2 = D_{\mathfrak{p}_2} = G, \qquad I_2 = I_{\mathfrak{p}_2} = \langle\sigma\tau\rangle, \qquad \mathrm{Frob}_2 = \tau \text{ or } \sigma.$$

In the last thing we have to choose anything that isn't in $I_2 = \langle\sigma\tau\rangle$.

Explicitly, write $\zeta = \zeta_3 = \frac{-1+\sqrt{-3}}{2}$; $\zeta^2 = -1 - \zeta$. Then

$$\mathcal{O}_F = \{a + bi + c\zeta + di\zeta | a, b, c, d \in \mathbb{Z}\}$$

and

$$\mathfrak{p}_2 = (1 + i) = \{a + bi + c\zeta + di\zeta | a, b, c, d \in \mathbb{Z}, a \equiv b, c \equiv d \mod 2\}.$$

Note that $\mathfrak{p}_2^2 = (2)$. Further,

$$\mathcal{O}_F/\mathfrak{p}_2 = \{\bar{0}, \bar{1}, \bar{\zeta}, \overline{1 + \zeta}\} \cong \mathbb{F}_4.$$

Consider $\sigma\tau$:

$\sigma\tau(\mathfrak{p}_2) = (1 - i) = \mathfrak{p}_2$, and $\sigma\tau$ fixes $0, 1, \zeta, 1 + \zeta$ so it's trivial on $\mathbb{F}_4$. Hence $\sigma\tau \in I_{\mathfrak{p}_2}$ - also note here that $I_2 = \mathrm{Gal}(F : \mathbb{Q}(\sqrt{-3}))$.

Also, $\tau(\mathfrak{p}_2) = \mathfrak{p}_2$ as τ fixes $1 + i$. Now τ fixes $0, 1$ and sends $\zeta \mapsto \zeta_2 \equiv 1 + \zeta$ (map is mod (2) and the congruence is mod $(\mathfrak{p}_2)$).

That is $\bar{\tau} : \mathbb{F}_4 \to \mathbb{F}_4$, $x \mapsto x^2$ so it acts on the residue field by squaring everything, and this is precisely what it means to be the Frobenius element for this prime, so $\tau = \mathrm{Frob}_2$. Thus $D_2 = \langle I_2, \mathrm{Frob}_2 \rangle = G$.

6 Galois Representations

Definition. *Take G a finite group. Then a d-**dimensional (complex) representation** of G is a group homomorphism,*

$$\rho : G \to \mathrm{GL}(d, \mathbb{C}) = \mathrm{GL}_d(\mathbb{C}) = \mathrm{GL}(V),$$

for V some complex d-dimensional vector space.

Example 6.1. *Suppose $G \cong C_4 = \langle g \rangle$. Then we could construct ρ via*

$$g \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

a rotation by $\pi/2$. Thus we 'represent G as a group of matrices'.

Definition. *When $G = \mathrm{Gal}(F/K)$, where F/K is some finite Galois extension, then we call the representation of this group a **Galois representation**,*

$$\rho : \mathrm{Gal}(F/K) \to \mathrm{GL}_d(\mathbb{C}),$$

or

$$\rho : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Gal}(F/K) \to \mathrm{GL}_d(\mathbb{C}).$$

*When F, K are number fields, then these representations are called **Artin** representations (over K).*

Definition. *To each such Artin representation, we can associate an L-function. Take*

$$\rho : \mathrm{Gal}(F/K) \to \mathrm{GL}(V),$$

an Artin representation. Then we define the (Artin) L-function,

$$L(\rho, s) = L(V, s) := \prod_{\mathfrak{p} \text{ prime of } K} F_{\mathfrak{p}}(N\mathfrak{p}^{-s}).$$

with

$$F_{\mathfrak{p}}(T) = \det\bigl(1 - \rho(\mathrm{Frob}_{\mathfrak{p}}^{-1})T | V^{I_{\mathfrak{p}}}\bigr).$$

Recall that $I_{\mathfrak{p}} = \{v \in V | \sigma(v) = v \; \forall \sigma \in I_{\mathfrak{p}}\}$. Also, note that mostly the inertia group is trivial - so it's not usually as scary as it looks. Thus for all but finitely many primes, $F_{\mathfrak{p}}(T)$ has degree d. It will have smaller degree for those which are ramified.

Exercise 6.1 (Do it!). *This is well-defined.*

Example 6.2. *Let $F = \mathbb{Q}(i)$, $K = \mathbb{Q}$. Then $G = \mathrm{Gal}(F/K) \cong C_2 = \langle 1, \sigma \rangle$. Recall that primes here fall in to 3 categories,*

$$p = \begin{cases} 2 & I_2 = G \\ 1 \mod 4 & I_p = \{1\}, D_p = \{1\}, \mathrm{Frob}_{\mathfrak{p}} = 1 \\ 3 \mod 4 & I_p = \{1\}, D_p = G, \mathrm{Frob}_{\mathfrak{p}} = \sigma. \end{cases}$$

As an example, take $G \to \mathbb{C}^\times = \mathrm{GL}(V_1)$, where $\dim V_1 = 1$. Then

$$1, \sigma \mapsto \mathrm{Id}\,.$$

So $V_1^{I_p} = V_1$ for all p and has dimension 1. Then we need to examine the characteristic polynomial of Frob_p:

$$\rho(\mathrm{Frob}_p) = \mathrm{Id} \quad \forall p, \qquad F_p(T) = \det(1 - \mathrm{Id} \cdot T) = 1 - T.$$

Thus the L-function $L(V_1, s) = \zeta(s)$ (unsurprisingly).

Now take a different rep, $G \to \mathbb{C}^\times = \mathrm{GL}(V_{-1})$, where $\dim V_{-1} = 1$ with

$$1 \mapsto \mathrm{Id}, \qquad \sigma \mapsto -\mathrm{Id}\,.$$

Then

$$V_{-1}^{I_p} = \begin{cases} 0 & p = 2 \\ V_{-1} & p > 2 \end{cases}.$$

Turning to the characteristic polynomials,

$$F_p(T) = \begin{cases} 1 & p = 2 \\ \det(1 - \mathrm{Id} \cdot T) = 1 - T & p \equiv 1 \mod 4 \\ \det(1 + \mathrm{Id} \cdot T) = 1 + T & p \equiv 3 \mod 4. \end{cases}$$

Therefore $L(V_{-1}, s) = L(\chi_4, s)$, where χ_4 is the Dirichlet character of conductor 4 (defined earlier on).

Final example of a rep: $G \to \mathrm{GL}(V)$ where V has dimension 2. Consider $V = \mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{C}$ - look at G acting on $\mathbb{Q}(i) = \mathbb{Q} \cdot 1 + \mathbb{Q} \cdot i$, $\mathbb{Q}$-linearly, and take the same matrices over $\mathbb{C}$. Thus

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \sigma \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Thus our space V decomposes as $V \cong V_1 \oplus V_{-1}$. We can see that $V^{I_p} = V_1^{I_p} \oplus V_{-1}^{I_p}$ and whatever determinant we are computing, it is going to be the product of determinants on the two subspaces. Thus,

$$L(V, s) = L(V_1, s) L(V_{-1}, s) = \zeta(s) L(\chi_4, s) = \zeta_{\mathbb{Q}(i)}(s).$$

In fact, any representation of $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong C_2$ *is*

$$V_1 \oplus \cdots V_1 \oplus V_{-1} \oplus \cdots \oplus V_{-1} = V_1^a \oplus V_{-1}^b,$$

so we will always get

$$\zeta(s)^a L(\chi_4, s)^b.$$

Question Why do we define Artin L-functions $L(V, s)$ like this, with

$$F_{\mathfrak{p}}(T) = \det\bigl(1 - \rho(\mathrm{Frob}_{\mathfrak{p}}^{-1})T | V^{I_{\mathfrak{p}}}\bigr)?$$

Write $G_K = \mathrm{Gal}(\bar{K}/K)$ where K is a number field. Then these are a collection of 'semi-good' reasons:

(1) $L(\mathbb{1}_{G_{\mathbb{Q}}}, s) = \zeta(s)$ where $\mathbb{1}_{G_{\mathbb{Q}}}$ is the trivial representation on $\mathrm{Gal}(\bar{Q}/Q)$. More generally, $L(\mathbb{1}_{G_{\mathbb{K}}}, s) = \zeta_K(s)$.

(2) Generally, 1-dimensional representations of $G_{\mathbb{Q}}$ correspond to Dirichlet L-functions. When K is a number field, we get Hecke L-functions of finite order.

(3) Suppose $[K : \mathbb{Q}] = d$ (not necessarily Galois) then K determines a natural d-dimensional representation V_K of $G_{\mathbb{Q}}$, the absolute Galois group of $\mathbb{Q}$. For example, let $K = \mathbb{Q}[X]/f(x)$ with roots $\alpha_1, \ldots, \alpha_d$. Then

$$V_K = \mathbb{C}\alpha_1 \oplus \cdots \oplus \mathbb{C}\alpha_d,$$

and the Galois group acts by permuting the basis elements $\alpha_1, \ldots, \alpha_d$. Then

$$V_K \cong \mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}} \mathbb{1}_{G_K},$$

and $\zeta_K(s) = L(V_K, s)$. The decomposition of V_K into irreducible representations leads to

$$\zeta_K(s) = \prod \text{Artin } L\text{-functions of irreps.}$$

(4) We have that (1) and (3) combine to give $L(\mathbb{1}_{G_K}, s) = L(\mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}} \mathbb{1}_{G_K}, s)$ and the same is true for any V of G_K in place of $\mathbb{1}_{G_K}$.

(5) The Brauer induction gives that (1)-(4) recovers all $L(V, s)$ uniquely from Dirichlet/Hecke L-functions, which shows that our definition of $F_{\mathfrak{p}}(T)$ is the only possible one, and gives meromorphic continuation of all $L(V, s)$ and the corresponding functional equation.

(6) Everything works in exactly the same way for non-finite image representations (elliptic curves etc.).

7 Special Case: $L(\chi, s)$

Theorem 7.1. *There is a bijection*

$$\{\textit{Dirichlet characters } \chi\} \longleftrightarrow \{1 - \textit{dim Artin reps } \rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times\}$$
$$\chi \mapsto \rho_\chi$$

such that

- χ *is of modulus m* $\iff$ ρ_χ *factors through* $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ *and not for smaller* $d|m$ $(\star)$.
- $L(\chi, s) = L(\rho_\chi, s)$.

Proof. Take χ of modulus m. Then

$$\rho_\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \underset{\cong}{\overset{\text{can.}}{\to}} (\mathbb{Z}/m\mathbb{Z})^\times \overset{\chi}{\to} \mathbb{C}^\times$$

where

$$\sigma : \zeta_m \mapsto \zeta_m^a \underset{\text{Artin map}}{\mapsto} a^{-1} \mapsto \chi(a)^{-1}.$$

Note that $p^{-1} \in (\mathbb{Z}/m\mathbb{Z})^\times$ corresponds to $\zeta_m \to \zeta_m^p$ which is Frob_p, (or in other words $p \leftrightarrow \mathrm{Frob}_p^{-1}$). Then χ of modulus m implies that it does not come from $(\mathbb{Z}/d\mathbb{Z})^\times$ for $d|m, d < m$ so this implies $(\star)$.

Kronecker-Weber gives that every representation of $G_\mathbb{Q} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ that factors through an abelian group, in particular every 1-dim one, ρ, factors through some $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Thus $\rho = \rho_\chi$ for some χ.

Finally we need to compare L-functions - we do this by separately considering 'good' and 'bad' primes. For $p \nmid m$, $L(\chi, s)$ has

$$F_p(T) = 1 - \chi(p)T, \quad \text{for } \chi(p) \in \mathbb{C}^\times, p \in (\mathbb{Z}/m\mathbb{Z})^\times.$$

Also, $L(\rho_\chi, s)$ has $F_p(T) = 1 - \rho_\chi(\mathrm{Frob}_p^{-1})T$ (inertia at p is trivial because p is unramified in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$). So $\rho_\chi(\mathrm{Frob}_p^{-1}) = \chi(p)$. For $p|m$, $L(\chi, s)$ has $F_p(T) = 1$ (as $p|m$ implies $\chi(p) = 0$ since this is how we extend characters).

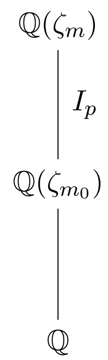


Figure 3: Extension Diagram for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$.

Since χ has modulus m (it is primitive), ρ_χ does not factor through $\mathrm{Gal}(\mathbb{Q}(\zeta_{m_0})/\mathbb{Q})$. Thus I_p acts non-trivially on $V_\chi(\cong \mathbb{C})$. Then we also note $V_\chi^{I_p} = 0 \implies F_p(T) = 1$. $\square$

Remark. *The same result holds for the one-to-one correspondence*

$$\textit{Hecke chars of finite order over } K \overset{1:1}{\longleftrightarrow} \textit{1-dim reps } G_K \to \mathbb{C}^\times.$$

The proof of this doesn't use Kronecker-Weber, but instead uses the full force of global CFT.

8 Permutation representations and Dedekind ζ

Let F/K be a finite Galois extension, with $G = \mathrm{Gal}(F/K)$. Then there are 1-1 correspondences (one from basic group theory and the Galois correspondence)

Transtive G-sets	$\overset{1:1}{\longleftrightarrow}$	Sbgrps of G up to conj		$\overset{1:1}{\longleftrightarrow}$	flds $K \subset M \subset F$ up to isom/K
X	$\leftarrow\!\shortmid$	Stabiliser (of an elmt) (of an elmt)	H	$\mapsto$	F^H
G/H	$\leftarrow\!\shortmid$	H	$\mathrm{Gal}(F/M)$	$\leftarrow\!\shortmid$	M.

Here $G/H = \{\text{left cosets } g_1H \dots g_dH \text{ with left mult action}\}$.

If $[M : K] = d$ then we find a transitive G-set X of size d. Or, it can be thought of as a $\mathrm{Gal}(\bar{K}/K)$-set which does not depend on F.

$$\begin{array}{ccc} F & & \\ \Big| & & \\ M & \rightsquigarrow & X = G/H \\ \Big| & & \\ K & & \end{array}$$

Explicitly, if $M = K(\alpha)$, α the root of some irreducible degree d-polynomial $f(x) \in K[x]$. Then set $H = \mathrm{Stab}_G(\alpha)$ and

$$\begin{aligned} X = X_{M/K} &= \{\text{roots of } f\} \circlearrowleft G \\ &\overset{1:1}{=} \{K - embeddings\ M \hookrightarrow \bar{K}\} \circlearrowleft G_K. \end{aligned}$$

Example 8.1. *Let $G = S_3$, $K = \mathbb{Q}$, $F = \mathbb{Q}(\zeta_3, \sqrt[3]{m})$.*

*Take a G-set X of size d. Then we get out a d-dim **permutation representation** $\mathbb{C}[X]$ - for the basis take elements of X and let G permute them.*

Fields M	SubGrps H	G-sets X	Acts $\circlearrowright$
$\mathbb{Q}$	S_3	$\cdot$	G acts trivially
$\mathbb{Q}(\zeta_3)$	C_3	$\cdot\ \cdot$	G acts through $S_3/C_3 \cong C_2$.
$\mathbb{Q}(\sqrt[3]{m})$	C_2	$\therefore$	G acts as $S_3 \circlearrowright \{1,2,3\}$
F	$\{1\}$	$\because\!\therefore$	Regular action (left mult).

Table 2: Galois correspondence for Exercise 8.1

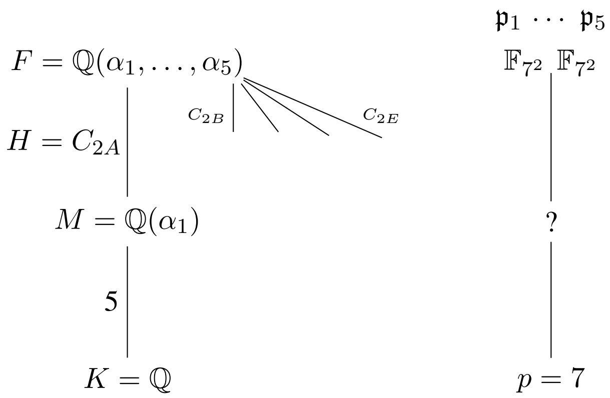
Note that any G-set X can be written as a union of transitive G-sets,

$$X = X_1 \amalg X_2 \amalg \dots$$

so $\mathbb{C}[X] \cong \mathbb{C}[X_1] \oplus \mathbb{C}[X_2] \oplus \cdots$*, so it's enough just to consider transitive ones.*

[Aside: Prime decomposition in arbitrary extensions.]

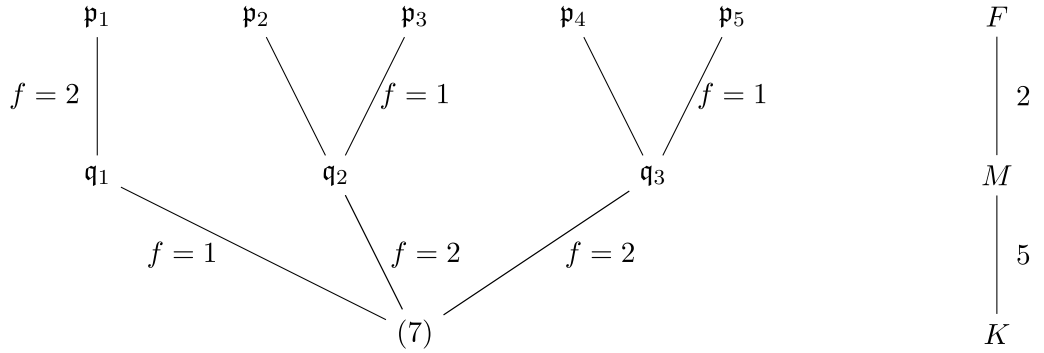
Example 8.2. *Let* $K = \mathbb{Q}$*,* $F = \mathbb{Q}$*(roots,* α_i *of* $x^5 - 5x^2 - 3$*), so* $G = \mathrm{Gal}(F/K) \cong D_5$*. Then*



Let's consider $D_{\mathfrak{p}_1} \in F/K$ *so* $D_{\mathfrak{p}_1} = C_{2A}$ *say, and* $I_{\mathfrak{p}_1} \in F/K$ *with* $I_{\mathfrak{p}_1} = \{1\}$*. In the top 'layer'* F/M*:*

$$D_{\mathfrak{p}_i}^{F/M} = D_{\mathfrak{p}_i}^{F/K} \cap H = \begin{cases} C_{2A} & i = 1 \leftarrow f_{\mathfrak{p}_1}^{F/M} = 2 \\ 1 & i = 2,3,4,5 \leftarrow f_{\mathfrak{p}_i}^{F/M} = 1. \end{cases}$$

Recall that $H = C_{2A}$ *and* $D_{\mathfrak{p}_1} \in \{C_{2A}, \dots, C_{2E}\}$*. Since the* f*'s are multiplicative in towers (see HW3), we have that*

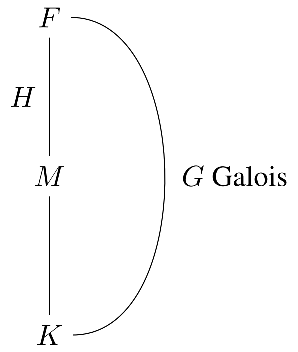


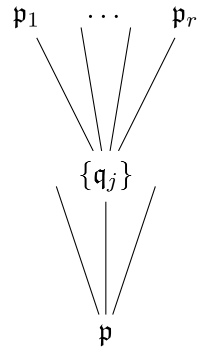
In practice of course we go the other way:

$$x^5 - 5x^2 - 3 = (x-1)(x^2+3x-2)(x^2-2x+2) \mod 7$$

therefore $(7) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$ *with* $f = 1, f = 2, f = 2$ *respectively in* M/K*. This implies that the decomposition group of* 7 *in* F/K*,* $D_7^{F/K} = C_2$ *(and not* C_1, C_5, D_5*).*

Proposition 8.1. *Let* K *be a number field,*





So $D_i = D_{\mathfrak{p}_i}^{F/K} < G$*,* $I_i = I_{\mathfrak{p}_i}^{F/K} \lhd D_i$*. So now write* $I = I_1, D = D_1, Frob_{\mathfrak{p}} \in D$*.*

(i) $D_{\mathfrak{p}_i}^{F/M} = D_i \cap H, I_{\mathfrak{p}_i}^{F/M} = I_i \cap H$

(ii) In M/K*, primes* $\mathfrak{q}_j|\mathfrak{p}$ *are in a 1-1 correspondence with 'double cosets'* $Dg_iH \in D\backslash G/H$*. They are also in a 1-1 correspondence with orbits of* D *on* G/H*. Each orbit has length* e_jf_j *(*e_j *the ramification and* f_j *the residue degree of* $\mathfrak{q}_j$ *in* M/K*) and is a union of* f_j I*-orbits of length* e_j *cyclically permuted by* $\mathrm{Frob}_{\mathfrak{p}}$ *.*

Proof. (i) is clear. (ii) By considering how H acts on $\{\mathfrak{p}_i\}$, we see that the orbits are in a 1-1 correspondence with $\mathfrak{q}_j$ and the stabilisers are $D_{\mathfrak{p}_i}^{F/M}$. Now, how does H act on G/D? Orbits are now in 1-1 correspondence with the double cosets, and stabilisers are $D_i \cap H$. By (i) the stabilisers are equal, so the orbits are the same. The rest of the proposition is bookwork. □

Definition. *The relative ζ-function is*

$$\zeta_{M/K}(s) = \prod_{\mathfrak{q} \subset \mathcal{O}_M} \frac{1}{1 - N_{M/K}(\mathfrak{q}^{-s})}.$$

Note that this is equal to ζ_M when $K = \mathbb{Q}$.

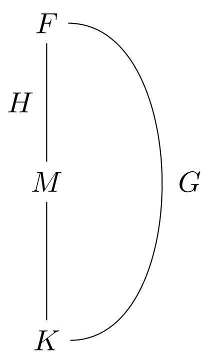
Theorem 8.2. *Let M/K be a finite extension. Then*

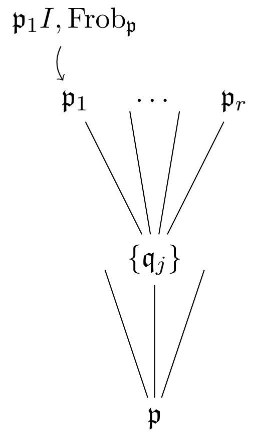
$$\zeta_{M/K}(s) = L(\mathbb{C}[X_{M/K}], s).$$

The RHS is the Artin L-function for the representation $\mathbb{C}[X_{M/K}] \circlearrowleft \mathrm{Gal}(\bar{K}/K)$.

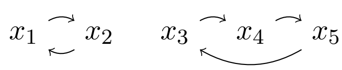
On the level of local polynomials, for every prime $\mathfrak{p}$ of K,

$$\prod_{\mathfrak{q}|\mathfrak{p}} (1 - T^{f_\mathfrak{q}}) \overset{\text{Thm}}{=} \det\bigl(1 - \mathrm{Frob}_\mathfrak{p}^{-1} T | \mathbb{C}[X_{M/K}]^{I_\mathfrak{p}}\bigr).$$





Proof. Recall that if X is a G-set then we have the representation $\mathbb{C}[X]^G \cong \mathbb{C}^{\#\text{orbits}}$. For example if



then $\mathbb{C}^G = \langle x_1 + x_2, x_3 + x_4 + x_5 \rangle$. As a D-set,

$$X_{M/K} = G/H = \coprod_{Dg_iH} D/D \cap g_j H g_j^{-1}.$$

Recall that I acts with f_i orbits of size $I \cap g_i H g_i^{-1}$ and they are cyclically permuted by $\mathrm{Frob}_\mathfrak{p}$. Therefore $\mathbb{C}[G/H]^I \cong \oplus_j \mathbb{C}^{f_j} \circlearrowleft \mathrm{Frob}_\mathfrak{p}$ cyclically (and therefore the inverse of Frob as well). Therefore,

$$\det\bigl(1 - \mathrm{Frob}_\mathfrak{p}^{-1} T | \mathbb{C}[G/H]^{I_\mathfrak{p}}\bigr) = \prod_j (1 - T^{f_j}) = \text{local factor of } \zeta_{M/K}(s) \text{ at } \mathfrak{p}.$$

□

9 Characters and Induction

There is the topic of character theory that says for G finite, $\rho : G \to \mathrm{GL}(V)$, there exists an object called a 'character' that encodes information about ρ.

Definition. *The **character** of V (or of ρ) is*

$$\chi_\rho = \chi_V : G \to \mathbb{C},$$

where $g \mapsto \mathrm{tr}(\rho(g))$.

Then note that $\chi_V(e) = \dim V$ and for ρ a one dimensional representation then '$\chi_\rho = \rho$'. Two conjugate elements have the same trace so characters are class functions.

Definition. *We have the following **inner product**,*

$$\langle \chi_V, \chi_W \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \overline{\chi_W(g)}.$$

Example 9.1. *Let $V = \mathbb{C}[X]$ be a permutation rep. Then*

$$\chi_\rho = \chi_V = \#\{\textit{fixed points under } V\} = \#\{x \in X : g \cdot x = x\}.$$

Example 9.2. *If $G = S_3$ which acts naturally on $X = \{1, 2, 3\}$. Then if $V = \mathbb{C}[X]$, we have that the conjugacy classes, $\mathcal{C} = \{[e], [(1, 2)], [(1, 2, 3)]\}$. Thus*

$$\chi_V = (3, 1, 0) : \mathcal{C} \to \mathbb{C}.$$

To examine the inner product:

$$\langle \chi_V, \chi_V \rangle = \frac{1}{6} [3 \cdot 3 \cdot 1 + 1 \cdot 1 \cdot 3 + 0] = 2.$$

Theorem 9.1. *Suppose G is a finite group, $\mathcal{C} = \{$conj classes$\}$, and $\mathcal{I} = \{$irreps $V_1, V_2, \dots\}$ up to isomorphism. Then*

- $|\mathcal{I}| = |\mathcal{C}|$, $\dim V_i$ *divides* $|G|$, $\sum_{i=1}^k \dim V_i^2 = |G|$.
- *Complete reducibility: every representation can be written*

  $$V \cong V_1^{\oplus n_1} \oplus \cdots \oplus V_k^{\oplus n_k}$$

  some $n_i \geq 0$ unique, V_i irreducible.
- *If $W = V_1^{\oplus m_1} \oplus \cdots \oplus V_k^{\oplus m_k}$, $m_i \geq 0$, then*

  $$\langle \chi_W, \chi_V \rangle = \langle \chi_V, \chi_W \rangle = \sum_{i=1}^k n_i m_i = \dim_{\mathbb{C}} \mathrm{Hom}_G(V, W).$$

  So in particular,

- $\langle \chi_V, \chi_V \rangle = \sum_{i=1}^k n_i^2$
- *V is irreducible* $\iff \langle \chi_V, \chi_V \rangle = 1$.
- $\langle \chi_{V_i}, \chi_{V_j} \rangle = \delta_{ij}$.

- $\chi_V + \chi_W = \chi_{V \oplus W}$
- $\chi_V \chi_W = \chi_{V \otimes W}$
- $\overline{\chi_V} = \chi_{V^\star}$ *- the character of the dual rep* $g \mapsto (\rho(g)^t)^{-1}$.

Example 9.3. *G is abelian if and only if $|\mathcal{C}| = |G|$ and $|\mathcal{I}| = |G|$. Further*

$$\sum \dim^2 = |G| \implies \textit{all } V_i \in \mathcal{I} \textit{ are 1-dimensional}.$$

We also have that

$$\{\textit{irreps of } G\} = \hat{G} = \mathrm{Hom}(G, \mathbb{C}^\times).$$

For any group G,

$$\{\textit{1-dim reps of } G\} = \hat{G} = \widehat{\frac{G}{[G,G]}},$$

where $\frac{G}{[G,G]}$ is the maximal abelian quotient of G, so

$$\#\{\textit{1-dim reps}\} = (G : [G,G]).$$

Example 9.4. *Let $G = S_4$, so $\mathcal{C} = \{e, [(1,2)], [(1,2,3)], [(1,2,3,4)], [(1,2)(3,4)]\}$ and $|\mathcal{I}| = 5$. So every rep of S_4 has the form*

$$V_1^{\oplus n_1} \oplus \cdots \oplus V_5^{\oplus n_5}.$$

We have 5 irreps ρ_i of dimension 1,1 (from $G/[G,G] = S_4/A_4 = C_2$) and three others of currently unknown dimensions. However

$$\sum_{i=1}^{5} \dim \rho_i^2 = |G| = 24 \implies 1 + 1 + 2 + 3 + 3.$$

Then we have characters from the following representations representations,

- χ_{ρ_1}*:* $\rho_1 = \mathbb{1} : S_4 \to \mathrm{GL}_1(\mathbb{C})$ *the trivial rep so* $\chi_{\rho_1} = (1,1,1,1,1)$.
- χ_{ρ_2}*:* ρ_2 *is the sign representation, so* $\chi_{\rho_2} = (1,-1,1,-1,1)$.
- χ_{ρ_4}*:* ρ_4 *comes from S_4 acting on $\{1,2,3,4\}$. Call this representation π then $\chi_\pi = (4,2,1,0,0)$ shows number of fixed points. This is reducible and we get that the inner product: $\langle \chi_\pi, \chi_\pi \rangle = 2$. Further*

  $$\langle \chi_\pi, \chi_{\rho_1} \rangle = 1 \implies \pi \cong \mathbb{1} \oplus \rho_4.$$

  Then $\chi_{\rho_4} = \chi_\pi - \chi_{\mathbb{1}} = (3,1,0,-1,-1)$.

- χ_{ρ_5}*: we get this by taking the product of* $\chi_{\rho_2}\chi_{\rho_4} = (3, -1, 0, 1, -1)$.
- *Finally* $\chi_{\rho_3} = (2, 0, -1, 0, 2)$. *We can get this in a number of ways: orthogonality, lifting from* $S_4/V_4 \cong S_3$*, from* $\chi_{\mathbb{C}[G]} = \sum_{i=1}^{5} \dim \rho_i \chi_{\rho_i}$*, or from* $\chi_5\chi_5$ *and reducing it.*

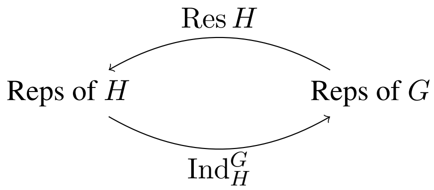
In total, this gives the character table

	e	$[(1,2)]$	$[(1,2,3)]$	$[(1,2,3,4)]$	$[(1,2)(3,4)]$
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	1	-1

Alternatively, we could have recovered all the characters using induction:

Theorem 9.2. *Let* $H < G$ *be a subgroup of index* d*. There are maps*

n-dim $\leftarrow$ n-dim



n-dim $\mapsto$ dn-dim

such that for all reps $\rho : G \to \mathrm{GL}(V)$*,* $\sigma : H \to \mathrm{GL}(W)$*.*

- *Frobenius Reciprocity holds:* $\langle V, \mathrm{Ind}\, W\rangle_G = \langle \mathrm{Res}\, V, W\rangle_H$.
- $\mathrm{Res}_H V =$ *same* V *with* H *action, i.e.*

$$\chi_{\mathrm{Res}_H V}(h) = \chi_V(h).$$

- $\mathrm{Ind}_H^G W = \{f : G \to W : f(hg) = \sigma(h)f(g)\ \forall h \in H, g \in G\}$*, and* $g \in G$ *acts by* $f(x) \mapsto f(xg)$.

  These are 'complicated' requirements, so instead often we use the following formula for the character of the induction representation:

$$\chi_{\mathrm{Ind}_H^G W}(g) = \frac{1}{|G|}\sum_{x\in G} \chi_W^0(xgx^{-1}),$$

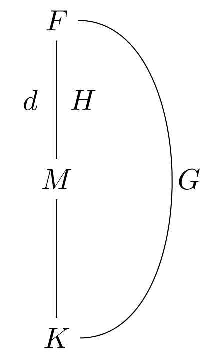
  where

$$\chi_W^0 = \begin{cases} \chi_W & \text{on } H \\ 0 & \text{else.} \end{cases}.$$

- $\mathrm{Ind}_H^G \mathbb{1} \cong \mathbb{C}[G/H]$.

10 Artin Formalism

Theorem 10.1 (L-functions are invariant under induction)**.** *If we have the following extension,*



and if $\rho : H \to \mathrm{GL}_d(\mathbb{C})$ is an Artin representation then

$$L(\rho, s) = L(\operatorname{Ind}_H^G \rho, s),$$

where $L(\rho, s)$ is a rep of G_M of dimension n, and $L(\operatorname{Ind}_H^G \rho, s)$ is a rep of G_K of dimension nd where $d = (G : H)$.

Proof. Same argument as for $\rho = \mathbb{1}$,

$$\operatorname{Ind}_H^G \rho = \mathbb{C}[G/H],$$

but instead of as a D-set

$$G/H = \amalg_{g_i \in D \backslash G/H} D/D \cap g_i H g_i^{-1},$$

we use Mackey's formula,

$$\operatorname{Res}_D \operatorname{Ind}_H^G \rho = \bigoplus_{g_i \in D \backslash G/H} \operatorname{Ind}_{D \cap g_i H g_i^{-1}}^D \rho^{g_i}.$$

□

Theorem 10.2 (Brauer Induction)**.** *Suppose we have a representation $\rho : G \to \mathrm{GL}_n(\mathbb{C})$. Then*

$$\chi_\rho = \sum_i n_i \operatorname{Ind}_{H_i}^G \chi_{\sigma(i)},$$

for some $n_i \in \mathbb{Z}$ (in particular can be negative), $H_i < G$ may be taken to be of the form cyclic$\times$p-group, $\sigma_i : H_i \to \mathbb{C}^\times$ are 1-dim representation with characters χ_i.

Remark. *This is used to construct character tables of groups.*

Corollary 10.2.1. *Every Artin L-function can be written in terms of L-functions of 1-dimensional representations,*

$$L(\rho, s) = \prod_i L(\sigma_i, s)^{n_i} \leftarrow \textit{Hecke L-fns.}$$

Recall that $\rho : G_K \to \mathrm{GL}_n(\mathbb{C})$ *then* $\sigma_i : G_{M_i} \to \mathbb{C}^\times$ *where* M_i/K *are finite extensions. In particular,* $L(\rho, s)$ *is meromorphic on* $\mathbb{C}$ *and satisfies functional equation under* $s \leftrightarrow 1 - s$.

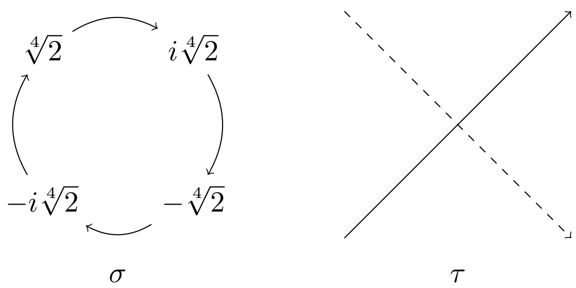
Conjecture (Artin)**.** *If* $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ *is an irreducible Artin rep,* $\rho \neq \mathbb{1}$*, then* $L(\rho, s)$ *has analytic continuation to* $\mathbb{C}$.

Remark. *The two properties:*

$$L(V_1 \oplus V_2, s) = L(V_1, s)L(V_2, s), \quad L(\mathrm{Ind}\, V, s) = L(V, s),$$

*that define L-functions uniquely from those of 1-dimensional representations are called **Artin formalism**.*

Example 10.1. *Let* $K = \mathbb{Q}$*,* $M = \mathbb{Q}(\sqrt[4]{2})$*, where* $\sqrt[4]{2}$ *is a root of* $x^4 - 2$*, and* $F = \mathbb{Q}(\sqrt[4]{2}, i)$ *which contains all four roots of* $x^4 - 2$*. Then the Galois groups contains maps,* σ *which permute the four roots cyclically, and a map* τ *acting as a reflection through complex conjugation:*



Then $G = \langle \sigma, \tau \rangle = \mathrm{Gal}(F/K) \cong D_4$.

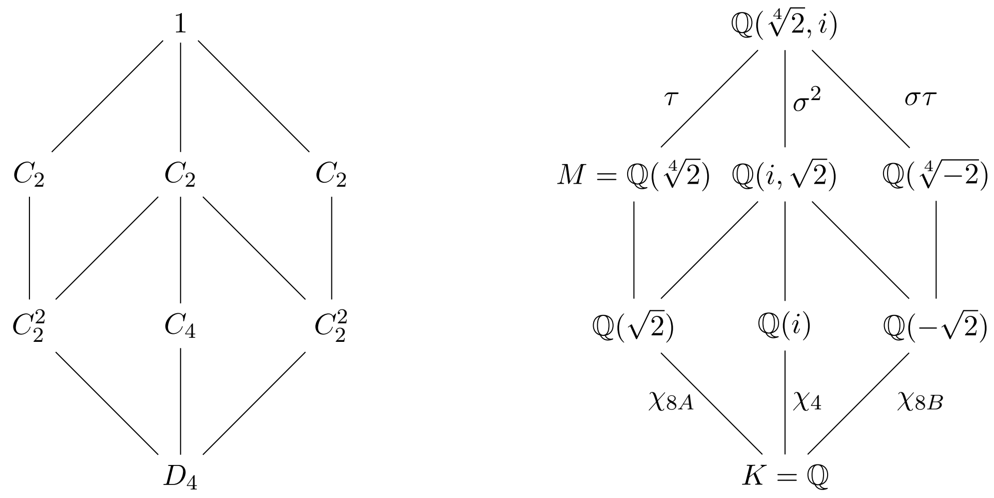


Figure 4: Galois correspondence between F/K and D_4.

Note[3] *that* $\sqrt[4]{-2} = \zeta_8 \cdot \sqrt[4]{2}$.
We also have a character table:

	1	σ^2	τ	σ	$\sigma\tau$
$\mathbb{1}$	1	1	1	1	1
χ_4	1	1	-1	1	-1
χ_{8A}	1	1	1	-1	-1
χ_{8B}	1	1	-1	-1	1
ψ	2	-2	0	0	0

Table 3: Characters of irreps of D_4.

The final character ψ *is the standard representation of* $D_4 \to \mathrm{GL}_2(\mathbb{C})$. *The commutator* $G' = Z(G) = \{e, \sigma^2\}$ *cuts out the maximal abelian extension of* $\mathbb{Q}$ *in* F. *Then*

$$F^{G'} = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8)$$

and

$$\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2,$$

has 1-dim reps $\mathbb{1}, \chi_4, \chi_{8A}, \chi_{8B}$ *where*

$$\chi_4 \leftrightarrow \binom{-1}{\cdot}, \chi_{8A} \leftrightarrow \binom{2}{\cdot}, \chi_{8B} \leftrightarrow \binom{2}{\cdot} \rightsquigarrow \textit{Dirichlet L-function.}$$

The only exceptional Dirichlet L*-function is the one coming from the 2-dim rep with character* ψ. *This yields* $L(\psi, s)$ *of degree 2,*

$$L(\psi, s) = 1 \cdot \frac{1}{1 - (3^{-s})^2} \cdot \frac{1}{1 + (5^{-s})^2} \cdot \frac{1}{1 - (7^{-s})^2} \cdots$$

[3]Also see D_4 on groupnames.org

The unit factor at the start comes from the case where we consider the prime 2*, then* $I_2 = D_4$ *and there are no invariants on* $\mathbb{C}^2$*. Then by examining the third factor more,* Frob_5 *is a rotation by* $\pi/2$ *so it has characteristic polynomial* $(1+T^2)$*, and the fourth gives* Frob_7 *is a reflection and has characteristic polynomial* $(1-T^2)$*. This can be expanded in to a Dirichlet series,*

$$L(\psi, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

with $a_p = \psi(\mathrm{Frob}_p)$ *at least on those* $p \nmid \Delta_F$*.*

Thus, all ζ*-functions of subfields of* F *are products of these, for example*

$$\zeta_{\mathbb{Q}(\sqrt[4]{2})}(s) = L(\mathbb{C}[G/\langle\tau\rangle], s),$$

where $\mathbb{C}[G/\langle\tau\rangle]$ *is the* G *set* $\{1,2,3,4\}$ *with natural* D_4 *action. So,*

$$\begin{aligned}\chi_{\mathbb{C}[G/\langle\tau\rangle]} &= (4,0,2,0,0)\\ &= (1,1,1,1) + (1,1,1,-1,-1) + (2,-2,0,0,0)\\ &= \mathbb{1} + \chi_{8A} + \psi,\end{aligned}$$

so

$$\begin{aligned}\zeta_{\mathbb{Q}(\sqrt[4]{2})}(s) &= L(\mathbb{1}, s)L(\chi_{8A}, s)L(\psi, s)\\ &= \zeta_{\mathbb{Q}(\sqrt{2})}(s) \cdot L(\psi, s).\end{aligned}$$

Similarly,

$$\begin{aligned}\zeta_{\mathbb{Q}(\sqrt[4]{-2})}(s) &= L(\mathbb{1}, s)L(\chi_{8B}, s)L(\psi, s)\\ &= \zeta_{\mathbb{Q}(\sqrt{-2})}(s) \cdot L(\psi, s),\end{aligned}$$

and

$$\begin{aligned}\zeta_{\mathbb{Q}(i,\sqrt{2})}(s) &= L(\mathbb{1}, s)L(\chi_4, s)L(\chi_{8A}, s)L(\chi_{8B}, s)\\ &= \frac{\zeta_{\mathbb{Q}(i)}(s) \cdot \zeta_{\mathbb{Q}(\sqrt{2})}(s) \cdot \zeta_{\mathbb{Q}(\sqrt{-2})}(s)}{\zeta(s)^2}.\end{aligned}$$

Remark. *This is in practice how* $\zeta_K(s)$ *are computed - e.g. in Magma.*

Theorem 10.3. *Suppose* $\rho, \sigma : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_\star(\mathbb{C})$ *be two Artin representations. Then*

$$\rho \cong \sigma \iff L(\rho, s) = L(\sigma, s)$$

as analytic functions on $\mathrm{Re}(s) \gg 0$*. So the L-function determines the representation uniquely.*

Proof. The forward direction ($\Longrightarrow$) is clear. To show the reverse, ($\Longleftarrow$),

Step 1: For any Dirichlet series, $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ for $\mathrm{Re}(s) \gg 0$, then we can recover the coefficients:

$$\begin{aligned} a_1 &= \lim_{x \to \infty} f(x) \\ a_2 &= \lim_{x \to \infty} \frac{f(x) - a_1}{2^x} \\ &\vdots \end{aligned}$$

so the a_i are uniquely determined by $f(s)$ as a function. Hence ρ, σ have the same local factors at all primes. Then $\dim \rho = \dim \sigma = \deg F_p(T)$ for p large.

Step 2: $\rho : \mathrm{Gal}(F_1/\mathbb{Q}) \to \mathrm{GL}_d(\mathbb{C})$, $\sigma : \mathrm{Gal}(F_2/\mathbb{Q}) \to \mathrm{GL}_d(\mathbb{C})$. Thus if we take the compositum $F = F_1 F_2$ then

$$\rho, \sigma : G \to \mathrm{GL}_d(\mathbb{C}),$$

where $G = \mathrm{Gal}(F/\mathbb{Q})$ is the same group.

Step 3: The Chebotarev density theorem implies that for every conjugacy class $C \subset G$, there exists infinitely many primes p such that $\mathrm{Frob}_p^{F/\mathbb{Q}} \in \mathbb{C}$. Then we have that

$$\chi_\rho(\mathcal{C}) = a_p = \chi_\sigma(C),$$

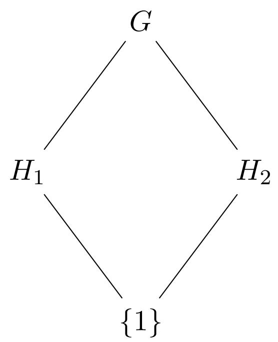
where a_p is the p^{th} term of the Dirichlet series. Thus $\chi_\sigma = \chi_\rho$.

Step 4: From representation theorem, equality of characters implies an isomorphism of representations, so $\chi_\rho = \chi_\sigma \implies \rho \cong \sigma$. ☐

Remark. *It is not true that $\zeta_{M_1}(s) = \zeta_{M_2}(s)$ implies that $M_1 \cong M_2$. There exist Gassmann triples (G, H_1, H_2) such that*

$$G/H_1 \ncong G/H_2 \quad \textit{as G-sets, but} \quad \mathbb{C}[G/H_1] \cong \mathbb{C}[G/H_2] \quad \textit{as representations}.$$

An example of this is the following: $G = \mathrm{GL}_3(\mathbb{F}_2)$, order 168, simple.



Above we have that H_1, H_2 are two non-conjugate subgroups of index 7 such that $\mathbb{C}[G/H_1] \cong \mathbb{C}[G/H_2]$. This leads to degree 7 fields M_1, M_2 over $\mathbb{Q}$ (for every realisation of G as $\mathrm{Gal}(F/\mathbb{Q})$) with $M_1 \ncong M_2$ but $\zeta_{M_1}(s) = \zeta_{M_2}(s)$.

This is the smallest possible example, it is easy to check that in degree less than 7, $\zeta_M(s)$ determines M. Such M_1, M_2 are called **arithmetically equivalent** fields. Many invariants of M_1, M_2 are the same, for example

$$\begin{aligned} r_1, r_2 &\leftarrow \text{ functions of complex conj acting on } \mathbb{C}[G/H]. \\ |\Delta_M| &\leftarrow \text{ conductor of } \mathbb{C}[G/H] \\ \frac{R \cdot h}{\#\text{roots of 1}} &\leftarrow \zeta_M(0), \end{aligned}$$

but for example h, R need not be the same (not functions of $\mathbb{C}[G/H]$).

Remark. *The above phenomenon has been explored for class groups, non-isomorphic curves with isomorphic Jacobians, BSD conjecture, and notably Sunada 1985:*

"Can you hear the shape of a drum?" : NO.

That is, there exists non-isomorphic manifolds with the same spectrum of the Laplacian (same construction).

11 Γ-factors, ε-factors, and conductors

Suppose that we have an Artin representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_d(\mathbb{C})$ with a degree d L-function $L(\rho, s)$, meromorphic. Then let us define the completed L-function:

$$\hat{L}(\rho, s) = \left(\frac{N}{\pi^d}\right)^{s/2} \gamma(s) L(\rho, s),$$

and this satisfies the function equation

$$\hat{L}(\rho, s) = w \cdot \hat{L}(\rho^*, s).$$

Above we have written

$$\begin{aligned} N &= N(\rho), \text{ conductor} \in \mathbb{N} \\ \gamma(s) &= \gamma_\rho(s), \Gamma\text{-factor} \\ w &= w_\rho, \text{ root number, sign in functional eq., } |w| = 1. \end{aligned}$$

Recall that 1-dimensional ρ correspond exactly to Dirichlet characters χ (and for $\rho : G_K \to \mathbb{C}^\times \leftrightarrow$ Hecke similarly). Then

$$N = \text{modulus}^4 \text{of } \chi = m$$

$$\gamma(s) = \begin{cases} \Gamma\left(\frac{s}{2}\right) & \text{if } \chi(-1) = 1 \iff \rho(\text{complex conj}) = +1, \\ \Gamma\left(\frac{s+1}{2}\right) & \text{if } \chi(-1) = -1 \iff \rho(\text{complex conj}) = -1. \end{cases}$$

$$w = \frac{\varepsilon}{|\varepsilon|}, \ \varepsilon = \sum_{a=1}^{m-1} \chi(a) \zeta_m^a, \text{ Gauss sum.}$$

For general ρ, we can define $N, \varepsilon, w = \frac{\varepsilon}{|\varepsilon|}, \gamma(s)$ from 1-dimenisonals and Brauer induction. In fact, for ε-factors cannot do much better,

$$\varepsilon(\rho) = \prod_{\substack{\text{v} \\ \text{places of } \mathbb{Q}}} \varepsilon_V(\rho) \leftarrow \text{local } \varepsilon\text{-facors} \begin{cases} \dim \rho = 1 & \text{Tate's thesis} \\ \dim \rho > 1 & \text{Langlands-Deligne.} \end{cases}$$

γ-**factors**: To work out the γ-factors for $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_d(\mathbb{C})$, we look at how complex conjugation works,

$$\text{complex conj} \mapsto \text{matrix of order 2 with } d_+ \text{ eigenvalues}$$
$$\text{and } d_- \text{ eigenvalues } -1 \text{ with } d_+ + d_- = d.$$

Then

$$\gamma(s) = \Gamma\left(\frac{s}{2}\right)^{d_+} \Gamma\left(\frac{s+1}{2}\right)^{d_-}.$$

To prove this just check that it is correct for 1-dimensionals and respects Artin formalism.

Example 11.1. *Let $M/\mathbb{Q}$ be finite. Then $\zeta_M(s) = L(\mathbb{C}[X], s)$ where $X = \{$embeddings $M \hookrightarrow \mathbb{C}\}$ on which $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ acts. Then complex conjugation fixes r_1 real embeddings and swaps complex ones in pairs. So the matrix*

$$\begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & 0 & 1 & & & & \\ & & & 1 & 0 & & & & \\ & & & & & \ddots & & & \\ & & & & & & & 0 & 1 \\ & & & & & & & 1 & 0 \end{pmatrix}$$

so there are $r_1 + r_2$ number of $+1$ eigenvalues and r_2 number of -1 eigenvalues. Therefore

$$\gamma(s) = \Gamma\left(\frac{s}{2}\right)^{r_1+r_2} \Gamma\left(\frac{s+1}{2}\right)^{r_2},$$

as expected for $\zeta_M(s)$.

Conductors:

Definition (Artin conductor)**.** *Let $\rho : \mathrm{Gal}(F/K) \to \mathrm{GL}(V)$, where K is a finite extension of $\mathbb{Q}$, F/K is Galois with group G, and $\dim V = d$. Then we define $N(\rho)$, the global Artin conductor, to be an ideal in $\mathcal{O}_K$,*

$$N(\rho) = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}},$$

where $n_{\mathfrak{p}}$ is the local conductor exponent at $\mathfrak{p}$ (sometimes $n_{\mathfrak{p}}$ is written $f_{\mathfrak{p}}$).

[4] If $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ primitive then the modulus of χ is m

Theorem 11.1 (Local conductor exponent)**.** *Let $D = D_{\mathfrak{p}}, I = I_{\mathfrak{p}} \subset G = \mathrm{Gal}(F/K)$ be the decomposition and inertia group of some*

$$\mathfrak{q}|\mathfrak{p}|p$$

where $\mathfrak{q}$ is in F, $\mathfrak{p}$ is in K, and $p \in \mathbb{Q}$. Then

$$n_{\mathfrak{p}} = n_{\mathfrak{p},\mathit{tame}} + n_{\mathfrak{p},\mathit{wild}}$$

(sometimes 'wild' is also called 'Swan'), and

$$\begin{aligned} n_{\mathfrak{p},\mathit{tame}} &= d - \dim V^I \leftarrow \text{'Missing degree for } F_{\mathfrak{p}}(T)\text{'} \\ n_{\mathfrak{p},\mathit{wild}} &= 0 \text{ if } p \nmid |I|. \end{aligned}$$

In general,

$$G > D \triangleright \underset{\text{inertia}}{I_0 = I} \triangleright \underset{\text{wild inertia}}{I_1 = p\text{-Sylow}(I)} \triangleright I_2 \triangleright \cdots$$

where

$$I_n = \{\sigma \in D | \sigma = \mathit{id} \text{ on } \mathcal{O}_f/\mathfrak{q}^{n+1}\},$$

are higher ramification groups,

$$= \{1\} \quad \text{for } n \text{ large.}$$

Then

$$n_{\mathfrak{p},\mathit{wild}} = \sum_{n \geq 1} \frac{|I_n|}{|I|}(d - \dim V^{I_n}) \in \mathbb{Z},$$

which measures how 'badly ramified' V is.

Example 11.2. *ρ is unramified at $\mathfrak{p}$ - that is ($V^I = 0$) $\iff$*

$$n_{\mathfrak{p},\mathit{tame}} = 0 \iff n_{\mathfrak{p}} = 0.$$

In particular $n_{\mathfrak{p}} = 0$ for all primes unramified in F/K.

Example 11.3. *Let $\rho : G_{\mathbb{Q}} \to \mathbb{C}^\times$ (thus they correspond to Dirichlet characters) then*

$$N(\rho) = \text{modulus of } \chi.$$

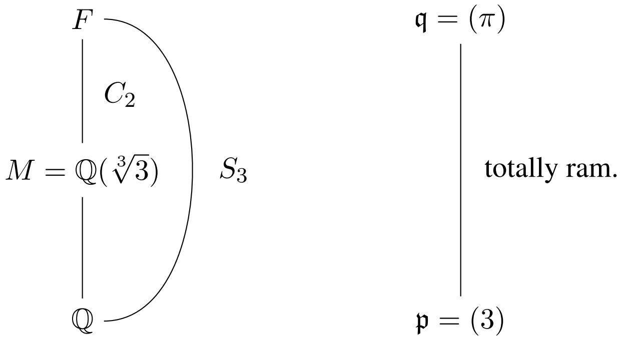
Theorem 11.2 (Conductor-discriminant formula, or Führerdiskriminantformel)**.** *Let M/K be a finite extension and*

$$\zeta_{M/K}(s) = L(\mathbb{C}[X_{M/K}], s),$$

where $\mathbb{C}[X_{M/K}]$ is K-embeddings $M \hookrightarrow \overline{K}$. Then $N_{\mathbb{C}[X_{M/K}]} = |\Delta_{M/K}|$ as ideals in $\mathcal{O}_K$.

Remark. *This gives a way to compute discriminants of number fields using Artin representations.*

Example 11.4. *Let $F = \mathbb{Q}(\zeta, \sqrt[3]{3})$, and*



Then $\pi = \frac{1-\zeta}{\sqrt[3]{3}}$ which has valuation $1/2 - 1/3$. We have that

$$\underset{\text{3-Sylow}}{C_3} = I_1 \triangleleft I = D = G = S_3.$$

Then the generator σ^{-1} of I_1:

$$\begin{aligned} \sqrt[3]{3} &\to \zeta\sqrt[3]{3} \\ 1-\zeta &\to 1-\zeta, \end{aligned}$$

so $\sigma(\pi) = \zeta\pi$. How wild is the valuation σ? We compute

$$\begin{aligned} v_{\mathfrak{q}}(\pi - \sigma(\pi)) &= v_{\mathfrak{q}}(\pi - \zeta\pi) \\ &= v_{\mathfrak{q}}(\pi)v_{\mathfrak{q}}(1-\zeta) \\ &= 1 + v_{\mathfrak{q}}(1-\zeta) \\ &= 4. \end{aligned}$$

Thus, σ is trivial mod π^4. However $\sigma \not\equiv 1 \mod \pi^5$ since $\sigma(\pi) \not\equiv \pi \mod \pi^5$. This tells us how deep σ lies in our inertia group:

$$\underbrace{\cdots \triangleleft \{1\}\ I_4}_{\{1\}} \triangleleft \underbrace{I_3 = I_2 = I_1}_{C_3} \triangleleft I = S_3$$

Take $V = \mathbb{C}[X_{M/K}] = \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$, and S_3 acts naturally on this (permuting the basis elements). Then S_3, C_3 have 1-dim invariants ($\#\{$orbits$\}$), and $\{1\}$ has 3-dim invariant.

Now

$$n_{V,3} = d - \dim V^I + n_{\mathfrak{p},\textit{wild}} = \overbrace{3-1}^{\textit{tame}} + \overbrace{\frac{3}{6}(3-1)}^{I_1} + \overbrace{\frac{3}{6}(3-1)}^{I_2} + \overbrace{\frac{3}{6}(3-1)}^{I_3} + 0 = 5.$$

At all other primes, $n_{V,p} = 0$, since p unramified in $F/\mathbb{Q}$. So easily $|\Delta_M| = N_V = 3^5$ (and $|\Delta_F| = 3^{11}$).

Finally, conductors (and ε-factors as well) are **inductive in degree** 0:

Theorem 11.3. *Suppose* $[K : \mathbb{Q}] = n$*. Then take two Artin representations* ρ_1, ρ_2 *of same dimension,*

$$\rho_1, \rho_2 : G_K \to \mathrm{GL}_d(\mathbb{C}).$$

We consider the inductions

$$\mathrm{Ind}\,\rho_1, \mathrm{Ind}\,\rho_2 : G_{\mathbb{Q}} \to \mathrm{GL}_{nd}(\mathbb{C}),$$

then

$$\mathrm{Norm}_{K/\mathbb{Q}} \frac{N(\rho_1)}{N(\rho_2)} = \frac{N(\mathrm{Ind}\,\rho_1)}{N(\mathrm{Ind}\,\rho_2)},$$

that is $N(\rho_1 \ominus \rho_2)$ *behaves well under induction.*

Corollary 11.3.1. *Take* $\rho = \rho_1$*,* $\rho_2 = \overbrace{\mathbb{1} \oplus \cdots \oplus \mathbb{1}}^{d}$*. Then*

$$N(\mathrm{Ind}\,\rho_1) = \mathrm{Norm}_{K/\mathbb{Q}} N(\rho) \cdot |\Delta_K|^d.$$

12 Local Fields

Let $K = \mathbb{Q}$, and p a prime then this gives rise to the p-adic absolute value, usually denoted

$$|\cdot|_p$$

on $\mathbb{Q}$. 'Absolute values' are multiplicative functions that satisfy the triangle inequality. In fact, the only absolute values on $\mathbb{Q}$ (up to a natural equivalence) are the classical absolute value and the p-adic ones, defined as

$$\left|p^n \frac{a}{b}\right|_p = \frac{1}{p^n}, \quad |0| = 0.$$

The p-adic absolute value gives rise to a metric

$$d_p(x, y) = |x - y|_p.$$

Definition (p-adic integers)**.** *Define the* p*-adic integers* $\mathbb{Z}_p$ *by*

$$\begin{aligned} \mathbb{Z}_p &= \textit{the topological completion of } \mathbb{Z} \textit{ with respect to } |\cdot|_p \\ &= \frac{\{\textit{Cauchy sequences } (x_n)_n \textit{ in } \mathbb{Z}\}}{\{\textit{sequences } x_n \to 0\}} \\ &= \varprojlim_{n} \mathbb{Z}/p^n\mathbb{Z} \\ &= \varprojlim_{n} \{\textit{seq. } x_n \in \mathbb{Z}/p^n\mathbb{Z} \textit{ s.t. } x_n \equiv x_{n+1} \mod p^n\} \\ &= \left\{ \sum_{n=0}^{\infty} a_n p^n | a_n \in \{0, \ldots, p-1\} \right\}. \end{aligned}$$

Then $\mathbb{Z}_p$ *is a DVR, local ring, which has only one maximal ideal* (p)*, and residue field* $\mathbb{F}_p$*. Further* $\mathbb{Z}_p \supseteq \mathbb{Z}$*.*

Definition (p-adic numbers)**.** *The p-adic numbers $\mathbb{Q}_p$ satisfy:*

$$\begin{aligned}\mathbb{Q}_p &= \textit{topological completion of } \mathbb{Q} \textit{ wrt } d_p \\ &= \textit{Field of fractions of } \mathbb{Z}_p \\ &= \left\{ \sum_{n=n_0}^{\infty} a_n p^n | a_n \in \{0, \dots, p-1\} \right\}.\end{aligned}$$

*This is a field that contains $\mathbb{Q}$, and so has **characteristic 0**.*

Example 12.1. *In $\mathbb{Q}_2$,*

$$\begin{aligned}21 &= 1 + 2^2 + 2^4 \in \mathbb{Z}_2. \\ \frac{3}{2} &= 2^{-1} + 1 \notin \mathbb{Z}_2 \\ -1 &= 1 + 2 + 2^2 + 2^3 + \cdots \in \mathbb{Z}_2 (= \frac{1}{1-x} \textit{ geo series with } x = 2, |x|_2 < 1.).\end{aligned}$$

Example 12.2. *Similarly, for $K/\mathbb{Q}$ finite, $\mathcal{O}, \mathfrak{p}$, with $\mathcal{O}/\mathfrak{p} = k$ finite. Then this gives $\mathfrak{p}$-adic absolute value:*

$$|x|_{\mathfrak{p}} = \left(\frac{1}{|k|}\right)^{v_{\mathfrak{p}}(x)}.$$

*Then we say that $K_{\mathfrak{p}}$ is the topological completion of K with respect to $|\cdot|_{\mathfrak{p}}$ and is called the **local** or $\mathfrak{p}$-adic field. We have that $K_{\mathfrak{p}}$ is a finite extension of $\mathbb{Q}_p$, wrt $\mathfrak{p}|p$, and every finite extension of $\mathbb{Q}_p$ arises this way. So*

$$K_{\mathfrak{p}} = \left\{ \sum_{n=n_0}^{\infty} a_n \pi^n | a_n \in A \right\}$$

where π is any uniformiser, $v_{\mathfrak{p}}(\pi) = 1$ (e.g. $\pi \in \mathfrak{p} \backslash \mathfrak{p}^2$), and A is any set of reprsentatives of $\mathcal{O}/\mathfrak{p}$.

Proposition 12.1. *Take*

$$\begin{array}{ccc} F & & \mathfrak{q} \\ \Big| \text{ Galois} & & \Big| \\ K & & \mathfrak{p} \end{array}$$

Then $F_{\mathfrak{q}}/K_{\mathfrak{p}}$ is Galois with $\mathrm{Gal}(F_{\mathfrak{q}}/K_{\mathfrak{p}}) = D_{\mathfrak{q}}$ - this is the same for all $\mathfrak{q}|\mathfrak{p}$. Passing to the algebraic closure,

$$\begin{array}{ccccc} \overline{\mathbb{Q}} & \text{prime } \mathfrak{q} \text{ above } p \text{ in } \overline{\mathbb{Q}} & & \overline{\mathbb{Q}}_{\mathfrak{p}} & \\ \Big| & \Big| & \overset{complete}{\rightsquigarrow} & \Big| & G_{\mathbb{Q}_p} = D_{\mathfrak{q}} < G_{\mathbb{Q}} \\ \mathbb{Q} & \mathfrak{p} & & \mathbb{Q}_o & \end{array}$$

We can think of these as the 'same' as number fields, but only one prime and much simpler (look at $\mathbb{R}, \mathbb{C}$ versus $\mathbb{Q}$). Further, inertia, Frobenius, and tame inertia etc. take the same definition. The structure of $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is as follows,

$$
\begin{array}{llll}
 & \overline{\mathbb{Q}}_{\mathfrak{p}} & & \\
 & \Big| \quad I \text{ wild} \quad \leftarrow\text{(pro-) p-group} & & \\
I \text{ itertia} \left\{ \right. & \mathbb{Q}_{\mathfrak{p}}^{t} = \bigcup_{p\nmid n} \mathbb{Q}_p(\zeta_n, \sqrt[n]{p}) & & \\
 & \Big| \quad I \text{ tame} \quad \leftarrow\text{(pro-) cyclic} & & \\
 & \mathbb{Q}_{\mathfrak{p}}^{nr} = \bigcup_{p\nmid n} \mathbb{Q}_p(\zeta_n) & (p) & \overline{\mathbb{F}_p} \\
 & \Big| \quad G_{\mathbb{F}_p} \quad \leftarrow\text{(pro-) cyclic gen. by } x \mapsto x^p, & & \\
 & \qquad\qquad \text{lift it to } \mathrm{Frob}_p \in G_{\mathbb{Q}_p} & & \\
 & \mathbb{Q}_p & (p) & \mathbb{F}_p
\end{array}
$$

Local fields have only finitely many extensions of a given degree. For example,

$$\mathbb{Q}_5(\sqrt{-3}) = \mathbb{Q}_5(\sqrt{2}) = \mathbb{Q}_5(\zeta_3) = \mathbb{Q}_5(\zeta_8) = \mathbb{Q}_5(\zeta_{24}),$$

all of which are the unique quadratic unramified extension of $\mathbb{Q}_5$.

13 l-adic reprsentations

Example 13.1. *Take*

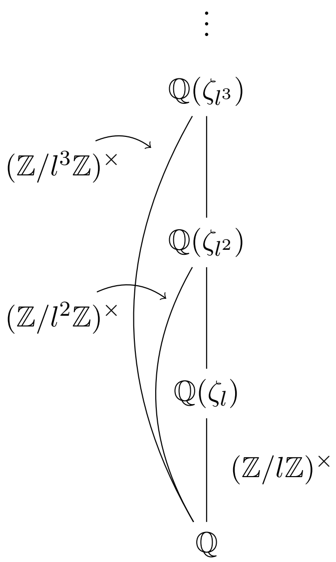
$$G_{\mathbb{Q}} \circlearrowright \{\textit{roots of unity in } \overline{\mathbb{Q}}\} = \{\textit{torsion points in } \mathbb{G}_m(\overline{\mathbb{Q}}) = \overline{\mathbb{Q}}^{\times}\}$$

This action of does not factor through a finite Galois group. We want to associate to it a 1-dimensional Galois representation as follows.

Take l prime.

$$
\begin{array}{ccc}
\cdots & \cdots & \\
\downarrow & \downarrow & \\
\{l^3 \textit{ roots of unity}\} \cong & \mathbb{Z}/l^3\mathbb{Z} & \circlearrowleft G_{\mathbb{Q}} \\
\downarrow x \mapsto x^l & \downarrow [l] & \\
\{l^2 \textit{ roots of unity}\} \cong & \mathbb{Z}/l^2\mathbb{Z} & \circlearrowleft G_{\mathbb{Q}} \\
\downarrow x \mapsto x^l & \downarrow [l] & \\
\{l^{th} \textit{ roots of unity}\} \cong & \mathbb{Z}/l\mathbb{Z} & \circlearrowleft G_{\mathbb{Q}}.
\end{array}
$$

We have that in the final line, $G_{\mathbb{Q}}$ acts from $(\mathbb{Z}/l\mathbb{Z})^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$. Pictorially:



Taking the inverse limit, we find that

$$G_{\mathbb{Q}} \circlearrowright \varprojlim_{n} \mathbb{Z}/l^n\mathbb{Z} \cong \mathbb{Z}_l.$$

In other words, we get a representation

$$\chi_l : G_{\mathbb{Q}} \to \mathbb{Z}_l^\times = \mathrm{GL}_1(\mathbb{Z}_l) = \varprojlim_{n} (\mathbb{Z}/l^n\mathbb{Z})^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_{l^\infty})/\mathbb{Q}).$$

Then if we embed $\mathbb{Z}_l \hookrightarrow \mathbb{Q}_l \hookrightarrow \mathbb{C}$, we can view χ_l as mapping

$$\chi_l : G_{\mathbb{Q}} \to \mathrm{GL}_1(\mathbb{C}),$$

*which is a 1-dimensional Galois representation (one for every l). This is called the **l-adic cyclotomic character**.*

Definition. *Let K be a number field, $G_K = \mathrm{Gal}(\overline{K}/K)$. An **$l$-adic representation over** K of dimension (or degree) d is a continuous homomorphism*

$$\rho_l : G_K \to \mathrm{GL}_d(\mathbb{Q}_l).$$

*A **compatible system** of l-adic representations (or 'a motive') is collection $\rho = (\rho_l)_{l\ prime}$ such that*

(1) There is a finite set S of 'bad' primes of K such that each ρ_l is unramified outside $S_l = S \cup \{primes|l\}$, i.e.

$$\mathfrak{p} \notin S_l \implies \rho_l(I_{\mathfrak{p}}) = 1.$$

(2) For every prime $\mathfrak{p}$ of K, then the local polynomial

$$F_{\mathfrak{p}}(T) = \det\Big(1 - \mathrm{Frob}_{\mathfrak{p}}^{-1} T | \rho_l^{I_{\mathfrak{p}}}\Big) \in \mathbb{Q}_l[T],$$

is a polynomial in $\mathbb{Q}[T]$ and is independent of l, for $\mathfrak{p} \nmid l$.

We then define the L-function of ρ to be

$$L(\rho, s) = \prod_{\mathfrak{p}} F_{\mathfrak{p}}(N\mathfrak{p}^{-s}).$$

The collection $(\rho_l)_l$ is really a 'poor man's version' of one global representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_d(\mathbb{Q})$.

We have the standard constructions $\oplus, \otimes, \mathrm{Ind}, \mathrm{Res}$, etc for compatible systems. Further, L-functions satisfy Artin formalism.

Example 13.2. *Take $\rho : G_K \to \mathrm{GL}_n(\mathbb{Q})$, Artin representation (so this has finite image and factors through some finite Galois group $\mathrm{Gal}(F/K)$). So*

$$\rho_l : G_K \to \mathrm{GL}_n(\mathbb{Q}) \hookrightarrow \mathrm{GL}_n(\mathbb{Q}_l),$$

is obviously a compatible system taking

$$S = \{\textit{primes ramified in } F/K\}.$$

Remark. *In principle, we can replace $(\mathbb{Q}_l)_{l \textit{ prime of } \mathbb{Q}}$ with $(M_\lambda)_{\lambda \textit{ primes of } M}$, where M is a number field, to include all Artin representations $G_K \to \mathrm{GL}_n(\mathbb{C})$, for example Dirichlet characters.*

Example 13.3. *Take $\chi = (\chi_l)_l$ a cyclotomic character. Recall that*

$$\chi_l : G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_{l^\infty})/\mathbb{Q}) = \mathbb{Z}_l^\times \hookrightarrow \mathrm{GL}_1(\mathbb{Q}_l).$$

Then we have that

$$\begin{aligned} I_p &\mapsto 1, && \textit{for all } p \neq l, \\ \mathrm{Frob}_p &\mapsto p^{-1} && \textit{can take } S = \varnothing, \textit{ so } S_l = \{l\}, \\ \zeta_{l^n} &\mapsto \zeta_{l^n}^p \end{aligned}$$

Then

$$F_p(T) = \det\Big(1 - \mathrm{Frob}_p^{-1} T | \mathbb{Z}_l^{I_p}\Big) = 1 - pT \in \mathbb{Q}[T],$$

and recall that $G_{\mathbb{Q}} \circlearrowleft \mathbb{Z}_l^{I_p}$. So $F_p(T)$ is independent of l. Thus the χ_l form a compatible system with

$$L(\chi, s) = \prod_p \frac{1}{1 - p \cdot p^{-s}} = \zeta(s-1).$$

In modern language, χ_l are l-adic realisations of the 'Tate motive $\mathbb{Q}(1)$' (and the χ_l denoted $\mathbb{Q}_l(1)$) which has associated L-function $\zeta(s-1)$.

13.1 Étale Cohomology (Grothendieck, Deligne, Verdier)

Take $V/\mathbb{Q}$ (or over some number field K) a non-signular projective variety of dimension d. Take $0 \leq i \leq 2d$ then this leads to

$$H^i(V) = H^i_{\text{ét}}(V_{\overline{\mathbb{Q}}}, \mathbb{Q}_l),$$

called the i^{th} étale cohomology group. It is a $\mathbb{Q}_l$-vector space of dimension $b_i(V(\mathbb{C}))$ (b_i the i^{th} Betti number) with a continuous action of $G_{\mathbb{Q}}$. This yields an l-adic representation of $G_{\mathbb{Q}}$ for every l - we check the conditions:

(1) We do have that it is unramified outside $S = \{\text{primes of bad reduction for } V\} \cup \{l\}$.

(2) This is known to be compatible at $p \notin S$, and often (H^0, H^1, curves, abelian varieties) for $p \in S$ as well.

Example 13.4. *Take $H^0(V) = \mathbb{Q}_l[\text{connected components of } V/\overline{\mathbb{Q}}]$ and $G_{\mathbb{Q}} \circlearrowright H^0(V)$. We can take a permutation representation on connected components (factors through some finite $\mathrm{Gal}(F/\mathbb{Q})$).*

Example 13.5. *Take a variety V with $\dim V = 0$ so we only have H^0. Then*

$$V : f(x) = 0 \subset \mathbb{A}^1_x$$

for $f \in \mathbb{Q}[x]$. So the absolute Galois group permutes the roots of f.

$$H^0(V) = \mathbb{Q}_l[\text{roots of } f].$$

If $f(x) = f_1(x) \cdots f_n(x)$, $f_i(x) \in \mathbb{Q}[x]$ irreducible, then take

$$K_i = \mathbb{Q}[x]/(f_i).$$

Hence

$$L(H^0(V), s) = \zeta_{K_1}(s) \cdots \zeta_{K_n}(s).$$

14 Torsion Points on Elliptic Curves & $H^1(E)$

Suppose we have an elliptic curve E and a number field K, where

$$y^2 = x^3 + ax + b; \quad a, b \in K,$$

defines an elliptic curve. Then $E(\overline{K})$ form an abelian group.

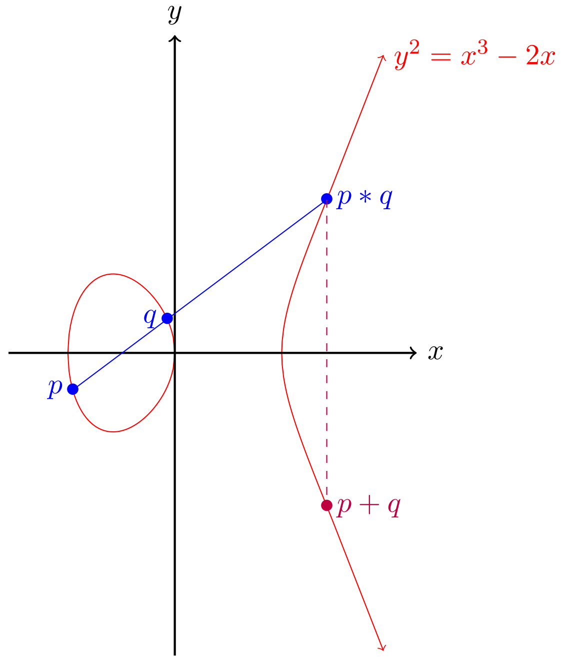


Figure 5: Plot of the elliptic curve $y^2 = x^3 - 2x$

Definition. *Take $m \geq 1$ integer. Then*

$$E[m] = \{p \in E(\overline{K}) | mP = 0\}$$

is the set of m-torsion points, called m-torsion. As an abelian group,

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2 \circlearrowleft G_k \quad \textit{acts linearly,}$$

so $(P+Q)^\sigma = P^\sigma + Q^\sigma$.

This gives a representation ['mod m' representation],

$$\rho_{E,m} : G_K \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Example 14.1. *Take $m = 2$, so we are considering the 2-torsion points. Then*

$$E[2] = \{0, (\alpha, 0), (\beta, 0), (\gamma, 0)\}$$

where α, β, γ are the roots of f. Again

$$E[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$$

and the Galois groups acts by permutation on the roots. Then we get

$$\rho_{E,2} : G_K \to \mathrm{GL}_2(\mathbb{F}_2) \cong S_3.$$

Now take $m = l^n$ where l is prime. Then we get a compatible system:

$$\begin{aligned} &\to E[l^n] \xrightarrow{[l]} E[L^{n-1}] \xrightarrow{[l]} \cdots \xrightarrow{[l]} E[l] \\ &\to (\mathbb{Z}/l^n\mathbb{Z})^2 \to \left(\mathbb{Z}/l^{n-1}\mathbb{Z}\right)^2 \to \cdots \to (\mathbb{Z}/l\mathbb{Z})^2 . \end{aligned}$$

Definition (The l-adic Tate module)**.** *We have*

$$T_l E = \lim_{\leftarrow n} E[l^n] \cong \mathbb{Z}_l^2 \circlearrowleft G_k$$

and

$$V_l E = T_l E \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \cong \mathbb{Q}_l^2 \circlearrowleft G_k.$$

Then by embedding $\mathbb{Q}_l \hookrightarrow \mathbb{C}$, we get a 2-dimensional l-adic representation for E/K,

$$H^1_{ét}(E_{\overline{K}}, \mathbb{Q}_l) = V_l E^*$$

as a G_K representation.

We will see that these form a compatible system so

Definition (The L-function of E/K)**.**

$$L(E/K, s) = \prod_{\mathfrak{p}} F_{\mathfrak{p}}(N\mathfrak{p}^{-s})$$

where

$$F_{\mathfrak{p}}(T) = \det\left(1 - \mathrm{Frob}_{\mathfrak{p}}^{-1} T | \rho_l^{I_p}\right)$$

for any l such that $p \nmid l$. This is a degree 2 L-function.

Recall that we let $E/\mathbb{Q}$ be an elliptic curve with:

$$\begin{array}{ccccc} \overline{\mathbb{Q}} & \mathfrak{q} & & \overline{\mathbb{Q}}_{\mathfrak{p}} & \\ | & | & & | & I_p \\ | & | & D_p = G_{\mathbb{Q}_p} & \mathbb{Q}_p^{nr} & G_{\mathbb{Q}_p} = D_{\mathfrak{q}} < G_{\mathbb{Q}} \\ | & | & & | & \langle \mathrm{Frob}_p \rangle \\ \mathbb{Q} & p & & \mathbb{Q}_p & \end{array}$$

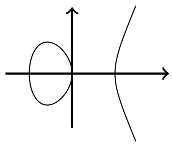
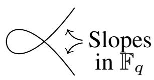
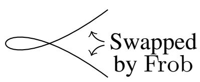
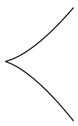
We want to understand D_p on $E_{\overline{\mathbb{Q}}}[l^n] =$ action of $G_{\mathbb{Q}_p}$ on $E_{\overline{\mathbb{Q}}_p}[l^n]$. From now onwards let K be a p-adic field (i.e. local),

$$\mathcal{O}_K/(\pi) \cong k \cong \mathbb{F}_q$$

where (π) is a maximal ideal. Then $I \triangleleft G_k$ and $\mathrm{Frob} \in G_K$. We write χ_l for the cyclotomic character ($I \mapsto 1, \mathrm{Frob} \mapsto q$).

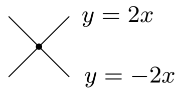
15 Good and bad reduction

Let E/K be an elliptic curve. Then this gives rise to a "minimal Weierstrass model", with coefficients in $\mathcal{O}_K$ and $v(\Delta)$ minimal. Upon reduction, $\tilde{E}/K$ is possibly singular. The possible reduction types are:

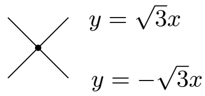
$\tilde{E}$	Reduction	Example over $\mathbb{Q}_5$
	Good	$E_1 : y^2 = x^3 - 1$ (Distinct roots mod 5)
	Split Multiplicative	$E_2 : y^2 = (x-1)(x^2-5)$ (Double root mod 5)
	Non-split Multiplicative	$E_{2'} : y^2 = (x-2)(x^2-5)$ (Double root mod 5)
	Additive	$E_3 : y^2 = x^3 - 5$ (Triple root)

Note that $(0,0)$ is the singular point. Then we have the following reductions, and how they behave near $(0,0)$:

$$\tilde{E}_2 : y^2 = 4x^2 + \text{h.o.t.}/\mathbb{F}_5 \xrightarrow{\text{near } (0,0)}$$



$$\tilde{E}_{2'} : y^2 = 3x^2 + \text{h.o.t.}/\mathbb{F}_5 \xrightarrow{\text{near } (0,0)}$$



for $\sqrt{3} \in \mathbb{F}_{5^2}$.

Theorem 15.1. *We have that*

(a) The set of non-singular points, $E_{ns}(\overline{k})$ form a group, under the same group law (3 points on a line $\iff$ they add up to 0),

(b) $V_l E^I \cong V_l \tilde{E}_{ns}$ as G_k-modules,

(c) $\det V_l E = \chi_l$, that is for $\rho_l : G_\pi \to \operatorname{Aut} V_l E = \mathrm{GL}_2(\mathbb{Q}_2)$, and

$$\det \rho_l(\sigma) = \begin{cases} 1 & \text{for } \sigma \in I \\ q & \text{for } \sigma = \mathrm{Frob}\,. \end{cases}$$

Remark. *This is very important since it relats geometry of the reduction to arithmetic of l-torsion. No analogue for general varieties (only for curves and abelian varieties).*

Remark. *For the Néron model, (b) holds for $E[l^n]$ and $T_l E$ as well.*

Example 15.1. *2-torsion on E_1, E_2, E_3.*

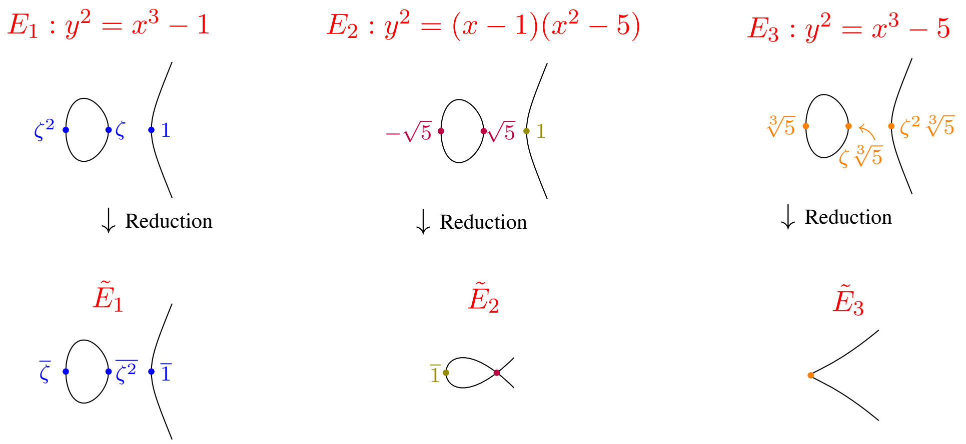


Figure 6: Plots showing how roots behave under different types of reduction. Note that the inertia group I swaps $-\sqrt{5} \leftrightarrow \sqrt{5}$ for E_2 and I permutes the roots for E_3.

Recall that our theorem says that inertia invariant points are non-singular when reduced.

Theorem 15.2. *The local factor $F(T)$ for the L-function of E is*

Reduction	$\tilde{E}_{ns}(\overline{k})$	$V_l\tilde{E}_{ns}$	F(T)
Good	Ell. curve	$\mathbb{Q}_l^2 \circlearrowleft G_K$	$1 - aT + qT^2$ $(a = q + 1 - \#\tilde{E}(\mathbb{F}_q))$
Split mult.	$\overline{k}^\times$	χ_l ($\mathbb{Q}_l$ with Frob acting as q)	$1 - T$
Nonsplit mult.	$\overline{k}^\times$	Quad. twist of $\mathbb{Q}_l$ ($\mathbb{Q}_l$ with Frob acting as $-q$)	$1 + T$
Additive	$(\overline{k}, +)$	0	1

In particular, $F(T) \in \mathbb{Z}[T]$ and is independent of l (i.e. $(V_lE)_l$ form a compatible system).

Proof. **Good reduction**
Let $\tilde{E}/k$ be an elliptic curve. Then

i^{th} Étale coho. group	Frob^{-1} eigenvalues
$H^0_{\text{ét}}(\tilde{E}) = \mathbb{Q}_l$	1
$H^1_{\text{ét}}(E) = H^1_{\text{ét}}(\tilde{E})$	Some α, β
$H^2_{\text{ét}}(\tilde{E}) = \chi_l^{-1}$	q
(Poincaré duality)	

Note that for the Frob^{-1}-eigenvalues, abs. value $|q|^{i/2}$ on H^i. The Lefschetz trace formula gives

$$Z_{\tilde{E}(\mathbb{F}_q)}(T) := \exp \sum_{n=1}^{\infty} \frac{\#\tilde{E}(\mathbb{F}_{q^n})}{n} T^n \overset{Lefschetz}{=} \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}.$$

This implies that

$$1 + \#\tilde{E}(\mathbb{F}_q)T + O(T^2) = 1 + (q + 1 - \alpha - \beta)T + O(T^2).$$

Hence

$$\#\tilde{E}(\mathbb{F}_q) = q + 1 - \mathrm{tr}\big(\mathrm{Frob}^{-1} | H^1_{\text{ét}}(E)\big)$$

and $\det\big(\mathrm{Frob}^{-1} | H^1_{\text{ét}}(E)\big) = q$, $\det V_l = \chi_l$. Thus we see that

$$\begin{aligned}\det\big(1 - \mathrm{Frob}^{-1} T | V_l E^I\big) &= \det\big(1 - \mathrm{Frob}^{-1} T | V_L E\big) \\ &= 1 - aT + qT^2\end{aligned}$$

where $a = q + 1 - \#\tilde{E}(\mathbb{F}_q)$.

Bad reduction
We have that

$$\tilde{E}_{ns} \overset{\text{normalisation}}{\overset{\longleftarrow}{\cong}} \begin{cases} \mathbb{P}'\backslash\{2 \text{ pts}/k\} & = \mathbb{A}'\backslash\{0\} = \mathbb{G}_m \\ \mathbb{P}'\backslash\{2 \text{ pts swapped by Frob}\} & = \text{quad. twist of } \mathbb{G}_m \\ \mathbb{P}'\backslash\{1 \text{ pt}\} & = \mathbb{A}' = \mathbb{G}_a. \end{cases}$$

The only algebraic groups of dimension 1 are elliptic curves, $\mathbb{G}_a$ and $\mathbb{G}_m$.

Additive
Then $\tilde{E}_{ns}(\overline{k}) = \mathbb{G}_a(\overline{k}) = (\overline{k}, +)$ and $\overline{k}$ is ∞-dim $\mathbb{F}_p$ vector space, $p = \operatorname{char} k$. Thus there is no l torsion for $l \neq \operatorname{char} k$ and

$$T_l E_{ns} = 0 \overset{\text{Thm}}{\Longrightarrow} V_l E^I = 0.$$

Hence $F(T) = 1$.

Split mult.
Now $\mathbb{G}_m(\overline{k}) = \overline{k}^\times$, $V_l \mathbb{G}_m = \chi_l$. So G_K acts on $V_l E$ as

$$\begin{pmatrix} \chi_l & \cdot \\ 0 & 1 \end{pmatrix}$$

where $\cdot$ is non-zero on inertia, and bottom row elements are 0 by I-invariants on $V_l E = V_l \mathbb{G}_m$ and 1 since $\det V_l = \chi_l$. Further, G_K acts on $H^1_{\text{ét}}(E) = V_l E^*$ as

$$\begin{pmatrix} \chi_l^{-1} & 0 \\ \cdot & 1 \end{pmatrix}.$$

Noting that $H^1_{\text{ét}}(E)^I$, trivial Frob action gives the second column as $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Thus

$$F(T) = \det\bigl(1 - \text{Frob}^{-1} T | H'(E)^I\bigr) = 1 - T.$$

Multiplicative
Similarly, unr. quad. $\otimes$ split: I acts as

$$\begin{pmatrix} 1 & \cdot \\ 0 & 1 \end{pmatrix},$$

and Frob as

$$\begin{pmatrix} 1 & 0 \\ \cdot & q \end{pmatrix} \begin{pmatrix} -q^{-1} & 0 \\ \cdot & -1 \end{pmatrix}.$$

So $F(T) = 1 + T$. □

In the multiplicative case, $E[l^n]$ is also completely described using the Tate curve: For $E/\mathbb{C}$,

$$E(\mathbb{C}) \cong \mathbb{C}/\mathbb{Z} + \tau\mathbb{Z} \overset{\exp(2\pi i \cdot)}{\cong} \mathbb{C}^\times / q^{\mathbb{Z}} \quad \text{for } q = e^{2\pi i \tau}.$$

This isomorphism from $E(\mathbb{C})$ to $\mathbb{C}^\times / q^{\mathbb{Z}}$ is analytic.

Theorem 15.3 (Tate)**.** *Let K be a local field, E/K an elliptic curve with split mult. red. Then $\exists! q \in K$, $v(q) > 0$ such that*

$$E(\overline{K}) \xrightarrow{\sim} \overline{K}^{\times}/q^{\mathbb{Z}},$$

as G_K-modules. This is the same analytic isomorphism as described above, e.g.

$$j(E) = q^{-1} + 744 + 196884q + \ldots; \quad v(j) = -v(q) < 0.$$

Corollary 15.3.1. *As a G_K-module,*

$$\begin{aligned} E[l^n] &\cong \{l^n - \textit{torsion pts in } \overline{K}^{\times}/q^{\mathbb{Z}}\} \\ &= \langle \zeta_{l^n}, \sqrt[l^n]{q} \rangle \\ &\cong (\mathbb{Z}/l^n\mathbb{Z})^2. \end{aligned}$$

So G_K acts on $T_l E$ as

$$\begin{pmatrix} \chi_l & \cdot \\ 0 & 1 \end{pmatrix}.$$

I acts as

$$\begin{pmatrix} 1 & c \cdot \tau_l \\ 0 & 1 \end{pmatrix},$$

where $c = v(q) = -v(j)$, and

$$\begin{aligned} \tau_l : I &\to \mathbb{Z}_l \quad \textit{l-adic tame char} \\ \sigma &\mapsto \left(\frac{\sigma(\sqrt[l^n]{\pi})}{\sqrt[l^n]{\pi}} \right)_n \in \varprojlim (l^n \textit{th roots of } 1) = \mathbb{Z}_l. \end{aligned}$$

$$[I_{\textit{wild}} \lhd I, \ I_{\textit{tame}} = I/I_{\textit{wild}} = \prod_{l \neq \operatorname{char} k} \mathbb{Z}_l, \quad \tau_l : I_{\textit{tame}} \twoheadrightarrow \mathbb{Z}_l.]$$

Remark. *In the additive reduction case, E/K acquires good ($v(j) \geq 0$) or multiplicative ($v(j) < 0$) reduction over some finite F/K. Thus, in the additive case, I has a finite index subgroup I_F (normally I_p) that acts on $T_l E$ as*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \textit{or as} \quad \begin{pmatrix} 1 & c \cdot \tau_l \\ 0 & 1 \end{pmatrix}.$$

Remark. *Good and multiplicative reduction are also called <u>stable</u> (stay the same in all finite extensions) and additive reduction is called <u>unstable</u>.*

Theorem 15.4 (Grothendieck Monodromy Theorem)**.** *Let K be a local field, V/K a non-singular projective variety. Then there exists a finite extension F/K such that I_F acts on $H^i_{\acute{e}t}(V_{\overline{K}}, \mathbb{Q}_l)$ as $\mathrm{Id} + \tau_l N$ for some nilpotent matrix N. Such a representation of G_K is called a <u>Weil representation</u> if $N = 0$, and a <u>Weil-Deligne representation</u> in general.*

Example 15.2. *Let E/K be an elliptic curve. Then we have*

$$\text{potentially good reduction } v(j) \geq 0, N = 0, H^1_{\acute{e}t}(E) \text{ is a Weil rep}$$
$$\text{potentially mult. } v(j) < 0, N = \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}, H^1(E) \text{ is a W-D rep.}$$

Example 15.3. *For varieties other than curves and abelian varieties, we do not have a geometric counterpart of this statement - it is conjectured, but not known, that any V/K acquires semistable reduction (only ordinary double points as singularities) after some finite extension F/K - if true this proves independence of l by roughly the same argument.*