Galois Representations and Automorphic Forms (MasterMath)

Peter Bruin and Arno Kret

Autumn 2016

Preliminary draft; comments and corrections are welcome

Contents

Chapter 1

Introduction

Contents

In this first chapter, our main goal will be to motivate why one would like to study the objects that this course is about, namely Galois representations and automorphic forms. We give two examples that will later turn out to be known special cases of the *Langlands correspondence*, namely Gauss's quadratic reciprocity theorem and the modularity theorem of Wiles et al. We note that the general Langlands correspondence is still largely conjectural and drives much current research in number theory.

Along the way, we will encounter various number-theoretic objects, such as number fields, elliptic curves, modular forms and Galois representations, and we will associate L-functions to them. These will turn out to form the link by which one can relate objects (such as elliptic curves and modular forms) that a priori seem to be very different.

1.1 Quadratic reciprocity

Recall that if p is a prime number, then the *Legendre symbol* modulo p is defined, for all $a \in \mathbb{Z}$, by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square in } (\mathbb{Z}/p\mathbb{Z})^\times, \\ -1 & \text{if } a \text{ is a non-square in } (\mathbb{Z}/p\mathbb{Z})^\times, \\ 0 & \text{if } a \text{ is congruent to 0 modulo } p. \end{cases}$$

Theorem 1.1 (Quadratic reciprocity law)**.** *Let p and q be two distinct odd prime numbers. Then*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

To put this in the context of this course, we consider two different objects. The first object (a Dirichlet character) lives in the "automorphic world", the second (a character of the Galois group of a number field) lives in the "arithmetic world".

On the one hand, consider the quadratic Dirichlet character

$$\chi_q \colon (\mathbb{Z}/q\mathbb{Z})^\times \to \{\pm 1\}$$

defined by the Legendre symbol

$$\chi_q(a \bmod q) = \left(\frac{a}{q}\right).$$

From the fact that the subgroup of squares has index 2 in $\mathbb{F}_q^\times$, it follows that χ_q is a surjective group homomorphism.

On the other hand, we consider the field

$$K_q = \mathbb{Q}(\sqrt{q^*})$$

where $q^* = (-1)^{(q-1)/2}q$. The Galois group $\mathrm{Gal}(K_q/\mathbb{Q})$ has order 2 and consists of the identity and the automorphism σ defined by $\sigma(\sqrt{q^*}) = -\sqrt{q^*}$.

To any prime $p \neq q$ we associate a *Frobenius element*

$$\mathrm{Frob}_p \in \mathrm{Gal}(K_q/\mathbb{Q}).$$

The general definition does not matter at this stage; it suffices to know that

$$\mathrm{Frob}_p = \begin{cases} \mathrm{id} & \text{if } p \text{ splits in } K_q, \\ \sigma & \text{if } p \text{ is inert in } K_q. \end{cases}$$

Furthermore, there exists a (unique) isomorphism

$$\epsilon_q \colon \mathrm{Gal}(K_q/\mathbb{Q}) \xrightarrow{\sim} \{\pm 1\}.$$

By definition, a prime $p \in \mathbb{Z}$ splits in K_q if and only if q^* is a square modulo p; in other words, we have

$$\epsilon_q(\mathrm{Frob}_p) = \left(\frac{q^*}{p}\right).$$

Note that

$$\left(\frac{q^*}{p}\right) = \left(\frac{-1}{p}\right)^{(q-1)/2}\left(\frac{q}{p}\right)$$

and

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2},$$

so the quadratic reciprocity law is equivalent to

$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right),$$

which is in turn equivalent to

$$\epsilon_q(\mathrm{Frob}_p) = \chi_q(p \bmod q).$$

Note that it is not at all obvious that the splitting behavior of a prime p in K_q only depends on a congruence condition on p.

Sketch of proof of the quadratic reciprocity law. The proof uses the cyclotomic field $\mathbb{Q}(\zeta_q)$. It is known that this is an Abelian extension of degree $\phi(q) = q - 1$ of $\mathbb{Q}$, and that there exists an isomorphism

$$\begin{aligned}(\mathbb{Z}/q\mathbb{Z})^\times &\xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \\ a &\longmapsto \sigma_a,\end{aligned}$$

where σ_a is the unique automorphism of the field $\mathbb{Q}(\zeta_q)$ with the property that $\sigma_a(\zeta_q) = \zeta_q^a$. There is a notion of Frobenius elements $\mathrm{Frob}_p \in \mathbb{Q}(\zeta_q)$ for every prime number p different from q, and we have

$$\sigma_{p \bmod q} = \mathrm{Frob}_p.$$

In Exercise (1.6), you will prove that there exists an embedding of number fields

$$K_q \hookrightarrow \mathbb{Q}(\zeta_q).$$

Such an embedding (there are two of them) induces a surjective homomorphism between the Galois groups. We consider the diagram

$$\begin{array}{ccc}\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) & \twoheadrightarrow & \mathrm{Gal}(K_q/\mathbb{Q}) \\ \sim\uparrow & & \sim\downarrow{\scriptstyle \epsilon_q} \\ (\mathbb{Z}/q\mathbb{Z})^\times & \xrightarrow[\chi_q]{} & \{\pm 1\}.\end{array}$$

Since the group $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic, there exists exactly one surjective group homomorphism $(\mathbb{Z}/q\mathbb{Z})^\times \to \{\pm 1\}$, so we see that the diagram is commutative. Furthermore, the map on Galois groups respects the Frobenius elements on both sides. Computing the image of p in $\{\pm 1\}$ via the two possible ways in the diagram, we therefore conclude that

$$\epsilon_q(\mathrm{Frob}_p) = \chi_q(p \bmod q),$$

which is the identity that we had to prove. □

1.2 First examples of L-functions

1.2.1 The Riemann ζ-function

The prototypical example of an L-function is the *Riemann ζ-function*. It can be defined in (at least) two ways: as a *Dirichlet series*

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

or as an *Euler product*

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

Both the sum and the product converge absolutely and uniformly on subsets of $\mathbb{C}$ of the form $\{s \in \mathbb{C} \mid \Re s \geq \sigma\}$ with $\sigma > 1$. Both expressions define the same function because of the geometric series identity

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n \quad \text{for } |x| < 1$$

and because every positive integer has a unique prime factorisation.

We define the *completed ζ-function* by

$$\mathrm{Z}(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Here we have used the Γ-function, defined by

$$\Gamma(s) = \int_0^{\infty} \exp(-t)t^s \frac{dt}{t} \quad \text{for } \Re s > 0.$$

By repeatedly using the functional equation

$$\Gamma(s+1) = s\Gamma(s),$$

one shows that the Γ-function can be continued to a meromorphic function on $\mathbb{C}$ with simple poles at the non-positive integers and no other poles.

Theorem 1.2 (Riemann, 1859)**.** *The function $\mathrm{Z}(s)$ can be continued to a meromorphic function on the whole complex plane with a simple pole at $s = 1$ with residue 1, a simple pole at $s = 0$ with residue -1, and no other poles. It satisfies the functional equation*

$$\mathrm{Z}(s) = \mathrm{Z}(1-s).$$

Proof. (We omit some details related to convergence of sums and integrals.) The proof is based on two fundamental tools: the *Poisson summation formula* and the *Mellin transform*. The Poisson summation formula says that if $f\colon \mathbb{R} \to \mathbb{C}$ is smooth and quickly decreasing, and we define the Fourier transform of f by

$$\hat{f}(y) = \int_{-\infty}^{\infty} f(x) \exp(-2\pi i x y) dx,$$

then we have

$$\sum_{m\in\mathbb{Z}} f(x+m) = \sum_{n\in\mathbb{Z}} \hat{f}(n)\exp(2\pi i n x).$$

(This can be proved by expanding the left-hand side in a Fourier series and showing that this yields the right-hand side.) In particular, putting $x = 0$, we get

$$\sum_{m\in\mathbb{Z}} f(m) = \sum_{n\in\mathbb{Z}} \hat{f}(n).$$

For fixed $t > 0$, we now apply this to the function

$$f_t(x) = \exp(-\pi t^2 x^2).$$

By Exercise 1.7, the Fourier transform of f_t is given by

$$\hat{f}_t(y) = t^{-1}\exp(-\pi y^2/t^2).$$

The Poisson summation formula gives

$$\sum_{m\in\mathbb{Z}} \exp(-\pi m^2 t^2) = t^{-1}\sum_{n\in\mathbb{Z}} \exp(-\pi n^2/t^2).$$

Hence, defining the function

$$\begin{aligned}\phi\colon (0,\infty) &\longrightarrow \mathbb{R}\\ t &\longmapsto \sum_{m\in\mathbb{Z}} \exp(-\pi m^2 t^2),\end{aligned}$$

we obtain the relation

$$\phi(t) = t^{-1}\phi(1/t). \tag{1.1}$$

The definition of $\phi(t)$ implies

$$\phi(t) \to 1 \quad \text{as } t \to \infty,$$

and combining this with the relation (1.1) between $\phi(t)$ and $\phi(1/t)$ gives

$$\phi(t) \sim t^{-1} \quad \text{as } t \to 0.$$

To apply the Mellin transform, we need a function that decreases at least polynomially as $t \to \infty$. We therefore define the auxiliary function

$$\begin{aligned}\phi_0(t) &= \phi(t) - 1\\ &= 2\sum_{m=1}^{\infty} \exp(-\pi m^2 t^2).\end{aligned}$$

Then we have

$$\phi_0(t) \sim t^{-1} \quad \text{as } t \to 0$$

and

$$\phi_0(t) \sim 2\exp(-\pi t^2) \quad \text{as } t \to \infty.$$

Furthermore, the equation (1.1) implies

$$\phi_0(t) = t^{-1}\phi_0(1/t) + t^{-1} - 1. \tag{1.2}$$

Next, we consider the *Mellin transform* of ϕ_0, defined by

$$(\mathcal{M}\phi_0)(s) = \int_0^\infty \phi_0(t) t^s \frac{dt}{t}.$$

Due to the asymptotic behaviour of $\phi_0(t)$, the integral converges for $\Re s > 1$. We will now rewrite $(\mathcal{M}\phi_0)(s)$ in two different ways to prove the analytic continuation and functional equation of $\mathrm{Z}(s)$.

On the one hand, substituting the definition of $\phi_0(t)$, we obtain

$$\begin{aligned}(\mathcal{M}\phi_0)(s) &= 2\int_0^\infty \Big(\sum_{n=1}^\infty \exp(-\pi n^2 t^2)\Big) t^s \frac{dt}{t} \\ &= 2\sum_{n=1}^\infty \int_0^\infty \exp(-\pi n^2 t^2) t^s \frac{dt}{t}.\end{aligned}$$

Making the change of variables $u = \pi n^2 t^2$ in the n-th term, we obtain

$$\begin{aligned}(\mathcal{M}\phi_0)(s) &= \sum_{n=1}^\infty \int_0^\infty \exp(-u) \Big(\frac{u}{\pi n^2}\Big)^{s/2} \frac{du}{u} \\ &= \pi^{-s/2} \sum_{n=1}^\infty n^{-s} \int_0^\infty \exp(-u) u^{s/2} \frac{du}{u} \\ &= \frac{\Gamma(s/2)}{\pi^{s/2}} \zeta(s) \\ &= \mathrm{Z}(s).\end{aligned}$$

On the other hand, we can split up the integral defining $(\mathcal{M}\phi_0)(s)$ as

$$(\mathcal{M}\phi_0)(s) = \int_0^1 \phi_0(t) t^s \frac{dt}{t} + \int_1^\infty \phi_0(t) t^s \frac{dt}{t}.$$

Substituting $t = 1/u$ in the first integral and using (1.2), we get

$$\begin{aligned}\int_0^1 \phi_0(t) t^s \frac{dt}{t} &= \int_1^\infty \phi_0(1/u) u^{-s} \frac{du}{u} \\ &= \int_1^\infty \Big(u\phi_0(u) + u - 1\Big) u^{-s} \frac{du}{u}.\end{aligned}$$

Using the identity $\int_1^\infty u^{-a} \frac{du}{u} = 1/a$ for $\Re a > 0$, we conclude

$$(\mathcal{M}\phi_0)(s) = \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \phi_0(t) t^s \frac{dt}{t} + \int_1^\infty \phi_0(t) t^{1-s} \frac{dt}{t}.$$

From the two expressions for $(\mathcal{M}\phi_0)(s)$ obtained above, both of which are valid for $\Re s > 1$, we conclude that $\mathrm{Z}(s)$ can be expressed for $\Re s > 1$ as

$$\begin{aligned}\mathrm{Z}(s) &= (\mathcal{M}\phi_0)(s) \\ &= \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \phi_0(t) t^s \frac{dt}{t} + \int_1^\infty \phi_0(t) t^{1-s} \frac{dt}{t}.\end{aligned}$$

Both integrals converge for all $s \in \mathbb{C}$. The right-hand side therefore gives the meromorphic continuation of $\mathrm{Z}(s)$ with the poles described in the theorem. Furthermore, it is clear that the right-hand side is invariant under the substitution $s \mapsto 1 - s$. □

Remark 1.3. Each of the above two ways of writing $\zeta(s)$ (as a Dirichlet series or as an Euler product) expresses a different aspect of $\zeta(s)$. The Dirichlet series is needed to obtain the analytic continuation, while the Euler product highlights the relationship to the prime numbers.

1.2.2 Dedekind ζ-functions

The Riemann ζ-function expresses information related to arithmetic in the rational field $\mathbb{Q}$. Next, we go from $\mathbb{Q}$ to general number fields (finite extensions of $\mathbb{Q}$). We will introduce Dedekind ζ-functions, which are natural generalisations of the Riemann ζ-function to arbitrary number fields.

Let K be a number field, and let $\mathcal{O}_K$ be its ring of integers. For every non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, the *norm* of $\mathfrak{a}$ is defined as

$$N(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a}).$$

Definition 1.4. Let K be a number field. The *Dedekind ζ-function* of K is the function

$$\zeta_K \colon \{s \in \mathbb{C} \mid \Re s > 1\} \to \mathbb{C}$$

defined by

$$\zeta_K(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} N(\mathfrak{a})^{-s},$$

where $\mathfrak{a}$ runs over the set of all non-zero ideals of $\mathcal{O}_K$.

By unique prime ideal factorisation in $\mathcal{O}_K$, we can write

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}},$$

where $\mathfrak{p}$ runs over the set of all non-zero *prime* ideals of $\mathcal{O}_K$.

The same reasons why one should be interested the Riemann ζ-function also apply to the Dedekind ζ-function: its non-trivial zeroes encode the distribution of prime ideals in $\mathcal{O}_K$, while its special values encode interesting arithmetic data associated with K.

Let $\Delta_K \in \mathbb{Z}$ be the discriminant of K, and let r_1 and r_2 denote the number of real and complex places of K, respectively. Then one can show that the completed ζ-function

$$\mathrm{Z}_K(s) = |\Delta_K|^{s/2} \big(\pi^{-s/2}\Gamma(s/2)\big)^{r_1} \big((2\pi)^{1-s}\Gamma(s)\big)^{r_2} \zeta_K(s)$$

has a meromorphic continuation to $\mathbb{C}$ and satisfies

$$\mathrm{Z}_K(s) = \mathrm{Z}_K(1-s).$$

Theorem 1.5 (Class number formula)**.** *Let K be a number field. In addition to the above notation, let h_K denote the class number, R_K the regulator, and w_K the number of roots of unity in K. Then $\zeta_K(s)$ has a simple pole in $s = 1$ with residue*

$$\mathrm{Res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{|\Delta_K|^{1/2} w_K}.$$

Furthermore, one has

$$\lim_{s \to 0} \frac{\zeta_K(s)}{s^{r_1+r_2-1}} = -\frac{h_K R_K}{w_K}.$$

1.2.3 Dirichlet L-functions

Next, we will describe a construction of L-functions that is of a somewhat different nature, since it does not directly involve number fields or Galois theory. Instead, it is more representative of the L-functions that we will later attach to automorphic forms.

Definition 1.6. Let n be a positive integer. A *Dirichlet character* modulo n is a group homomorphism

$$\chi\colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times.$$

Let n be a positive integer, and let χ be a Dirichlet character modulo n. We extend χ to a function

$$\tilde{\chi}\colon \mathbb{Z} \to \mathbb{C}$$

by putting

$$\tilde{\chi}(m) = \begin{cases} \chi(m \bmod n) & \text{if } \gcd(m,n) = 1, \\ 0 & \text{if } \gcd(m,n) > 1. \end{cases}$$

By abuse of notation, we will usually write χ for $\tilde{\chi}$. Furthermore, we let $\bar{\chi}$ denote the complex conjugate of χ, defined by

$$\begin{aligned} \bar{\chi}\colon \mathbb{Z} &\to \mathbb{C} \\ m &\mapsto \overline{\chi(m)}. \end{aligned}$$

One checks immediately that $\bar{\chi}$ is a Dirichlet character satisfying

$$\chi(m)\bar{\chi}(m) = \begin{cases} 1 & \text{if } \gcd(m,n) = 1, \\ 0 & \text{if } \gcd(m,n) > 1. \end{cases}$$

For fixed n, the set of Dirichlet characters modulo n is a group under pointwise multiplication, with the identity element being the trivial character modulo n and the inverse of χ being $\bar{\chi}$. This group can be identified with $\mathrm{Hom}((\mathbb{Z}/n\mathbb{Z})^\times, \mathbb{C}^\times)$. It is *non-canonically* isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, and its order is $\phi(n)$, where ϕ is Euler's ϕ-function.

Let n, n' be positive integers with $n \mid n'$, and let χ be a Dirichlet character modulo m. Then χ can be *lifted* to a Dirichlet character $\chi^{(n')}$ modulo n' by putting

$$\chi^{(n')}(m) = \begin{cases} \chi(m) & \text{if } \gcd(m,n') = 1, \\ 0 & \text{if } \gcd(m,n') > 1. \end{cases}$$

The *conductor* of a Dirichlet character χ modulo n is the smallest divisor n_χ of n such that there exists a Dirichlet character χ_0 modulo n_χ satisfying $\chi = \chi_0^{(n)}$. A Dirichlet character χ modulo n is called *primitive* if $n_\chi = n$.

Remark 1.7. If you already know about the topological ring $\widehat{\mathbb{Z}} = \varprojlim_{n\geq 1} \mathbb{Z}/n\mathbb{Z}$ of profinite integers, you may alternatively view a Dirichlet character as a continuous group homomorphism

$$\chi\colon \widehat{\mathbb{Z}}^\times \to \mathbb{C}^\times.$$

This is a first step towards the notion of *automorphic representations*. Vaguely speaking, these are representations (in general infinite-dimensional) of non-commutative groups somewhat resembling $\widehat{\mathbb{Z}}^\times$.

Note that when we view Dirichlet characters as homomorphisms $\chi\colon \widehat{\mathbb{Z}}^\times \to \mathbb{C}^\times$, there is no longer a notion of a modulus of χ. However, we can recover the conductor of χ as the smallest positive integer n_χ for which χ can be factored as a composition

$$\chi\colon \widehat{\mathbb{Z}}^\times \to (\mathbb{Z}/n_\chi\mathbb{Z})^\times \to \mathbb{C}^\times.$$

Definition 1.8. Let $\chi\colon \mathbb{Z} \to \mathbb{C}$ be a Dirichlet character modulo n. The *Dirichlet L-function* attached to χ is the function

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

In a similar way as for the Riemann ζ-function, one shows that the sum converges absolutely and uniformly on every right half-plane of the form $\{s \in \mathbb{C} \mid \Re s \geq \sigma\}$ with $\sigma > 1$. This implies that the above Dirichlet series defines a holomorphic function $L(\chi, s)$ on the right half-plane $\{s \in \mathbb{C} \mid \Re s > 1\}$.

Furthermore, the multiplicativity of $L(\chi, s)$ implies the identity

$$L(\chi, s) = \prod_{p \text{ prime}} \frac{1}{1 - \chi(p)p^{-s}} \quad \text{for } \Re s > 1.$$

In Exercise 1.8, you will show that $L(\chi, s)$ admits an analytic continuation and functional equation similar to those for $\zeta(s)$.

Remark 1.9. The functions $L(\chi, s)$ were introduced by P. G. Lejeune-Dirichlet in the proof of his famous theorem on primes in arithmetic progressions:

Theorem (Dirichlet, 1837)**.** *Let n and a be coprime positive integers. Then there exist infinitely many prime numbers p with $p \equiv a \pmod{n}$.*

1.2.4 An example of a Hecke L-function

Just as Dedekind ζ-functions generalise the Riemann ζ-function, the Dirichlet L-functions $L(\chi, s)$ can be generalised to L-functions of *Hecke characters*. As the definition of Hecke characters is slightly involved, we just give an example at this stage.

Let I be the group of fractional ideals of the ring $\mathbb{Z}[\sqrt{-1}]$ of Gaussian integers. We define a group homomorphism

$$\begin{aligned} \chi\colon I &\to \mathbb{Q}(\sqrt{-1})^\times \\ \mathfrak{a} &\mapsto a^4, \end{aligned}$$

where $a \in \mathbb{Q}(\sqrt{-1})$ is any generator of the fractional ideal $\mathfrak{a}$. Such an a exists because $\mathbb{Z}[\sqrt{-1}]$ is a principal ideal domain, and is unique up to multiplication by a unit in $\mathbb{Z}[\sqrt{-1}]$. In particular, since all units in $\mathbb{Z}[\sqrt{-1}]$ are fourth roots of unity, $\chi(\mathfrak{a})$ is independent of the choice of the generator a. Furthermore, we have $N(\mathfrak{a}) = |a|^2$. After choosing an embedding $\mathbb{Q}(\sqrt{-1}) \rightarrowtail \mathbb{C}$, we can view χ as a homomorphism $I \to \mathbb{C}^\times$. This is one of the simplest examples of a Hecke character.

We define a Dirichlet series $L(\chi, s)$ by

$$L(\chi, s) = \sum_{\mathfrak{a}} \chi(\mathfrak{a}) N(\mathfrak{a})^{-s},$$

where $\mathfrak{a}$ runs over all non-zero *integral* ideals of $\mathbb{Z}[\sqrt{-1}]$, and where as before $N(\mathfrak{a})$ denotes the norm of the ideal $\mathfrak{a}$. One can check that this converges for $4-2s<-2$ and therefore defines a holomorphic function on $\{s\in\mathbb{C}\mid \Re s>3\}$. By unique ideal factorisation in $\mathbb{Z}[\sqrt{-1}]$, this L-function admits an Euler product

$$\begin{aligned} L(\chi,s) &= \prod_{\mathfrak{p}} \frac{1}{1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s}} \\ &= \prod_{p \text{ prime}} \prod_{\mathfrak{p}\mid p} \frac{1}{1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s}}. \end{aligned}$$

where $\mathfrak{p}$ runs over the set of all non-zero prime ideals of $\mathbb{Z}[\sqrt{-1}]$.

Concretely, the ideals of smallest norm in $\mathbb{Z}[\sqrt{-1}]$ and the values of χ on them are

$\mathfrak{a}$	(1)	$(1+i)$	(2)	$(2+i)$	$(2-i)$	$(2+2i)$	(3)	$(3+i)$	$(3-i)$
$N(\mathfrak{a})$	1	2	4	5	5	8	9	10	10
$\chi(\mathfrak{a})$	1	-4	16	$-7+24i$	$-7-24i$	-64	81	$28-96i$	$28-96i$

This gives the Dirichlet series

$$L(\chi,s) = 1^{-s} - 4\cdot 2^{-s} + 16\cdot 4^{-s} - 14\cdot 5^{-s} - 64\cdot 8^{-s} + 81\cdot 9^{-s} + 56\cdot 10^{-s} + \cdots$$

and the Euler product

$$\begin{aligned} L(\chi,s) &= \frac{1}{1+2^2\cdot 2^{-s}} \cdot \frac{1}{1-(-7+24i)\cdot 5^{-s}} \cdot \frac{1}{1-(-7-24i)\cdot 5^{-s}} \cdot \frac{1}{1-9^2\cdot 9^{-s}} \cdots \\ &= \frac{1}{1+2^2\cdot 2^{-s}} \cdot \frac{1}{1-3^4\cdot 3^{-2s}} \cdot \frac{1}{1-14\cdot 5^{-s}+5^4\cdot 5^{-2s}} \cdots . \end{aligned}$$

1.3 Modular forms and elliptic curves

1.3.1 Elliptic curves

Let E be an elliptic curve over $\mathbb{Q}$, given by a Weierstrass equation

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with coefficients $a_1,\ldots,a_6\in\mathbb{Z}$. We will assume that this equation has minimal discriminant among all Weierstrass equations for E with integral coefficients. For every prime power $q=p^m$, we let $\mathbb{F}_q$ denote a finite field with q elements, and we consider the number of points of E over $\mathbb{F}_q$. Including the point at infinity, the number of points is

$$\#E(\mathbb{F}_q) = 1 + \#\{(x,y)\in\mathbb{F}_q \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 = 0\}.$$

For every prime number p, we then define a power series $\zeta_{E,p}\in\mathbb{Q}[[t]]$ by

$$\zeta_{E,p} = \exp\left(\sum_{m=1}^{\infty} \frac{\#E(\mathbb{F}_{p^m})}{m} t^m\right).$$

Theorem 1.10 (Schmidt, 1931; Hasse, 1934)**.** *If E has good reduction at p, then there exists an integer a_p such that*

$$\zeta_{E,p} = \frac{1 - a_p t + pt^2}{(1-t)(1-pt)} \in \mathbb{Z}[[t]].$$

Furthermore, a_p satisfies

$$|a_p| \leq 2\sqrt{p}.$$

Looking at the coefficient of t in $\zeta_{E,p}$, we see in particular that the number of $\mathbb{F}_p$-rational points is given in terms of a_p by

$$\#E(\mathbb{F}_p) = p + 1 - a_p. \tag{1.3}$$

Next, suppose that E has bad reduction at p. Then an analogue of Theorem 1.10 holds without the term pt^2, and the formula (1.3) remains valid. In this case, there are only three possibilities for a_p, namely

$$a_p = \begin{cases} 1 & \text{if } E \text{ has split multiplicative reduction at } p, \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p, \\ 0 & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

Remark 1.11. If E has bad reduction at p, then the reduction of E modulo p has a unique singular point, and this point is $\mathbb{F}_p$-rational. The formula (1.3) for $\#E(\mathbb{F}_p)$ includes this singular point. It is not obvious at first sight whether this point should be included in $\#E(\mathbb{F}_p)$ or not; it turns out that including it is the right choice for defining the L-function.

We combine all the functions $\zeta_{E,p}$ by putting

$$\zeta_E(s) = \prod_{p \text{ prime}} \zeta_{E,p}(p^{-s}).$$

By Theorem 1.10, the infinite product converges absolutely and uniformly on every set of the form $\{s \in \mathbb{C} \mid \Re s \geq \sigma\}$ with $\sigma > 3/2$.

More generally, one can try to find out what happens when we replace the elliptic curve E by a more general variety X (more precisely, a scheme of finite type over $\mathbb{Z}$). We can define local factors $\zeta_{X,p}$ and their product

$$\zeta_X(s) = \prod_{p \text{ prime}} \zeta_{X,p}(p^{-s}).$$

in the same way as above; some care must be taken at primes of bad reduction. However, much less is known about the properties of $\zeta_X(s)$ for general X. The function $\zeta_X(s)$ is known as the *Hasse–Weil ζ-function* of X, and the *Hasse–Weil conjecture* predicts that $\zeta_X(s)$ can be extended to a meromorphic function on the whole complex plane, satisfying a certain functional equation.

For elliptic curves E over $\mathbb{Q}$, the Hasse–Weil conjecture is true because of the *modularity theorem*, which implies that $\zeta_E(s)$ can be expressed in terms of the Riemann ζ-function and the L-function of a modular form. More generally, for other varieties X, one may try to express $\zeta_X(s)$ in terms of "modular", or more appropriately, "automorphic" objects, and use these to establish the desired analytic properties of $\zeta_X(s)$. This is one of the motivations for the Langlands conjecture.

Remark 1.12. For an interesting overview of both the mathematics and the history behind ζ-functions and the problem of counting points on varieties over finite fields, see F. Oort's article [11].

1.3.2 Modular forms

We will denote by $\mathcal{H}$ the upper half-plane

$$\mathcal{H} = \{z \in \mathbb{C} \mid \Im z > 0\}.$$

This is a one-dimensional complex manifold equipped with a continuous left action of the group

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}.$$

A particular role will be played by the group

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

and the groups

$$\Gamma(n) = \left\{ \gamma \in \mathrm{SL}_2(Z) \;\middle|\; \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod n \right\}$$

for $n \geq 1$.

Definition 1.13. A *congruence subgroup* of $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that contains $\Gamma(n)$ for some $n \geq 1$.

Definition 1.14. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and let k be a positive integer. A *modular form* of weight k is a holomorphic function

$$f \colon \mathcal{H} \to \mathbb{C}$$

with the following properties:

(i) For all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, we have

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z).$$

(ii) The function f is "holomorphic at the cusps of Γ". (We will not make this precise now.)

From now on we assume (for simplicity) that Γ is of the form

$$\Gamma_1(n) = \left\{ \gamma \in \mathrm{SL}_2(Z) \;\middle|\; \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod n \right\}$$

for some $n \geq 1$. Then Γ contains the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Then the above definition implies that every modular form for Γ can be written as

$$f(z) = \sum_{m=0}^{\infty} a_m \exp(2\pi i z) \quad \text{with } a_0, a_1, \ldots \in \mathbb{C}.$$

1.4 More examples of L-functions

1.4.1 Artin L-functions

We now introduce *Artin L-functions*, which are among the most fundamental examples of L-functions in the "arithmetic world". The easiest non-trivial Artin L-functions are already implicit in the quadratic reciprocity law, and are obtained as follows.

Example 1.15. Let K be a quadratic field of discriminant d, so that $K = \mathbb{Q}(\sqrt{d})$. Furthermore, let ϵ_K be the unique isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} \{\pm 1\}$. Similarly to what we did in §1.1, to every prime p that is unramified in K (i.e. to every prime $p \nmid d$), we associate a Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q})$ by putting

$$\mathrm{Frob}_p = \begin{cases} \mathrm{id} & \text{if } p \text{ splits in } K, \\ \sigma & \text{if } p \text{ is inert in } K. \end{cases}$$

In other words, we have

$$\mathrm{Frob}_p = \left(\frac{d}{p}\right)$$

The Artin L-function attached to ϵ_K is then defined by the Euler product

$$\begin{aligned} L(\epsilon_K, s) &= \prod_{p \text{ unramified in } K} (1 - \epsilon_K(\mathrm{Frob}_p)p^{-s})^{-1} \\ &= \prod_{p \text{ prime}} \left(1 - \left(\frac{d}{p}\right)p^{-s}\right)^{-1}. \end{aligned}$$

The quadratic reciprocity law can be viewed as saying that if q is a prime number and $K = \mathbb{Q}(\sqrt{q^*})$, where $q^* = (-1)^{(q-1)/2}q$, and χ_q is the quadratic Dirichlet character defined by $\chi_q(a \bmod q) = \left(\frac{a}{q}\right)$, then we have an equality of L-functions

$$L(\epsilon_K, s) = L(\chi_q, s).$$

As a first step towards studying non-Abelian Galois groups and their (higher-dimensional) representations, we make the following definition.

Definition 1.16. Let K be a finite Galois extension of $\mathbb{Q}$, and let n be a positive integer. An *Artin representation* is a group homomorphism

$$\rho\colon \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\mathbb{C}).$$

Artin representations are examples of *Galois representations*. More general Galois representations are obtained by looking at arbitrary Galois extensions of fields and GL_n over other rings.

Remark 1.17. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and view K as a subfield of $\overline{\mathbb{Q}}$ by choosing an embedding. Then $\mathrm{Gal}(K/\mathbb{Q})$ is a finite quotient of the infinite Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Just as we can view a Dirichlet character as a continuous one-dimensional $\mathbb{C}$-linear representation of the topological group $\widehat{\mathbb{Z}}^\times$, we can view an Artin representation as a continuous n-dimensional $\mathbb{C}$-linear representation of the topological group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ factoring through the quotient map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$.

Next, we want to attach an L-function to an Artin representation. If p is a prime number such that the number field K is unramified at p, then we can define a *Frobenius conjugacy class* at p in $\mathrm{Gal}(K/\mathbb{Q})$. If σ_p is any Frobenius element at p (i.e. an element of the Frobenius conjugacy class), then we define the *characteristic polynomial of Frobenius* $F_{\rho,p} \in \mathbb{C}[t]$ by the formula

$$F_{\rho,p} = \det(1 - \rho(\sigma_p)t) \in \mathbb{C}[t].$$

(This is the determinant of an $n \times n$-matrix with coefficients in $\mathbb{C}[t]$.) More generally, if K is possibly ramified at p, we have to modify the above definition; this gives rise to a polynomial $F_{\rho,p} \in \mathbb{C}[t]$ of degree at most n.

Definition 1.18. Let $\rho\colon \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ be an Artin representation. The *Artin L-function* of ρ is the function

$$\prod_{p \text{ prime}} \frac{1}{F_{\rho,p}(p^{-s})}.$$

One can show that the product converges absolutely and uniformly for s in sets of the form $\{s \in \mathbb{C} \mid \Re s \geq a\}$ with $a > 1$.

Example 1.19. Let K be the splitting field of the irreducible polynomial $f = x^3 - x - 1 \in \mathbb{Q}[x]$. Because the discriminant of f equals -23, which is not a square, we have

$$K = \mathbb{Q}(\alpha, \sqrt{-23}),$$

where α is a solution of $\alpha^3 - \alpha - 1 = 0$. The number field K has discriminant -23^3, and the Galois group of K over $\mathbb{Q}$ is isomorphic to the symmetric group S_3 of order 6.

The group S_3 has a two-dimensional representation $S_3 \to \mathrm{GL}_2(\mathbb{C})$ defined by

$$\begin{array}{lll} (1) \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), & (12) \mapsto \left(\begin{smallmatrix} -1 & -1 \\ 0 & 1 \end{smallmatrix}\right), & (123) \mapsto \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right), \\ (23) \mapsto \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), & (13) \mapsto \left(\begin{smallmatrix} 1 & 0 \\ -1 & -1 \end{smallmatrix}\right), & (132) \mapsto \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right). \end{array}$$

Composing this with some isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} S_3$ gives an Artin representation

$$\rho\colon \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C}).$$

The Frobenius conjugacy class at a prime p can be read off from the splitting behaviour of p in K, which in turn can be read off from the number of roots of the polynomial $x^3 - x - 1$ modulo p. (These are only equivalent because the Galois group is so small; for general Galois groups, the situation is more complicated.) It is a small exercise to show that for a prime number $p \neq 23$, there are three possibilities:

- -23 is a square modulo p, the polynomial $x^3 - x - 1$ has three roots modulo p, and the Frobenius conjugacy class is $\{(1)\}$;
- -23 is a square modulo p, the polynomial $x^3 - x - 1$ has no roots modulo p, and the Frobenius conjugacy class is $\{(123), (132)\}$;
- -23 is not a square modulo p, the polynomial $x^3 - x - 1$ has exactly one root modulo p, and the Frobenius conjugacy class is $\{(12), (13), (23)\}$.

Moreover, one computes the polynomial $F_{\rho,p} \in \mathbb{C}[t]$ by taking the characteristic polynomial of the matrices in the corresponding Frobenius conjugacy class. For the first few prime numbers p, this gives

p	2	3	5	7	11	...	23	...	59	...
$[\sigma_p]$	(123)	(123)	(12)	(12)	(12)	...	$-$	...	(1)	...
$F_{\rho,p}$	$1+t+t^2$	$1+t+t^2$	$1-t^2$	$1-t^2$	$1-t^2$	...	$1-t$	...	$1-2t+t^2$	...

The Euler product and Dirichlet series of $L(\rho, s)$ look like

$$\begin{aligned} L(\rho,s) &= \frac{1}{1+2^{-s}+2^{-2s}} \cdot \frac{1}{1+3^{-s}+3^{-2s}} \cdot \frac{1}{1-5^{-2s}} \cdot \frac{1}{1-7^{-2s}} \cdots \frac{1}{1-23^{-s}} \cdots \\ &= 1^{-s} - 2^{-s} - 3^{-s} + 6^{-s} + 8^{-s} - 13^{-s} - 16^{-s} + 23^{-s} - 24^{-s} + \cdots . \end{aligned}$$

1.4.2 L-functions attached to elliptic curves

We have seen several examples of L-functions attached to number-theoretic objects such as number fields, Dirichlet characters and Artin representations. It turns out to be very fruitful to define L-functions for geometric objects as well. Our first example is that of elliptic curves over $\mathbb{Q}$.

Let E be an elliptic curve over $\mathbb{Q}$. For every prime number p, we define a_p as in §1.3.1, and we put

$$\epsilon(p) = \begin{cases} 1 & \text{if } E \text{ has good reduction at } p, \\ 0 & \text{if } E \text{ has bad reduction at } p. \end{cases}$$

We can now define the *L-function* of the elliptic curve E as

$$L(E,s) = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s} + \epsilon(p) p^{1-2s}}.$$

As we saw in §1.3.1, this infinite product defines a holomorphic function $L(E,s)$ on the right half-plane $\{s \in \mathbb{C} \mid \Re s > 3/2\}$. Furthermore, the ζ-function of E can be expressed as

$$\zeta_E(s) = \frac{\zeta(s)\zeta(s-1)}{L(E,s)}.$$

Example 1.20. Let E be the elliptic curve

$$E\colon y^2 = x^3 - x^2 + x.$$

This curve has bad reduction at the primes 2 and 3. Counting points on E over the fields $\mathbb{F}_p$ for $p \in \{2,3,5,7,11\}$ gives

p	2	3	5	7	11
a_p	0	-1	-2	0	4

This shows that the L-function of E looks like

$$\begin{aligned} L(E,s) &= \frac{1}{1} \cdot \frac{1}{1+3^{-s}} \cdot \frac{1}{1+2\cdot 5^{-s}+5\cdot 5^{-2s}} \cdot \frac{1}{1+7\cdot 7^{-2s}} \cdot \frac{1}{1-4\cdot 11^{-s}+11\cdot 11^{-2s}} \cdots \\ &= 1^{-s} - 3^{-s} - 2\cdot 5^{-s} + 9^{-s} + 4\cdot 11^{-s} + \cdots \end{aligned}$$

We recall that by the Mordell–Weil theorem, the set $E(\mathbb{Q})$ of rational points on E has the structure of a finitely generated Abelian group. The rank of this Abelian group is still far from understood; it is expected to be linked to the L-function of E by the following famous conjecture.

Conjecture 1.21 (Birch and Swinnerton-Dyer)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then $L(E, s)$ can be continued to a holomorphic function on the whole complex plane, and its order of vanishing at $s = 1$ equals the rank of $E(\mathbb{Q})$.*

Some partial results on this conjecture are known; in particular, it follows from work of Gross, Zagier and Kolyvagin that if the order of vanishing of $L(E, s)$ at $s = 1$ is at most 1, then this order of vanishing is equal to the rank of $E(\mathbb{Q})$.

Remark 1.22. There exists a refined version of the conjecture of Birch and Swinnerton-Dyer that also predicts the leading term in the power series expansion of $L(E, s)$ around $s = 1$. The predicted value involves various arithmetic invariants of E; explaining these is beyond the scope of this course.

1.4.3 L-functions attached to modular forms

Let n and k be positive integers, and let f be a modular form of weight k for the group $\Gamma_1(n)$, with q-expansion

$$f(z) = \sum_{m=0}^{\infty} a_m q^m \quad (q = \exp(2\pi i z)).$$

The *L-function* of f is defined as the Dirichlet series

$$L(f, s) = \sum_{m=1}^{\infty} a_m m^{-s}$$

for $\Re s > (k + 1)/2$. (Note that a_0 does not appear in the sum defining $L(f, s)$.)

Furthermore, we define the *completed L-function* attached to f as

$$\Lambda(f, s) = n^{s/2} \frac{\Gamma(s)}{(2\pi)^s} L(f, s).$$

Theorem 1.23. *Suppose f is a primitive cusp form. Then $\Lambda(f, s)$ can be continued to a holomorphic function on all of $\mathbb{C}$. Furthermore, there exist a primitive cusp form f^* and a complex number ϵ_f of absolute value 1 such that $\Lambda(f, s)$ and $\Lambda(f^*, s)$ are related by the functional equation*

$$\Lambda(f, k - s) = \epsilon_f \Lambda(f^*, s).$$

The proof of this theorem has some similarities to that of Theorem 1.2. The main tools are the theory of newforms, the Fricke (or Atkin–Lehner) operator w_n, and the Mellin transform.

The following theorem was proved by Wiles in 1993, with an important contribution by Taylor, in the case of *semi-stable* elliptic curves, i.e. curves having good or multiplicative reduction at every prime. The proof for general elliptic curves was finished by a sequence of papers by Breuil, Conrad, Diamond and Taylor.

Theorem 1.24 (Modularity of elliptic curves over $\mathbb{Q}$)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then there exist a positive integer n and a primitive cusp form f of weight 2 for the group $\Gamma_0(n)$ such that*

$$L(E,s) = L(f,s).$$

1.5 Exercises

Exercise 1.1. Let p be an odd prime number. Prove the following formulae for the Legendre symbol $\left(\frac{-}{p}\right)$:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4; \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8, \\ -1 & \text{if } p \equiv 3, 5 \pmod 8; \end{cases}$$

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 3 \pmod 8, \\ -1 & \text{if } p \equiv 5, 7 \pmod 8. \end{cases}$$

(*Hint:* embed the quadratic fields $\mathbb{Q}(\sqrt{d})$ for $d \in \{-1, 2, -2\}$ into the cyclotomic field $\mathbb{Q}(\zeta_8)$.)

Remark: Together with the quadratic reciprocity law $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$ for odd prime numbers $q \neq p$, these formulae make it possible to express $\left(\frac{a}{p}\right)$ in terms of congruence conditions on p for all $a \in \mathbb{Z}$.

Exercise 1.2. Let K be a quadratic field, and let ϵ_K be the unique injective homomorphism from $\mathrm{Gal}(K/\mathbb{Q})$ to $\mathbb{C}^\times$. Prove the identity

$$\zeta_K(s) = \zeta(s)L(\epsilon_K, s).$$

Exercise 1.3. Show that the character $\chi\colon I \to \mathbb{C}^\times$ defined in §1.2.4, where I the group of fractional ideals of $\mathbb{Z}[\sqrt{-1}]$, is injective.

Exercise 1.4. Let χ be a Dirichlet character modulo n. We consider the function $\mathbb{Z} \to \mathbb{C}$ sending an integer m to the complex number

$$\tau(\chi, m) = \sum_{j=0}^{n-1} \chi(j) \exp(2\pi i j m/n).$$

(This can be viewed as a discrete Fourier transform of χ.) The case $m = 1$ deserves special mention: the complex number

$$\tau(\chi) = \tau(\chi, 1) = \sum_{j=0}^{n-1} \chi(j) \exp(2\pi i j/n)$$

is called the *Gauss sum* attached to χ.

(a) Compute $\tau(\chi)$ for all non-trivial Dirichlet characters χ modulo 4 and modulo 5, respectively.

(b) Suppose that χ is primitive. Prove that for all $m \in \mathbb{Z}$ we have

$$\tau(\chi, m) = \bar{\chi}(m)\tau(\chi).$$

(*Hint:* writing $d = \gcd(m, n)$, distinguish the cases $d = 1$ and $d > 1$.)

(c) Deduce that if χ is primitive, we have

$$\tau(\chi)\tau(\bar{\chi}) = \chi(-1)n$$

and

$$\tau(\chi)\overline{\tau(\chi)} = n.$$

Exercise 1.5. Let χ be a primitive Dirichlet character modulo n. The *generalised Bernoulli numbers* attached to χ are the complex numbers $B_k(\chi)$ for $k \geq 0$ defined by the identity

$$\sum_{k=0}^{\infty} \frac{B_k(\chi)}{k!} t^k = \frac{t}{\exp(nt) - 1} \sum_{j=1}^{n} \chi(j) \exp(jt)$$

in the ring $\mathbb{C}[[t]]$ of formal power series in t.

(a) Prove that if χ is non-trivial (i.e. $n > 1$), then we have

$$\sum_{j=0}^{n-1} \chi(j) \frac{x + \exp(2\pi ij/n)}{x - \exp(2\pi ij/n)} = \frac{2n}{\tau(\bar{\chi})(x^n - 1)} \sum_{m=0}^{n-1} \bar{\chi}(m) x^m$$

in the field $\mathbb{C}(x)$ of rational functions in the variable x. (*Hint:* compute residues.)

(b) Prove that for every integer $k \geq 2$ such that $(-1)^k = \chi(-1)$, the special value of the Dirichlet L-function of χ at k is

$$L(\chi, k) = -\frac{(2\pi i)^k B_k(\bar{\chi})}{2\tau(\bar{\chi}) n^{k-1} k!}.$$

(*Hint:* use the identity $\frac{\cos z}{\sin z} = \frac{1}{z} + \sum_{m=1}^{\infty} \left(\frac{1}{z - m\pi} + \frac{1}{z + m\pi} \right)$.)

Exercise 1.6. Let q be an odd prime number, and let $q^* = (-1)^{(q-1)/2} q$. Use Gauss sums to prove that there exists an inclusion of fields

$$\mathbb{Q}(\sqrt{q^*}) \hookrightarrow \mathbb{Q}(\zeta_q).$$

Exercise 1.7. The *Fourier transform* of a quickly decreasing function $f \colon \mathbb{R} \to \mathbb{C}$ is defined by

$$\hat{f}(y) = \int_{-\infty}^{\infty} f(x) \exp(-2\pi ixy) dx.$$

(a) Let $f \colon \mathbb{R} \to \mathbb{C}$ be a quickly decreasing function, let $c \in \mathbb{R}$, and let $f_c(x) = f(x + c)$. Show that $\widehat{f_c}(y) = \exp(2\pi icy)\hat{f}(y)$.

(b) Let $f \colon \mathbb{R} \to \mathbb{C}$ be a quickly decreasing function, let $c > 0$, and let $f^c(x) = f(cx)$. Show that $\widehat{f^c}(y) = c^{-1}\hat{f}(y/c)$.

(c) Let $g_+(x) = \exp(-\pi x^2)$. Show that $\hat{g}_+(y) = g_+(y)$.

(d) Let $g_-(x) = \pi x \exp(-\pi x^2)$. Show that $\hat{g}_-(y) = -ig_-(y)$.

(*Hint* for (c) and (d): shift the line of integration in the complex plane.)

Exercise 1.8. Let n be a positive integer, and let χ be a primitive Dirichlet character modulo n. Recall that the Dirichlet L-function attached to χ is defined by

$$L(\chi, s) = \sum_{m=1}^{\infty} \chi(m) m^{-s} \quad \text{for } \Re s > 1.$$

Recall that χ is called *even* if $\chi(-1) = 1$ and *odd* if $\chi(-1) = -1$. We define the *completed Dirichlet L-function* $\Lambda(\chi, s)$ by

$$\Lambda(\chi, s) = \begin{cases} n^{s/2} \frac{\Gamma(s/2)}{\pi^{s/2}} L(\chi, s) & \text{if } \chi \text{ is even} \\ n^{s/2} \frac{\Gamma((s+1)/2)}{\pi^{(s-1)/2}} L(\chi, s) & \text{if } \chi \text{ is odd.} \end{cases}$$

The goal of this exercise is to generalise the proof of Theorem 1.2 to show that $\Lambda(\chi, s)$ admits an analytic continuation and functional equation.

We define two functions $g_+, g_- : \mathbb{R} \to \mathbb{C}$ by

$$g_+(x) = \exp(-\pi x^2),$$
$$g_-(x) = \pi x \exp(-\pi x^2).$$

For every primitive Dirichlet character χ modulo n, we define a function

$$\phi_\chi(t) = \begin{cases} \sum_{m \in \mathbb{Z}} \chi(m) g_+(mt) & \text{if } \chi \text{ is even,} \\ \sum_{m \in \mathbb{Z}} \chi(m) g_-(mt) & \text{if } \chi \text{ is odd.} \end{cases}$$

(a) Prove the identity

$$\phi_\chi(t) = \begin{cases} \frac{\tau(\chi)}{nt} \phi_{\bar{\chi}}\left(\frac{1}{nt}\right) & \text{if } \chi \text{ is even,} \\ \frac{\tau(\chi)}{int} \phi_{\bar{\chi}}\left(\frac{1}{nt}\right) & \text{if } \chi \text{ is odd.} \end{cases}$$

(*Hint:* use the Poisson summation formula and Exercises 1.4 and 1.7.)

From now on, we assume that χ is non-trivial, i.e. $n > 1$.

(b) Give asymptotic expressions for $\phi_\chi(t)$ as $t \to 0$ and as $t \to \infty$. (Note: the answer depends on χ.)

(c) Let $\mathcal{M}\phi_\chi$ be the Mellin transform of ϕ_χ,defined by

$$(\mathcal{M}\phi_\chi)(s) = \int_0^\infty \phi_\chi(t) t^s \frac{dt}{t}.$$

Prove that the integral converges for all $s \in \mathbb{C}$, and that the completed L-function can be expressed as

$$\Lambda(\chi, s) = n^{s/2} (\mathcal{M}\phi_\chi)(s) \quad \text{for } \Re s > 1.$$

(d) Conclude that $\Lambda(\chi, s)$ can be continued to a holomorphic function on all of $\mathbb{C}$ (without poles), and that $\Lambda(\chi, s)$ and $\Lambda(\bar{\chi}, s)$ are related by the functional equation

$$\Lambda(\chi, s) = \epsilon_\chi \Lambda(\bar{\chi}, 1 - s),$$

where ϵ_χ is the complex number of absolute value 1 defined by

$$\epsilon_\chi = \begin{cases} \frac{\tau(\chi)}{\sqrt{n}} & \text{if } \chi \text{ is even,} \\ \frac{\tau(\chi)}{i\sqrt{n}} & \text{if } \chi \text{ is odd.} \end{cases}$$

Exercise 1.9. Let $a, b \in \mathbb{Z}$, and suppose that the integer $\Delta = -16(4a^3 + 27b^2)$ is non-zero. Let E over $\mathbb{Z}[1/\Delta]$ be the elliptic curve given by the equation $y^2 = x^3 + ax + b$. Let p be a prime number not dividing Δ, and write

$$N_E(\mathbb{F}_p) = 1 + \#\{(x, y) \in \mathbb{F}_p \mid y^2 = x^3 + ax + b\}.$$

Prove that

$$N_E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(\left(\frac{x^3 + ax + b}{p} \right) + 1 \right)$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol.

Exercise 1.10. Up to isogeny, there are three distinct elliptic curves of conductor 57, namely

$$E_1 \colon y^2 + y = x^3 - x^2 - 2x + 2,$$
$$E_2 \colon y^2 + xy + y = x^3 - 2x - 1,$$
$$E_3 \colon y^2 + y = x^3 + x^2 + 20x - 32.$$

The newforms of weight 2 for the group $\Gamma_0(57)$ are

$$f_1 = q - 2q^2 - q^3 + 2q^4 - 3q^5 + O(q^6),$$
$$f_2 = q - 2q^2 + q^3 + 2q^4 + q^5 + O(q^6),$$
$$f_3 = q + q^2 + q^3 - q^4 - 2q^5 + O(q^6).$$

Which form corresponds to which elliptic curve under Wiles's modularity theorem?

Chapter 2

Algebraic number theory

Contents

In this chapter we will recall notions from algebraic number theory. Our goal is to set up the theory in sufficient generality so that we can work with it later. Unfortunately, realistically we cannot be self-contained here. Thus, we encourage the reader to also read up on algebraic number theory from Neukirch's book, the course of Stevenhagen, and the course on p-adic numbers.

2.1 Profinite groups

Topological groups and algebraic groups

In this course a central role will be played by groups that are equipped with a topology. This concept will be both important for automorphic forms and Galois representations.

Definition 2.1. A group (G, m) is a *topological group* if the underlying set G is equipped with the structure of a topological space such that the multiplication map $m\colon G \times G \to G$, $(g, h) \mapsto gh$ and the inversion map $G \to G$, $g \mapsto g^{-1}$ are continuous.

Example 2.2. The following groups are all topological groups

- $(\mathbb{R}^n, +)$, $(\mathbb{C}^n, +)$, $(\mathbb{R}^\times, \times)$, $(\mathbb{R}_{>0}, \times)$, $(\mathrm{GL}_n(\mathbb{R}), \cdot)$, $(\mathrm{GL}_n(\mathbb{C}), \cdot)$.
- $(\mathbb{R}/\mathbb{Z}) = S^1$, the circle group.
- The set of solutions $E(\mathbb{R}) \cup \{\infty\}$ to the equation $y^2 = x^3 + ax + b$ of an elliptic curve $E/\mathbb{R}$ adjoined with the point '∞' at infinity, with the usual addition of points where ∞ serves as the identity element for addition.
- Any finite group is a topological group for the discrete topology and also the indiscrete topology.
- An algebraic group $G/\mathbb{C}$ is actually a topological group for (at least) two topologies: The Zariski topology, and the complex topology on $G(\mathbb{C})$.
- .... and so on

Remark 2.3. A more formal way to think about topological groups is to use the concept of "group object". Consider a category $\mathcal{C}$ in which fibre products exist, so that in particular $\mathcal{C}$ has a terminal object t. If $A, B \in \mathcal{C}$ are objects, we write $A(B) = \mathrm{Hom}_{\mathcal{C}}(B, A)$. This way A can be viewed as a covariant functor from $\mathcal{C}$ to the category of sets (cf. the Yoneda lemma). A group object in $\mathcal{C}$ is a triple (G, e, m, i) with $G \in \mathcal{C}$ an object, $e\colon t \to G$ the 'unit element', $m\colon G \times G \to G$ the 'multiplication' and $i\colon G \to G$ the 'inversion', such that $(\star)$ for every test object $T \in \mathcal{C}$ the maps $m(T)$ and $i(T)$ on $G(T)$ turn the set $G(T)$ into a group with unit $t(T)(\bullet)$ (where '$\bullet$' is the unique element of $t(T)$). The condition $(\star)$ can also be stated be requiring that a certain amount of diagrams involving m and i are commutative (expressing for instance the fact that m should be associative). In this sense, a topological group is a group object in the category of topological spaces.

Apart from topological groups, a typical example are the Lie groups. A *Lie group* is a smooth manifold equipped with $\mathcal{C}^\infty$-maps $m\colon G \times G \to G$ and $i\colon G \to G$ making G into a group. Finally, in this course, *algebraic groups* will play an important role as well.

Definition 2.4. Let k be a commutative ring (for instance an algebraically closed field). An *algebraic group* over k is an affine or projective variety X over k with a section $e\colon \mathrm{spec}(k) \to X$, a multiplication morphism $m\colon X \times X \to X$ and an inversion morphism $i\colon X \to X$ satisfying the usual group axioms, *i.e.* (X, e, m, i) is a group object in the category of k-varieties.

Example 2.5. The following are all algebraic groups,

- The variety GL_n defined by the polynomial equation

$$\det \begin{pmatrix} X_{11} & X_{21} & \cdots & X_{n1} \\ X_{21} & X_{22} & \cdots & X_{n2} \\ \vdots & \vdots & & \vdots \\ X_{1n} & X_{2n} & \cdots & X_{nn} \end{pmatrix} \neq 0$$

  in n^2-dimensional affine space, with coordinates X_{11}, …, X_{nn}. The map sending X_{ij} to 1 if $i = j$ and to 0 otherwise defines the unit section $\operatorname{spec}(k) \to \mathrm{GL}_n$. The usual matrix product $(X_{ij})_{i,j=1}^n \cdot (Y_{ij})_{i,j=1}^n = (\sum_{k=1}^n X_{ik}Y_{kj})_{i,j=1}^n$ is a morphism of varieties $m\colon \mathrm{GL}_n \times \mathrm{GL}_n \to \mathrm{GL}_n$. Similarly, the inverse map $X = (X_{ij})_{i,j=1}^n \mapsto \frac{1}{\det(X)} \left(\det(X^{ij})\right)_{i,j=1}^n$ is a morphism of varieties (in the above formula X^{ij} is the minor of X, obtained by removing the i-th row and j-th column from X). Thus (G, e, m, i) is an algebraic group.

- The multiplicative group $\mathbb{G}_{\mathrm{m}} = \operatorname{spec} \mathbb{Z}[X^{\pm 1}]$.

- The additive group $\mathbb{G}_{\mathrm{a}} = \operatorname{spec} \mathbb{Z}[X]$.

- An elliptic curve $E/\mathbb{C}$ equipped with its usual addition is an algebraic group.

Projective limits

Let I be a set, and X_i for each $i \in I$ another set. We assume that I is equipped with an ordering $\leq$ that is *directed*, *i.e.* for every pair $i, j \in I$ there exists a k with $i \leq k$ and $j \leq k$. For every inequality $i \leq j$ we assume that we are given a map $f_{ji}\colon X_j \to X_i$ such that whenever $i \leq j \leq k$ we have $f_{ki} = f_{ji} \circ f_{kj}$ and $f_{ii} = \mathrm{id}_{X_i}$. We call the collection of all these data $(X_i, I, \leq, f_{ji})$ a *projective system of sets*. Viewing the ordered set $(I, \leq)$ as a category in the obvious way, one could also say that a projective system is a functor from the category I to the category of sets. The *projective limit* (or *inverse limit*) of the projective system (X_i, I, f_{ij}) is by definition the topological space

$$\varprojlim_{i \in I} X_i = \left\{ x = (x_i)_{i \in I} \in \prod_{i \in I} X_i \mid \text{for all } i, j \in I \text{ with } i \leq j\colon,\ f_{ji}(x_j) = x_i \right\}, \tag{2.1}$$

equipped with the topology induced from the product topology on $\prod_{i \in I} X_i$ with the X_i equipped with the discrete topology.

The projective limit $X = \varprojlim X_i$ has projections $p_i\colon X \to X_i$. Conversely, if any other set Y has maps $q_i\colon Y \to X_i$ such that that for all $i \leq j$ we have $f_{ji} \circ q_j = q_i$, then there exist a unique map $u\colon Y \to X$, such that $q_i = p_i \circ u$ for all $i \in I$. This is the *universal property* of the projective limit.

Example 2.6. Consider a sequence of rational numbers $(x_i)_{i=1}^{\infty} \in \mathbb{Q}$ converging to $\pi = 3.1415\ldots$ (for instance take the decimal approximations). Put $I = \mathbb{N}$ with the usual ordering of natural numbers. Put for each $i \in \mathbb{N}$, $X_i = \{x_1, x_2, \ldots, x_i\}$ with discrete topology, and whenever $i \leq j$ define the surjection $f_{ji}\colon X_j \to X_i$, $x_a \mapsto x_{\min(a,i)}$. Then $\varprojlim_{i \in I} X_i = \{x_1, x_2, \ldots, \pi\}$ with the weakest topology such that the points x_i, $i \in I$ are all open, and a system of open neighborhoods of π is given by the subsets whose complement is finite.

Example 2.7. Take X a set and let $(X_i)_{i\in I}$ be a 'decreasing' collection of subsets of X: Whenever $i \leq j$ we have $X_j \subset X_i$. Take the canonical inclusion maps f_{ji}. Then $(X, \leq, f_{ji})$ is a projective system. The projective limit of this system is the intersection $\bigcap_{i\in I} X_i \subset X$.

Example 2.8. Take I to be the set of number fields F that are contained in $\mathbb{C}$, and which are Galois over $\mathbb{Q}$. We write $F_1 \leq F_2$ whenever $F_1 \subset F_2$. We take for each $i \in I$ with corresponding number field $F_i \subset \mathbb{C}$, X_i equal to $\mathrm{Gal}(F_i/\mathbb{Q})$. Then $\varprojlim_{i\in I} \mathrm{Gal}(F_i/\mathbb{Q}) = \mathrm{Aut}_{\mathrm{field}}(\overline{\mathbb{Q}})$, where the topology on the automorphism group is the weakest topology such that for each $x \in \overline{\mathbb{Q}}$ the stabilizer is an open subgroup of $\mathrm{Aut}_{\mathrm{field}}(\overline{\mathbb{Q}})$. In fact, this will be one of our main examples of a projective limit.

Example 2.9. Consider the circle group $S^1 = \mathbb{R}/\mathbb{Z}$, take for each integer $N \in \mathbb{Z}$, $X_N = \mathbb{R}/N\mathbb{Z}$. If $M|N$ then we have the surjection $f_{NM}\colon X_N \to X_M$, $x \mapsto x \mod M\mathbb{Z}$. Then $\varprojlim_N X_N = \varprojlim_N \mathbb{R}/N\mathbb{Z}$ is called the *solenoid*.

Example 2.10. Consider for $N \in \mathbb{Z}$ the group $\Gamma(N)$ of matrices $g \in \mathrm{GL}_2(\mathbb{Z})$ such that $g \equiv \left(\begin{smallmatrix} 1 & 0 \\ 1 & 0 \end{smallmatrix}\right) \mod N$. Consider the upper half plane $\mathfrak{H}^{\pm} = \{z \in \mathbb{C} \mid \Im(z) \neq 0\}$. If $M|N$ we have the canonical surjection $p_{MN}\colon \Gamma(N)\backslash\mathfrak{H}^{\pm} \to \Gamma(M)\backslash\mathfrak{H}^{\pm}$, $x \mapsto \Gamma(M)x$. The projective limit $Y = \varprojlim_N \Gamma(N)\backslash\mathfrak{H}^{\pm}$ with respect to these maps p_{mn} is the modular curve of infinite level. As we defined it here, Y is a topological space, but, as it turns out, Y is has naturally the structure of a (non-noetherian) scheme.

Besides projective limits there are also inductive limits, basically obtained by making the arrows 'go in the other direction'. A first example is $\overline{\mathbb{Q}} = \varinjlim F$, where F ranges over the number fields contained in $\overline{\mathbb{Q}}$ (in fact any set-theoretic union is an inductive limit). We encourage the reader to read on this subject. Projective systems, inductive systems and limits of these can be defined in arbitrary categories, although they no longer need to automatically exist (just as a product objects, may, or may not exist in your favorite category $\mathcal{C}$). For instance a projective system of groups is a projective system of sets $(X_i, \leq, f_{ji})$, where the X_i are groups and the f_{ji} are group morphisms. This projective limit is a topological group (observe that the obvious group operations on (2.1) are indeed continuous), and thus all projective limits exist in the category of groups.

Example 2.11. The ring $R[[t]]$of formal power series over a commutative ring R is the projective limit the rings $R[t]/t^nR[t]$, ordered in the usual way, with the morphisms from $R[t]/t^{n+j}R[t]$ to $R[t]/t^nR[t]$ given by the natural projection. The topology on $R[[t]]$ coming from the projective limit is referred to as the *t-adic topology*.

Example 2.12. Let $\mathcal{O}_F$ be the ring of integers in a number field. Let $\mathfrak{p} \subset \mathcal{O}_F$ be a prime ideal. Then $\varprojlim_{n\in\mathbb{Z}_{\geq 1}} \mathcal{O}_F/\mathfrak{p}^n$ is the completion $\mathcal{O}_{F,\mathfrak{p}}$ of $\mathcal{O}_F$ at the prime $\mathfrak{p}$. The projective limit $\mathcal{O}_{F,\mathfrak{p}}$ is a complete discrete valuation ring.

Example 2.13. Continuing with the previous example, the group $\mathrm{GL}_d(\mathcal{O}_F)$ is profinite as well, obtained as the projective limit $\varprojlim_{n\in\mathbb{Z}_{\geq 1}} \mathrm{GL}_d(\mathcal{O}_F/\mathfrak{p}^n)$. In fact for any algebraic group G over $\mathcal{O}_F$, $G(\mathcal{O}_F)$ is profinite, given by a similar projective limit.

Profinite groups

Proposition 2.14. *Let G be a topological group. The following conditions are equivalent*

(i) G is a projective limit of finite discrete groups

(ii) The topological space underlying to G is Hausdorff, totally disconnected and compact.

(iii) The identity element $e \in G$ has a basis of open neighborhoods which are open subgroups of finite index in G.

These conditions are equivalent. If they are satisfied, we call the group G profinite.

The first examples of profinite groups are the (additive) groups $\mathbb{Z}_p$ of p-adic integers, and the group of profinite integers $\widehat{\mathbb{Z}}$. We define $\widehat{\mathbb{Z}} = \varprojlim_{N \in \mathbb{Z}_{\geq 1}} \mathbb{Z}/N\mathbb{Z}$, so $\widehat{\mathbb{Z}}$ is a profinite group. In fact, $\widehat{\mathbb{Z}}$ is even a topological ring, called the "Prüfer ring", or the ring of "profinite integers". Similarly, for each prime number p, $\mathbb{Z}_p$ is also a ring: "the ring of p-adic integers". By the Chinese remainder theorem the mapping $\widehat{\mathbb{Z}} \xrightarrow{\sim} \prod_p \mathbb{Z}_p$, $(x_N)_{N \in \mathbb{Z}_{\geq 1}} \mapsto \prod_{p \text{ prime}} (x_{p^n})_{n \in \mathbb{Z}_{\geq 1}}$ is an isomorphism of topological rings.

In fact, the group $\widehat{\mathbb{Z}}$ arises as the absolute Galois group of a finite field. For a finite extension $\mathbb{F}_{q^N}/\mathbb{F}_q$ we have the famous Frobenius automorphism $\mathrm{Frob}\colon \mathbb{F}_{q^N} \to \mathbb{F}_{q^N}$, $x \mapsto x^q$. This Frobenius allows us to identify $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ with $\widehat{\mathbb{Z}}$ via the isomorphism $\widehat{\mathbb{Z}} \xrightarrow{\sim} \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, $x \mapsto \mathrm{Frob}_q^x$. What does raising Frob_q to the power of the profinite integer x actually mean? Note that any $t \in \overline{\mathbb{F}}_q$ actually lies in a finite extension $\mathbb{F}_{q^N} \subset \overline{\mathbb{F}}_q$ for $N \in \mathbb{Z}_{\geq 1}$ sufficiently large. Then for $x = (x_N) \in \widehat{\mathbb{Z}}$ the power Frob_q^x acts on t as $\mathrm{Frob}_q^{x_N}$, which by the divisibility relations does not depend on the choice of N. We will see that Galois theory goes through to the infinite setting and gives an inclusion reversing bijection between the closed subgroups H of a Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ and the subfields $M \subset \overline{\mathbb{F}}_q$ that contain $\mathbb{F}_q$. In Exercise 2.16 we use this statement to classify all the algebraic extensions of $\mathbb{F}_q$.

Locally profinite groups

Let G be a totally disconnected locally compact topological group, then G is called *locally profinite*. Equivalently, a topological group is locally profinite if and only if there exists an open profinite subgroup $K \subset G$ (Exercise 2.5). A typical example is the group $\mathbb{Q}_p$, with open profinite subgroup $\mathbb{Z}_p \subset \mathbb{Q}_p$. Another example is $\mathrm{GL}_n(\mathbb{Q}_p)$, which is locally profinite and has $\mathrm{GL}_n(\mathbb{Z}_p)$ as profinite open subgroup. At first the study of these locally profinite groups may appear like a 'niche', but later in the course the groups $\mathrm{GL}_n(\mathbb{Q}_p)$ play a crucial role in describing the prime factor components of automorphic representations.

The topology on $\mathrm{GL}_n(R)$, R a topological ring

Consider a topological ring R. Then we can make $\mathrm{GL}_n(R)$ into a topological ring by pulling back the topology via the inclusion $i_1\colon \mathrm{GL}_n(R) \to \mathrm{M}_n(R) \times \mathrm{M}_n(R)$, $g \mapsto (g, g^{-1})$, where $\mathrm{M}_n(R) \times \mathrm{M}_n(R) \cong R^{2n^2}$ has the product topology. In many cases, for instance when $R = \mathbb{Q}_p, \mathbb{C}, \mathbb{R}$ it turns out that this topology is the same as pulling back the topology from the inclusion $i_2\colon \mathrm{GL}_n(R) \to \mathrm{M}_n(R)$, $g \mapsto g$, with $\mathrm{M}_n(R) \cong R^{n^2}$ the product topology. However, this is not always the case. The problem if you use i_2 as opposed to i_1, the inversion mapping $\mathrm{GL}_n(R) \to \mathrm{GL}_n(R), g \mapsto g^{-1}$ is no longer guaranteed to be continuous. Hence, one should use i_1 to define the topology. The standard counter example is the ring of adèles, which we will encounter later in the course.

2.2 Galois theory for infinite extensions

Apart from studying Galois groups of finite Galois extensions of fields L/F it will be important for us to also consider infinite Galois extensions L/F.

We call the extension L/F *algebraic*, if for every element $x \in L$ there exists a polynomial $f \in F[X]$ such that $f(x) = 0$. The extension is *separable* if, for all $x \in L$, we can choose the polynomial f such that it has no repeated roots over $\overline{F}$. The extension is *normal* if the minimal polynomial of x over F splits completely in L. Finally we call L/F *Galois* if it is normal and separable. As in the finite case, the *Galois group* $\mathrm{Gal}(L/F)$ is then the group of field automorphisms $\sigma\colon L \xrightarrow{\sim} L$ that are the identity on F. The group $\mathrm{Gal}(L/F)$ is given the weakest topology such that the stabilizers

$$\mathrm{Gal}(L/F)_x = \{\sigma \in \mathrm{Gal}(L/F) \mid \sigma(x) = x\} \subset \mathrm{Gal}(L/F), \tag{2.2}$$

are open, for all $x \in L$. Equivalently, $\mathrm{Gal}(L/F)$ identifies with the projective limit

$$\mathrm{Gal}(L/F) = \varprojlim_{M} \mathrm{Gal}(M/F), \tag{2.3}$$

where M ranges over all finite Galois extensions of F that are contained in L. If M, M' are two such fields with $M \subset M'$, then we have the map $p_{M',M}\colon \mathrm{Gal}(M'/F) \to \mathrm{Gal}(M/F)$, $\sigma \mapsto \sigma|_M$. The projective limit in (2.3) is taken with respect to the maps $p_{M',M}$. In Exercise 2.17 you will show that the topology on $\mathrm{Gal}(L/F)$ defined in (2.3) is equivalent to the topology from (2.2).

Theorem 2.15 (Galois theory for infinite extensions)**.** *Let L/F be a Galois extension of fields. The mapping*

$$\Psi\colon \{M \mid F \subset M \subset L\} \to \{\text{closed subgroups } H \subset \mathrm{Gal}(L/F)\}, \quad M \mapsto \mathrm{Gal}(L/M),$$

is a bijection with inverse $H \mapsto L^H$. Let H, H' be closed subgroups of $\mathrm{Gal}(L/F)$ with corresponding fields M, M'. Then

(i) $M \subset M'$ if and only if $H \supset H'$.

(ii) Assume $M \subset M'$. The extension M'/M is finite if and only if H' is of finite index in H. Moreover, $[M' : M] = [H : H']$.

(iii) L/M is Galois with group $\mathrm{Gal}(L/M) = H$

(iv) $\sigma(M)$ corresponds to $\sigma H \sigma^{-1}$ for all $\sigma \in \mathrm{Gal}(L/F)$.

(v) M/F is Galois if and only if the subgroup $H \subset \mathrm{Gal}(L/F)$ is normal, and $\mathrm{Gal}(M/F) = \mathrm{Gal}(L/F)/H$.

2.3 Local p-adic fields

The p-adic numbers

Let p be a prime number. The ring of p-adic integers $\mathbb{Z}_p$ is defined as the projective limit $\varprojlim_{n \in \mathbb{Z}_{\geq 0}} \mathbb{Z}/p^n\mathbb{Z}$ taken with respect to the surjections $\mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ whenever $m \geq n$.

A second way to think about the p-adic integers is as infinite sequences $x = a_0 + a_1p^1 + a_2p^2 + a_3p^3 + \ldots$ with $a_i \in \{0, 1, 2, \ldots, p-1\}$. If $y = b_0 + b_1p^1 + b_2p^2 + b_3p^3 + \ldots$ is another such p-adic integer, we have the usual formula $x+y = (a_0+b_0)+(a_1+b_1)p^1+(a_2+b_2)p^2+\ldots$ for addition, and the usual formula

$$x \cdot y = a_0b_0 + (a_1b_0 + a_0b_1)p^1 + (a_2b_0 + a_1b_1 + a_0b_2)p^2 + \\ + (a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3)p^3 + \ldots$$

for multiplication. The p-adic integer x corresponds to the element

$$\left(a_0 + a_1p^1 + a_2p^2 + \ldots + a_np^n\right)_{n\in\mathbb{Z}_{\geq 0}} \in \varprojlim_{n\in\mathbb{Z}_{\geq 0}} \mathbb{Z}_p/p^n\mathbb{Z}_p.$$

If $x \in \mathbb{Z}_p$, we write $v_p(x)$ for the largest integer n such that $x \equiv 0 \mod p^n$. Then $v_p(x)$ is the valuation on $\mathbb{Z}_p$. We define the norm $|\cdot|_p$ by the formula $|x|_p = p^{-v_p(x)}$. The p-adic valuation and p-adic norm $|x|_p$ make sense for integers $x \in \mathbb{Z}$ as well. In particular we can introduce a notion of *p-adic Cauchy sequence of integers*: Let $(x_i)_{i\in\mathbb{Z}_{\geq 0}}$ a sequence of integers $x_i \in \mathbb{Z}$, then it is *p-Cauchy*, if for every $\varepsilon > 0$ there exists an integer $M \in \mathbb{Z}_{\geq 1}$ such that for all $m, n > M$ we have $|x_m - x_n|_p < \varepsilon$. In this sense $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$. Via the distance function $d(x, y) = |x - y|_p$, $\mathbb{Z}_p$ is a metric space.

Example 2.16. If N is an integer that is coprime to p, then N has an inverse y_n modulo p^n, for every n. Moreover these y_N are unique, and hence form an element of the projective system $(y_N) \in \varprojlim_{n\in\mathbb{Z}_{\geq 1}} \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$.

By the example, $\mathbb{Z}_p$ contains the localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at the prime ideal (p). Just as $\mathbb{Z}_{(p)}$, the ring $\mathbb{Z}_p$ is a discrete valuation ring with prime ideals (0) and (p). So $\mathbb{Z}_p$ is a completion of $\mathbb{Z}_{(p)}$. In fact any local ring $(R, \mathfrak{m})$ can be completed for its $\mathfrak{m}$-adic topology, by taking the projective limit over the quotients $R/\mathfrak{m}^n$. For example, we will often consider completions at the various prime ideals of the ring of integers of a number field.

We define the *field of p-adic numbers* $\mathbb{Q}_p$ to be the fraction field of $\mathbb{Z}_p$. Similar to $\mathbb{Z}_p$, the elements of $x = \mathbb{Q}_p$ can be expressed as series $x = \sum_{i\in\mathbb{Z}} a_ip^i$, where $a_i \in \{0, 1, 2, \ldots, p-1\}$ and such that for some $M \in \mathbb{Z}$ we have $a_i = 0$ for all $i < M$. The topology on $\mathbb{Q}_p$ is the weakest such that $\mathbb{Z}_p \subset \mathbb{Q}_p$ is an open subring. The valuation v on $\mathbb{Z}_p$ extends to $\mathbb{Q}_p$ by setting $v(x) = v(a) - v(b)$ if $x = a/b \in \mathbb{Q}_p$ with $a, b \in \mathbb{Z}_p$ and $b \neq 0$. One checks easily that $v(x)$ does not depend on the choice of a and b.

Norms

Let F be a field. A *norm* on F is a function $|\cdot|: F \to \mathbb{R}_{\geq 0}$ satisfying

(N1) for all $x \in F$, $|x| = 0$ if and only if $x = 0$,

(N2) for all $x, y \in F$, $|xy| = |x||y|$,

(N3) for all $x, y \in F$, $|x + y| \leq |x| + |y|$.

Example 2.17. The trivial norm: $|x| = 1$ if and only if $x \neq 0$ is a norm on any field. Other than this one we have $|\cdot|_p$ and the absolute value on $\mathbb{Q}$, which are both norms.

Let F be normed field. A sequence $(x_i)_{i=1}^{\infty}$ of elements $x_i \in F$ is a *Cauchy sequence* if for all $\varepsilon > 0$, there exists $N > 0$ such that for all $n, m \geq N$ we have $|x_n - x_m| < \varepsilon$. The space F is *complete* if every Cauchy sequence converges. We say that two norms $|\cdot|_1$, $|\cdot|_2$ on a field are *equivalent* if a sequence of elements x_i is Cauchy for the one norm, if and only if it is Cauchy for the other norm. It turns out that $|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if $|\cdot|_2^{\alpha} = |\cdot|_1$ for some $\alpha > 0$.

Theorem 2.18 (Ostrowski's theorem)**.** *Any non-trivial norm $|\cdot|$ on $\mathbb{Q}$ is equivalent to either the usual norm or a p-adic norm for some prime number p.*

We call a norm $|\cdot|$ *non-Archimedean*, if it satisfies the stronger condition

(N3+) $|x + y| \leq \max(|x|, |y|)$.

When working with number fields and p-adic fields, all the non-archimedean norms are *discrete*. We call $|\cdot|$ *discrete* if for every positive real number x there exists an open neighborhood $U \subset \mathbb{R}_{>0}$ of x such that $|F| \cap U = \{x\}$.

Places of a number field

If F is a number field, we write Σ_F for the set of non-trivial norms on F, taken modulo equivalence. We call the elements of Σ_F the *places* or *F-places* if the field F is not clear from the context. We have seen that $\Sigma_{\mathbb{Q}} = \{\infty, 2, 3, 5, \dots, \}$ so the elements of Σ_F can be thought of as an extension of the set of primes, in the following sense

Lemma 2.19. *Write Σ_F^{∞} for the finite F-places. The mapping*

$$\Sigma_F^{\infty} \to \{\text{non-zero prime ideals } \mathfrak{p} \subset \mathcal{O}_F\}, \quad v \mapsto \{x \in \mathcal{O}_F \mid |x|_v < 1\}$$

is a bijection.

In general if L/F is an extension of number fields, we have the mapping $\Sigma_L \to \Sigma_F$, $w \mapsto v$ given by restricting a norm $|\cdot|_w$ on L to the subfield $F \subset L$, which yields a norm $|\cdot|_v$ on F that corresponds to a place $v \in \Sigma_F$. The fibres of this map are finite, and we say that the place w *lies above* v, and that v *lies under* w.

Completion

Recall that $\mathbb{R}$ is constructed from $\mathbb{Q}$ using Cauchy sequences. In fact, we may carry out this construction in much greater generality. Let F be a number field and $v \in \Sigma_F$ be a place with corresponding norm $|\cdot|_v$. Then $(F, |\cdot|_v)$ is not complete, but, we can form its completion F_v. This completion is a map $i_v \colon F \to F_v$, with the following universal property. For any morphism $f \colon F \to M$ of F into a normed field M, such that $|x|_F = |f(x)|_M$ and for any Cauchy sequence $(x_i)_{i=1}^{\infty}$ in F the sequence $(f(x_i))_{i=1}^{\infty}$ has a limit point in M, there exists a unique map from $u \colon F_v \to M$ such that $u \circ i_v = f$. The field F_v can be constructed from F by considering the ring $\mathcal{R}$ of all Cauchy sequences and taking the quotient by the ideal $\mathcal{I}$ in $\mathcal{R}$ of sequences that converge to 0.

Example 2.20. The field $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ for the p-adic norm $|\cdot|_p$.

Norms on a vector space

If V is a finite-dimensional vector space over a normed field $(F, |\cdot|)$, a *norm* on V is a function $\|\cdot\|\colon V \to \mathbb{R}_{\geq 0}$ satisfying

(NV1) for all $v \in V$, we have $\|v\| = 0$ if and only if $v = 0$,

(NV2) for all $v \in V$ and $\lambda \in F$, we have $\|\lambda v\| = |\lambda|\|v\|$,

(NV3) for all $v, w \in V$, we have $\|v + w\| \leq \|v\| + \|w\|$.

Example 2.21. If $V = F^n$, then $v = \sum_{i=1}^n v_i e_i \mapsto \|v\|_{\max} := \max_{i=1}^n |v_i|$ is a norm on V.

Proposition 2.22. *Let F be a normed field which is complete. Let V be a finite-dimensional vector space over F. Let $\|\cdot\|_1, \|\cdot\|_2$ be two norms on V. Then there exist constants $c, C \in \mathbb{R}_{>0}$ such that for all $v \in V$ we have $c\|v\|_1 \leq \|v\|_2 \leq C\|v\|_2$, i.e. all norms on V are equivalent.*

Valuations

To any non-Archimedean norm we may attach a valuation by taking the logarithm. Even though the one can be deduced by a simple formula from the other, it is often more convenient and intuitive to use both concepts. A *valuation* v on a field F is a mapping $F \to \mathbb{R}_{\geq 0}$ such that

(V1) $v_F(x) = \infty$ if and only if $x = 0$,

(V2) $v_F(xy) = v_F(x) + v_F(y)$,

(V3) $v_F(x + y) \geq \min(v_F(x), v_F(y))$,

for all $x, y \in F$.

p-Adic fields

Let F be a non-Archimedean local field. With this we mean a field F that is equipped with a discrete norm $|\cdot|_F$ which induces a locally compact topology on F. It turns out that these fields F are precisely those fields that are obtained as a finite extensions of $\mathbb{Q}_p$ for some prime number p.

Proposition 2.23. *(i) The topology on F is totally disconnected and $|\cdot|_F$ is non-Archimedean. In particular the topology on F is induced from a discrete valuation $v_F\colon F \to \mathbb{Z} \cup \{\infty\}$.*

*(ii) The subset $\mathcal{O}_F = \{x \in F \mid |x|_F \leq 1\} \subset F$ is a subring (*the ring of integers*).*

(iii) The subset $\mathfrak{p} = \{x \in F \mid |x|_F < 1\} \subset \mathcal{O}_F$ is a maximal ideal.

(iv) $\mathcal{O}_F \subset F$ is profinite and equal to the projective limit $\varprojlim_{n \in \mathbb{Z}_{\geq 0}} \mathcal{O}_F/\mathfrak{p}^n$.

(v) $\mathcal{O}_F$ is local.

(vi) $\mathcal{O}_F$ is a discrete valuation ring.

(vii) $\mathcal{O}_F$ is of finite type over $\mathbb{Z}_p$ (and hence the integral closure of $\mathbb{Z}_p$ in F).

Proof. (i) If $|\cdot|_F$ were Archimedean, then F would be $\mathbb{R}$ or $\mathbb{C}$, which do not have a discrete norm. Thus (N3+) must hold, and then (N3+) implies that the topology on F is totally disconnected. Since the norm is non-Archimedean, it induces a valuation v_F on F, which we may normalize so that it has value group $\mathbb{Z}$.

(ii) By (N2), $\mathcal{O}_F$ is stable under multiplication, and by (N3+), $\mathcal{O}_F$ is stable under addition, since also $0, 1 \in \mathcal{O}_F$ it is indeed an open subring of F.

For (iii) it is easy to see that $\mathfrak{p}$ is an ideal. It is also prime, since if $|xy| < 1$ for $|x|, |y| \leq 1$ we must have $|x| < 1$ or $|y| < 1$. In (iv) we will see that the index of $\mathfrak{p}$ in $\mathcal{O}_F$ is finite. Thus $\mathcal{O}_F/\mathfrak{p}$ is a finite domain and therefore a field.

(iv) Note that $\mathfrak{p}$ and $\mathcal{O}_F$ are open subsets of F. Moreover, since we assumed F to be locally compact, $\mathcal{O}_F$ must contain an open neighborhood U of 1 with compact closure $\overline{U}$ in F. Since the topology on F is induced from the norm, we have $s \in \mathbb{Z}$ large enough such that $\mathfrak{p}^s \subset U$. Thus $\mathfrak{p}^s$ is compact, hence profinite. The cosets of $\mathfrak{p}^{s+1}$ form a disjoint open covering of $\mathfrak{p}^s$, which must be finite. By multiplying with a uniformizer we get bijections $\mathfrak{p}^t/\mathfrak{p}^{t-1} \cong \mathfrak{p}^{t-1}/\mathfrak{p}^{t-2}$. Thus all the $\mathfrak{p}^t/\mathfrak{p}^{t-1}$ are finite. Hence $\mathcal{O}_F$ is profinite.

(v) If $x \in \mathcal{O}_F \backslash \mathfrak{p}$, then $|x|_F = 1$, hence $|x^{-1}|_F = 1$ as well and thus $x \in \mathcal{O}_F^\times$. Hence any element not in $\mathfrak{p}$ is a unit, and therefore $\mathcal{O}_F$ is local.

(vi) Exercise.

(vii) One way to see this is to use a topological version of Nakayama's lemma, which states that if you have a pro-p profinite ring Λ, a Λ-module X, also pro-p profinite, and $I \subset \Lambda$ a closed ideal. Then X is of finite type over Λ if and only if X/I is of finite type over Λ/I; see Serre [12, page 89]. By this lemma, it suffices to show that $\mathcal{O}_F/p\mathcal{O}_F$ is finite, which is true. □

Convention on normalizations

Both the valuation and norm on a p-adic F can be normalized is several ways. For now in, these notes we will work with the convention that $|\cdot|_F$ has no preferred normalization, so strictly speaking, we work with $|\cdot|_F$ well-defined only up to positive powers. However, we will normalize the valuation v_F in such a way that its value group is $\mathbb{Z}$. In particular $v_F(\varpi_F) = 1$, where $\varpi_F \in F$ is a uniformizer, *i.e.* a generator of the non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_F$.

Hensel's lemma

Arguably the most important basic result in the theory of p-adic integers is Hensel's lemma. Let us first illustrate the lemma with an example.

Example 2.24. The number 7 is a square modulo 3, since $7 \equiv 1^2 \mod 3$. Even though 7 is not congruent to 1^2 modulo 25, we can replace $x_1 = 1$ with $x_2 = 1 + a \cdot 3$, and find the equation $(1 + a_1 \cdot 3)^2 \equiv 1 + 6a \mod 3^2$ which is satisfied for $a = 1$, so $x_2 = 1 + 3^1$ is a root of 7 modulo 3^2. Similarly, if $x_3 = (1 + a_1 \cdot 3 + a_2 \cdot 3^2)$ for some $a_2 \in \{0, 1, 2\}$. Then

$$7 \equiv x_3^2 \equiv (x_2 + a_2 \cdot 3^2) \equiv x_2^2 + 2x_2 a_2 3^2 \equiv 16 + 8a_2 3^2 \mod 3^3$$

Hence $a_2 = 1$. Inductively, if we have

$$x_{n-1}^2 = (a_0 + a_1 3^1 + a_2 3^2 + \ldots + a_{n-1}5^{n-1})^2 \equiv 7 \mod 3^n$$

with $a_i \in \{0, 1, 2\}$, then we can solve for a_n the equation $(x_{n-1} + a_n 3^n)^2 \equiv 7 \mod 3^{n+1}$ which rewrites to (noting that $2x_{n-1} \not\equiv 0 \mod 3$, so $2x_{n-1} \in (\mathbb{Z}/3^{n+1}\mathbb{Z})^\times$)

$$a_n 3^n \equiv \frac{7 - x_{n-1}^2}{2x_{n-1}} \mod 3^{n+1}.$$

Since $7 \equiv x_{n-1}^2 \mod 3^n$, there is a unique choice for $a_n \in \{0, 1, 2\}$ satisfying this congruence. Hence we have inductively defined a sequence of approximations x_n of $\sqrt{7}$ in $\mathbb{Z}_3$. Since these approximations x_n are 'correct' modulo 3^n, the sequence x_n is Cauchy for $|\cdot|_3$ and hence converges to a 3-adic integer which we denote by the symbol $\sqrt{7} \in \mathbb{Z}_3$. Note for a_0 we had two choices, we chose $a_0 = 1$ for no good reason as we could also have taken $a_0 = 2$. After a_0 has been fixed, the a_i for $i > 0$ are uniquely determined by the above inductive procedure. This reflects the fact that, as in any domain of characteristic $\neq 2, 7$, we have two (or zero!) choices for the square root $\pm\sqrt{7}$ of 7.

Proposition 2.25 (Hensel's lemma)**.** *Let $f \in \mathbb{Z}_p[X]$ be a monic polynomial such that $f(x) \equiv 0 \mod p$ for some $x \in \mathbb{Z}_p$ and $f'(x) \neq 0 \mod p$. Then f has a root α in $\mathbb{Z}_p$ such that $\alpha \equiv x \mod p$.*

Sketch. Define a_n inductively by $a_0 = x$, $a_{n+1} = a_n - f(a_n)y$, where $y \in \mathbb{Z}$ is a lift of the inverse of $f'(x)$ modulo p. Now show that $\lim_{n\to\infty} a_n = \alpha$. □

Example 2.26. For any prime number p the $p-1$-th roots of unity lie in $\mathbb{Z}_p$. To see this, consider the cyclotomic polynomial $\Phi_{p-1} \in \mathbb{Z}_p[X]$. For $\zeta \in \mathbb{F}_p$ a generator of $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, we have $\overline{\Phi}_{p-1}(\zeta) = 0$. Moreover, Φ_{p-1} divides the polynomial X^{p-1} which is separable modulo p. If the derivative $\frac{d}{dX}\overline{\Phi}_{p-1}(\zeta)$ were 0 then ζ would be a repeated zero of $\overline{\Phi}_{p-1}|X^{p-1} - 1$. Hence $\Phi'_{p-1}(\zeta) \neq 0$. By Hensel's lemma ζ lifts to a root in $\mathbb{Z}_p$.

Hensel's lemma has many more forms. The first obvious generalizations are from $\mathbb{Q}_p$ to p-adic fields F, and instead of linear factors modulo p, look at lifting a factorization of a polynomial that exists modulo $\mathfrak{p}$ to a factorization in $\mathcal{O}_F[x]$.

Proposition 2.27. *Assume that $f \in \mathcal{O}_F[X]$ is a monic polynomial, and that $\overline{f} \in \kappa_F[X]$ factors into a product $\overline{f} = h \cdot g$ of two monic, relatively prime polynomials $h, g \in \kappa_F[X]$. Then there exists polynomials $H, G \in \mathcal{O}_F[X]$ such that $H \cdot G = f$ and $\overline{H} = h$, $\overline{G} = g$.*

Another, very general form of Hensel's lemma is given in EGA IV [**?**, 18.5.17].

Theorem 2.28. *Let R be an Henselian local ring with maximal ideal $\mathfrak{m}$, and let X be a smooth R-scheme. Then $X(R) \to X(R/\mathfrak{m})$ is surjective.*

In this theorem a local ring $(R, \mathfrak{m})$ is 'Henselian' if R satisfies the conclusion of Proposition 2.25 stating that a mod $\mathfrak{m}$ root α of a polynomial f lifts if $f'(\alpha) \notin \mathfrak{m}$. There are many equivalent ways to characterize henselian rings [16, Tag 04GE]. In particular the ring $\mathcal{O}_F$ for F a p-adic field is Henselian. Another example of an Henselian ring is $\mathbb{Z}_{(p)}^h$, by which we mean the ring of all $\alpha \in \mathbb{Z}_p$ that are algebraic over $\mathbb{Q}$. Since $\mathbb{Z}_{(p)}^h$ is countable while $\mathbb{Z}_p$ is uncountable, the subring $\mathbb{Z}_{(p)}^h \subset \mathbb{Z}_p$ is strict with a 'huge' index.

For readers which are not familiar with schemes, we spell out explicitly what Theorem 2.28 translates to in terms of a system of polynomials (affine R-schemes). Suppose that we are given a collection of polynomials $f_1, f_2, \ldots, f_n \in R[X_1, X_2, \ldots, X_d]$ and elements $\alpha_1, \alpha_2, \ldots, \alpha_d \in R/\mathfrak{m}$ such that $\overline{f}_i(\alpha_1, \alpha_2, \ldots, \alpha_d) = 0 \in R/\mathfrak{m}$ for $i = 1, 2, \ldots, n$ and the *Jacobian matrix*

$$\mathrm{Jac}(\alpha_1, \alpha_2, \ldots, \alpha_d) = \begin{pmatrix} \frac{\partial \overline{f}_1(\alpha_1)}{\partial X_1} & \frac{\partial \overline{f}_1(\alpha_1)}{\partial X_2} & \cdots & \frac{\partial \overline{f}_1(\alpha_1)}{\partial X_d} \\ \frac{\partial \overline{f}_2(\alpha_1)}{\partial X_1} & \frac{\partial \overline{f}_1(\alpha_2)}{\partial X_2} & \cdots & \frac{\partial \overline{f}_1(\alpha_2)}{\partial X_d} \\ \vdots & \vdots & & \vdots \\ \frac{\partial \overline{f}_n(\alpha_1)}{\partial X_1} & \frac{\partial \overline{f}_n(\alpha_2)}{\partial X_2} & \cdots & \frac{\partial \overline{f}_n(\alpha_2)}{\partial X_d} \end{pmatrix} \in \mathrm{Mat}_{d \times n}(R/\mathfrak{m})$$

has maximal rank $d - n$ (in general the rank of $\mathrm{Jac}(\alpha_1, \alpha_2, \ldots, \alpha_d)$ is at most $d - n$). Then Theorem 2.28 states that $\alpha_1, \alpha_2, \ldots, \alpha_d$ lift to elements $\widetilde{\alpha}_1, \widetilde{\alpha}_2, \ldots, \widetilde{\alpha}_d \in R$ such that $f_i(\widetilde{\alpha}_1, \widetilde{\alpha}_2, \ldots, \widetilde{\alpha}_d) = 0 \in R$ for $i = 1, 2, \ldots, n$.

Example 2.29. Consider the (affine part of the) elliptic curve E over $\mathbb{Z}_p$ given by the equation $Y^2 = X^3 + aX + b$, so with discriminant $\Delta = -16(4a^3 + 27b^2)$ not divisible by p. The Jacobian matrix J is given by $\Big(3x^2 + a, -2y\Big)$. If the rank of $J_{\mathbb{F}_p}$ were $0 < 1$ at some point $(x, y) \in \mathbb{F}_p^2$, then both entries of $J(x, y)$ had to be zero modulo p, and then the polynomial $f = X^3 + aX + b$ has a root in common with its derivative $3X^2 + a$, contradicting $\Delta \not\equiv 0 \mod p$. Thus the mapping $E(\mathbb{Z}_p) \to E(\mathbb{F}_p)$ is surjective. More abstactly, any elliptic curve is *smooth*, so Theorem 2.28 applies.

Finite extensions of p-adic fields

Let L/F be a finite extension of p-adic fields. Let $N_{L/F} \colon L \to F$, be the norm mapping from Galois theory, *i.e.* if $x \in L$, let x act on $L \cong F^n$ by multiplication, which gives a matrix $M_x \in \mathrm{M}_n(F)$, well-defined up to conjugacy. We put $N_{L/F}(x) := \det(M_x)$, which does not depend on the choice of basis. Recall that $N_{L/F}$ is compatible in towers, and if $\alpha \in L$ is a primitive element, then $N_{L/F}(\alpha)$ is (up to sign) the constant term of the minimal polynomial of α over F.

Proposition 2.30. *The mapping $x \mapsto |N_{L/F}(x)|$ defines a norm on L.*

Proof. The properties (N1) and (N2) being easy; let us focus on showing (N3+). We have to show that for all $x, y \in L$

$$|N_{L/F}(x + y)|_F \leq \max(|N_{L/F}(x)|_F, |N_{L/F}(y)|_F).$$

We may assume that $x/y \in \mathcal{O}_L$ (otherwise $y/x \in \mathcal{O}_L$, and we can relabel). Dividing by y, it is equivalent to show that for all $x \in \mathcal{O}_L$ we have

$$|N_{L/F}(x + 1)|_F \leq \max(|N_{L/F}(x)|_F, 1).$$

Since $x \in \mathcal{O}_L$, we have $x + 1 \in \mathcal{O}_L$ as well. The statement thus reduces to $N_{L/F}\mathcal{O}_L \subset \mathcal{O}_F$, which is clear. □

Eisenstein polynomials

When studying extensions of local fields a crucial role is played by the Eisenstein polynomials. Later we will see that these polynomials give precisely the totally ramified extensions.

Proposition 2.31. *Let $f = a_0 + a_1X^1 + a_2X^2 + \ldots + X^n \in \mathcal{O}_F[X]$ be a monic polynomial of degree n whose constant term a_0 has $v_F(a_0) = 1$. Then f is irreducible if and only if $a_i \in \mathfrak{p}$ for all i. In this case we call f an* Eisenstein polynomial.

Proof. Assume f is Eisenstein and $f = g \cdot h$ is a factorization of f in $F[X]$ where we may assume g and h are monic. Any algebraic number that is a root of g is also a root of f and hence is integral. Modulo $\mathfrak{p}$ we have $\overline{g} \cdot \overline{h} \equiv X^n$, hence every non-leading coefficient of g and h lies in $\mathfrak{p}$. Let g_0 (resp. h_0) be the constant coefficient of g (resp. v). Then $g_0h_0 = a_0$, the constant coefficient of f. Since $a_0 \in \mathfrak{p}\backslash\mathfrak{p}^2$ exactly one of the two coefficients $\{g_0, h_0\}$ lies in $\mathfrak{p}$. Say it is g_0. Then h_0 is a unit, and hence must be the leading coefficient of h (because we established that all other coefficients lie in $\mathfrak{p}$). Thus $\deg(h) = 0$ and f is irreducible. Conversely, assume that f is irreducible and $v_F(a_0) = 1$. Modulo $\mathfrak{p}$ we may factor $\overline{f} = X^i \cdot \overline{g}$ where $\overline{g} \in \kappa_F[X]$ is some polynomial with non-zero constant term. By Hensel's lemma this factorization lifts to a factorization $f = h \cdot g$ with $\overline{h} = X^i$. Since $\deg(h) > 1$, we must have $\deg(h) = \deg(f)$ and $\deg(g) = 0$ by irreducibility of f. Thus $\overline{f} = X^{\deg(f)}$ and f is an Eisenstein polynomial. □

Example 2.32. For an odd prime number p there are by Exercise 2.44 exactly $3 = \#\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times,2} - 1$ quadratic extensions. They are easily written down: $\mathbb{Q}_p(\sqrt{\zeta})$, $\mathbb{Q}_p(\sqrt{p})$, $\mathbb{Q}_p(\sqrt{\zeta p})$, where $\zeta \in \mathbb{Q}_p$ is a primitive root of unity of order $p-1$ (cf. Example 2.26). The quadratic extension $\mathbb{Q}_p(\sqrt{\zeta})$ is 'unramified' and hence can not given by an Eisenstein polynomial (this will be explained in the next section). The other two minimal polynomials are $X^2 + p$ and $X^2 + \zeta p \in \mathbb{Z}_p[X]$, which are clearly Eisenstein. As we will see later, studying quadratic extensions is in fact most interesting over $\mathbb{Q}_2$, due to the presence of 'wild ramification'. For $p = 2$, the following $7 = \#(\mathbb{Q}_2/\mathbb{Q}_2^\times) - 1$ extensions are all the quadratic extensions of $\mathbb{Q}_2$

$$\begin{array}{cccc} \mathbb{Q}_2(\sqrt{2}), & \mathbb{Q}_2(\sqrt{6}), & \mathbb{Q}_2(\sqrt{3}), & \mathbb{Q}_2(i) \\ \mathbb{Q}_2(\sqrt{-2}), & \mathbb{Q}_2(\sqrt{-6}), & \mathbb{Q}_2(\sqrt{-3}) & \end{array}$$

Precisely 1 of these 7 extensions is 'unramified', and hence can not given by an Eisenstein polynomial (see next section). From the above list, this is the extension $\mathbb{Q}_2(\sqrt{-3})$, since $\sqrt{-3} = 2\zeta_3 + 1$. For all these extensions, except $\mathbb{Q}_2(i)$ and $\mathbb{Q}_2(\sqrt{3})$, the minimal polynomial of the given generator is Eisenstein. For the other two fields we can 'shift' the primitive element to obtain an Eisenstein polynomial

$$\mathbb{Q}_2[X]/(X^2 + 2X + 2) \xrightarrow{\sim} \mathbb{Q}_2(i), \quad X \mapsto 1 - i,$$

$$\mathbb{Q}_2[X]/(X^2 + 2X - 2) \xrightarrow{\sim} \mathbb{Q}_2(\sqrt{3}), \quad X \mapsto \sqrt{3} - 1.$$

Ramification of local extensions

Let L/F be a finite extension of p-adic fields. We write v_L, v_F for the valuations on L and F whose value group is $\mathbb{Z} \subset \mathbb{R}$, so they are normalized in such a way that they take uniformizing elements to 1. Let $\mathfrak{P}$ be the maximal ideal of $\mathcal{O}_L$ and $\mathfrak{p}$ the maximal ideal

of $\mathcal{O}_F$. Then we have $\mathcal{O}_F/(\mathfrak{P} \cap \mathcal{O}_F) \subset \mathcal{O}_L/\mathfrak{P}$. Consequently, $\mathcal{O}_F/(\mathfrak{P} \cap \mathcal{O}_F)$ is a finite domain, and hence a field. Thus $\mathfrak{P} \cap \mathcal{O}_F$ equals the maximal ideal $\mathfrak{p}$ of $\mathcal{O}_F$. In the other direction for the $\mathcal{O}_L$-ideal generated by $\mathfrak{p}$ we have $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^{e_{L/F}}$, where $e_{L/F} \in \mathbb{Z}$ is called the *ramification index*. We write $f_{L/F} = [\kappa_L : \kappa_F]$ for the *inertial degree*. The *unramified extensions* are those L/F with $e_{L/F} = 1$, and the *totally ramified extensions* are those with $e_{L/F} = [L : F]$.

Proposition 2.33. *We have* $[L : F] = f_{L/F} \cdot e_{L/F}$.

Sketch. Since $\mathcal{O}_L$ is torsion-free, it is projective over $\mathcal{O}_F$ and hence free as $\mathcal{O}_F$ is local (see, *e.g.* [9, Exercise 11.10, Theorem 2.5], [9, Theorem 2.5]). Thus, $\mathcal{O}_L \cong \mathcal{O}_F^d$ as $\mathcal{O}_F$-module, and hence also $L \cong F^d$ which implies $d = [L : F]$. Similarly, the κ_F-dimension of $\mathcal{O}_L \otimes \kappa_F \cong \mathcal{O}_F^d \otimes \kappa_F$ is d. On the other hand the successive quotients of the filtration $\mathfrak{P}^i/\mathfrak{P}^{e_{L/F}}$ of $\mathcal{O}_L \otimes \kappa_F = \mathcal{O}_L/\mathfrak{P}^{e_{L/F}}$ are all κ_F-isomorphic to κ_L. Since the filtration is of length $e_{L/F}$, we obtain $[L : F] = \dim_{\kappa_F}(\mathcal{O}_L \otimes \kappa_F) = e_{L/F} \cdot f_{L/F}$. □

Corollary 2.34. *If $L/M/F$ is a tower of finite extensions of p-adic fields, then $e_{L/F} = e_{L/M} \cdot e_{M/F}$ and $f_{L/F} = f_{L/M} \cdot f_{M/F}$.*

Theorem 2.35. *Let L/F be an extension of p-adic fields of degree n.*

(i) The valuation v_L is given by the formula $v_L(x) = f_{L/F}^{-1} \cdot v_F(N_{L/F}(x))$.

(ii) The extension L/F is unramified if and only if it is of the form $L = F(\zeta)$ where ζ is root of unity whose order is prime to p.

(iii) The subfield $F(\varpi_L) \subset L$ is a (in general non-unique) maximal totally ramified extension of F in L.

(iv) The minimal polynomial $f \in \mathcal{O}_F[X]$ of ϖ_L over F is an Eisenstein polynomial.

(v) Let $f \in \mathcal{O}_F[X]$ be an Eisenstein polynomial. Then $L = F[X]/(f)$ is a totally ramified extension of F with uniformizer X.

Proof. (i) We know that $|N_{L/F}(\cdot)|_F$ defines a norm on L. Since all these norms are equivalent, it follows that $|\cdot|_L$ and $|N_{L/F}(\cdot)|_L$ differ by a power of a positive real number. Thus also $v_L(\cdot) = \alpha v_F(N_{L/F}(\cdot))$ for some $\alpha \in \mathbb{R}_{>0}$. Filling in an F-uniformizer, we obtain $v_L(\varpi_F) = \alpha v_F(N_{L/F}(\varpi_F))$, and hence $e_{L/F} = \alpha v_F(\varpi_F^{[L:F]}) = \alpha[L : F]$. By Proposition 2.33 we have $\alpha = f_{L/F}^{-1}$.

(ii) Let $\zeta \in L$ be a root of unity of prime to p order. We check that $F(\zeta)/F$ is unramified. The minimal polynomial f of ζ over F divides the polynomial $X^m - 1 \in \mathcal{O}_F[X]$, with m coprime to p. Hence $\overline{f}$ is separable modulo p. By Hensel's lemma any factorization of $\overline{f}$ lifts, and hence $\overline{f}$ must be irreducible. Consequently, the degree of $\kappa_{F(\zeta)}$ over κ_F is equal to $\deg(f) = [F(\zeta) : F]$. By Proposition 2.33, the extension $F(\zeta)/F$ is unramified. The converse statement is similar: If M/F is an unramified subfield of L, then κ_M is generated by a root of unity ζ over κ_F, whose order is prime to p. By Hensel's lemma this root of unity lifts to a root of unity $\widetilde{\zeta} \in M$. It is then easy to see that $M = F(\widetilde{\zeta})$.

(iii) Exercise 2.21.

(iv) By Proposition 2.33 we have $\kappa_F = \kappa_L$ in the totally ramified case. Let $\varpi_L \in \mathcal{O}_L$ be a primitive element and $f \in \mathcal{O}_F[X]$ its minimal polynomial over F. We have

$v_F(N_{L/F}(\varpi_L)) = v_L(\varpi_L) = 1$. Write $f = \sum_{i=0}^{[L:F]} a_i X^i$, then $a_0 = \pm N_{L/F}(\varpi_L)$. Hence $v_F(a_0) = 1$, thus the constant term of f has valuation 1. On the other hand, assume $f \equiv \prod_{i=1}^{k} \phi_i^{e_i} \in \kappa_F[X]$, with the $\phi_i \in \kappa_F[X]$ irreducible and coprime. By Hensel's lemma this factorization lifts to a factorization $f = \prod_{i=1}^{k} f_i \in \mathcal{O}_F[X]$, where f_i lifts $\phi_i^{e_i}$. Since f is irreducible, we must have $k = 1$. Now $\varpi_L \equiv 0 \mod \mathfrak{P}$ is a root of the irreducible polynomial ϕ_1. Hence $\phi_1 = X$ and $\overline{f} = X^{[L:F]}$.

(v) Put $L = F[X]/(f)$. The norm of X acting on L is equal to the constant term a_0 of f, which has the property that $a_0 \in \mathfrak{p}\backslash\mathfrak{p}^2$. Hence $v_L(X) = f_{L/K}^{-1} v_F(a_0) = f_{L/F}^{-1}$, which is only possible if $f_{L/F} = 1$. □

Primitive element theorem for p-adic rings

A basic theorem for finite extensions L/F of number fields is that any such extension has a *primitive element* α such that $L = F(\alpha)$. However, on the level of rings of integers there are many examples where $\mathcal{O}_L$ can not be generated by a single element over $\mathcal{O}_F$. In case of finite extensions of p-adic number rings the situation is better, in this case we can find a fairly explicit generator.

Let L/F be a finite extension of p-adic fields. The first basic observation is that if $S \subset \mathcal{O}_L$ is a system of representatives for the quotient $\mathcal{O}_L/\mathfrak{P}$, then any element $x \in \mathcal{O}_L$ can be written as an infinite sum $x = \sum_{i=0}^{\infty} s_i \varpi_L^i$ for $s_i \in S$. In particular, we may take $\mu \subset \mathcal{O}_L$ the set of roots of unity of prime to p-order contained in $\mathcal{O}_L^\times$. Then μ is a system of representatives for $\mathcal{O}_L/\mathfrak{P}$, and hence $\mathcal{O}_L = \mathbb{Z}_p[\varpi_L, \zeta]$, if $\zeta \in \mu$ is of maximal order. Thus, in case L/F is totally ramified, $\mathcal{O}_L$ equals $\mathcal{O}_F[\varpi_L]$, and if L/F is unramified, $\mathcal{O}_L$ equals $\mathcal{O}_F[\zeta]$. In general we have

Proposition 2.36. *We have $\mathcal{O}_L = \mathcal{O}_F[\varpi_L + \zeta]$.*

Proof. Let Φ be the minimal polynomial of ζ over $\mathcal{O}_F$. Then $\Phi(\zeta + \varpi_L) = \frac{d}{dX}\Phi(\zeta)\varpi_L + \varepsilon$ for some $\varepsilon \in \mathcal{O}_L$ with $v_L(\varepsilon) \geq 2$. Since Φ is separable modulo $\mathfrak{p}$ we have $\Phi'(\zeta) \in \mathcal{O}_L^\times$. Hence $v_L(\Phi(\varpi_L + \zeta)) = 1$ and $\Phi(\varpi_L + \zeta)$ is a uniformizing element of $\mathcal{O}_L$. For each integer $a \in \mathbb{Z}_{\geq 0}$ we have $(\zeta + \varpi_L)^a = \zeta^a + \varpi_L \varepsilon$ for some $\varepsilon \in \mathcal{O}_L$. Consider the set S consisting of 0 and the elements $(\zeta + \varpi_L)^a$ for $a = 0, 1, 2, \ldots, p^{f_{F/L}} - 1$. Then S is a system of representatives S for the quotient $\mathcal{O}_L/\mathfrak{P}$. The result now follows by applying the remark above the proposition to the uniformizer $\Phi(\zeta + \varpi_L)$ and the set of representatives S. □

Ramification groups, the lower numbering filtration

Let L/F be a finite Galois extension of p-adic fields with Galois group $G = \mathrm{Gal}(L/F)$. Write n for the degree $[L : F]$, $\mathfrak{p}$ for the maximal ideal of $\mathcal{O}_F$ and $\mathfrak{P}$ for the maximal ideal of L. The group $\mathrm{Gal}(L/F)$ preserves the valuation $v_L(x)$ of elements $x \in L$. In particular G acts on $\mathcal{O}_L$, which is easily seen to be faithful (choose a primitive element α of L/F that is also integral, $\alpha \in \mathcal{O}_L$). From this action we obtain $G \rightarrowtail \mathrm{Aut}_{\mathcal{O}_F}(\mathcal{O}_L)$. The i-th ramification subgroup $G_i \subset G$ is defined to be the kernel of the composition

$$G \rightarrowtail \mathrm{Aut}_{\mathcal{O}_F}(\mathcal{O}_L) \to \mathrm{Aut}_{\mathcal{O}_F}(\mathcal{O}_L/\mathfrak{P}^{i+1}).$$

Equivalently, $G_i = \{\sigma \in G \mid \forall x \in \mathcal{O}_L \ v_L(\sigma(x) - x) \geq i + 1\}$. The first 3 groups of this sequence have a special name:

- $G_{-1} = G$ is the total Galois group,
- $G_0 = I(L/F)$ is the *inertia subgroup*,
- $G_1 = I(L/F)^{\text{wild}}$ is the *wild inertia subgroup.*

Let's first analyze the case $i = -1$. Then we are looking at the mapping

$$G/G_0 = \text{Gal}(L/F)/I(L/F) \to \text{Aut}_{\mathcal{O}_F}(\mathcal{O}_L/\mathfrak{P}) = \text{Aut}_{\kappa_F}(\kappa_L) = \langle \text{Frob} \rangle, \quad \text{Frob}\colon x \mapsto x^q.$$

The subgroup $I(L/F)$ corresponds via Galois theory to the maximal extension $L^{\text{ur}} \subset L$ of F that is unramified. We have seen that $L^{\text{ur}} = F(\zeta)$, where ζ is a primitive root of unity, whose order is prime to p. Hence Frob lifts to an automorphism of $F(\zeta)$: Send ζ to ζ^q. This gives the *Frobenius element* $\text{Frob} \in \text{Gal}(L/F)/I(L/F)$. Abusing language, one sometimes speaks of Frobenius elements $\text{Frob} \in \text{Gal}(L/F)$, with the understanding that only their $I(L/F)$ coset is well-defined.

Let's now look at the higher ramification groups. Let $i \geq 0$, and define the subgroups

$$U_L^{(i)} = \{x \in \mathcal{O}_L^\times \mid x \equiv 1 \mod \varpi_L^i\}.$$

Choose a uniformizing element $\varpi_L \in \mathcal{O}_L$, so that $\mathcal{O}_L = \mathcal{O}_F[\alpha]$, then we obtain the injection

$$G_i/G_{i+1} \rightarrowtail U_L^{(i)}/U_L^{(i+1)}, \quad \sigma \mapsto \sigma(\varpi_L)/\varpi_L.$$

We have

$$U_L^{(i)}/U_L^{(i)} \subset \begin{cases} (\kappa_L^\times, \cdot), & i = 0 \\ (\kappa_L, +), & i > 0 \end{cases}$$

Observe that $\kappa_L^\times$ is a finite group of order prime to p, while κ_L is a p-group. In particular the wild inertia $I(L/F)^{\text{wild}}$ is a p-Sylow subgroup of $\text{Gal}(L/F)$, and this Sylow p-subgroup is normal.

Example: Ramification groups of the cyclotomic extension

Let us look at the example $\mathbb{Q}_p(\zeta_{p^n})$ over $\mathbb{Q}_p$, where ζ_{p^n} is a primitive p^n-th root of unity. We claim that $\mathbb{Q}_p(\zeta_{p^n})$ is a totally ramified extension of $\mathbb{Q}_p$. We have

$$\text{Gal}(\mathbb{Q}_p(\zeta_{p^n} | n \in \mathbb{Z}_{\geq 1})/\mathbb{Q}_p) \subset \mathbb{Z}_p^\times.$$

in particular by the computation below it will follow that the degree of $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ is $(p-1)p^{n-1} = \deg(\Phi_{p^n})$, hence the inclusion above is actually equality.

The minimal polynomial of ζ_{p^n} over $\mathbb{Q}$ is given by the polynomial

$$\Phi_{p^n}(X) = \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1} = 1 + X^{p^{n-1}} + X^{2p^{n-1}} + \ldots + X^{p^n - p^{n-1}} \in \mathbb{Q}[X].$$

By Theorem 2.35 we should be able to find a primitive element in the extension $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ whose minimal polynomial is Eisenstein. Clearly $\Phi_{p^n}(X)$ is not such a polynomial. In fact, since $\zeta_{p^n} \in \mathbb{Z}[\zeta_{p^n}]$ is a unit, it has no chance of being a uniformizer. The element $1 - \zeta_{p^n} \in \mathbb{Z}[\zeta_{p^n}]$ seems to be a better choice, since $\mathbb{Z}_p[\zeta_{p^n}]/(1 - \zeta_{p^n}) \xrightarrow{\sim} \mathbb{F}_p$, $\zeta_{p^n} \mapsto 1$ and hence $1 - \zeta_{p^n} \in \mathbb{Z}_p[\zeta_{p^n}]$ can't be a unit.

We check with induction that indeed $\Phi_{p^n}(X+1)$ is an Eisenstein polynomial. Clearly, $\Phi_{p^n}(1) = p$ by the above formula, so we need only to check that the coefficients are divisible by p. For $n = 1$ we have

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} \equiv \frac{(X^p+1)-1}{X} = X^{p-1} \in \mathbb{F}_p[X],$$

hence all its coefficients are divisible by p. Assume that the desired divisibility is true for $m < n$, then compute

$$\begin{aligned}\Phi_{p^n}(X+1) &= \frac{(X+1)^{p^n}-1}{(X+1)^{p^{n-1}}-1} = \frac{(X+1)^{p^n}-1}{X\Phi_p(X+1)\cdots\Phi_{p^{n-1}}(X+1)} \\ &\equiv \frac{(X+1)^{p^n}-1}{X\cdot X^{p-1}\cdots X^{p^{n-1}-1}} = X^{p^n-p^{n-1}} \in \mathbb{F}_p[X].\end{aligned}$$

Hence $\Phi_{p^n}(X+1)$ is indeed Eisenstein. Consequently, $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ is totally ramified.

We compute the ramification subgroups $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)_i \subset \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)$. By definition, $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)_i$ consists of those $\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)$ such that $v(\sigma(\zeta_{p^n}) - \zeta_{p^n}) \geq i+1$. Let $x \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ be such that $\sigma(\zeta_{p^n}) = \zeta_{p^n}^x$, then

$$v(\sigma(\zeta_{p^n}) - \zeta_{p^n}) = v(\zeta_{p^n}^x - \zeta_{p^n}) = v(\zeta_{p^n}^{x-1} - 1) = v_p(N_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p}(\zeta_{p^n}^{x-1} - 1))$$

Observe that $\zeta_{p^n}^{x-1} - 1$ generates the intermediate extension $\mathbb{Q}_p \subset \mathbb{Q}_p(\zeta_{p^n}^{x-1}) \subset \mathbb{Q}_p(\zeta_{p^n})$ where each step is totally ramified. Hence $v(\zeta_{p^n}^{x-1} - 1)$ equals $[\mathbb{Q}_p(\zeta_{p^n}) : \mathbb{Q}_p(\zeta_{p^n}^{x-1})] = v_p(x-1)$, and $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)_i$ identifies with the subgroup

$$\{x \in (\mathbb{Z}/p^n\mathbb{Z})^\times \mid x \equiv 1 \mod p^{i+1}\} \subset (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Example: Ramification subgroups of $\mathbb{Q}_p(\zeta_p, \sqrt[p]{2})/\mathbb{Q}_p$

We assume that $p \neq 2$ and also that $v_p(2^{p-1}-1) = 1$ (by Fermat's little theorem $v_p(2^{p-1}-1) > 0$). In fact, with a simple for loop in Sage I found that among the odd prime numbers $p \leq 10^6$ this condition fails for $p = 1093$ and $p = 3511$, and holds true for all other p. (We thank Maarten Derickx for helping us out with the exceptional primes, see below).

Write $L = \mathbb{Q}_p(\zeta_p, \sqrt[p]{2})$. We have the tower of subfields $\mathbb{Q}_p \subset \mathbb{Q}_p(\zeta_p) \subset L$. The first step in this tower being understood already in a previous example, let's look at the second step of the tower. The element $\sqrt[p]{2}$ is a root of the polynomial $f = X^p - 2 \in \mathbb{Q}_p(\zeta_p)[X]$. We have $\overline{f} = (X-2)^p \in \mathbb{F}_p[X]$. By the assumption $v_p(2^{p-1}-1) = 1$ the polynomial $f(X+2) = (X+2)^p - 2 \in \mathbb{Q}_p[X]$ is Eisenstein. Hence the element $\alpha = \sqrt[p]{2} - 2 \in L$ is a uniformizer of a totally ramified degree p extension $M/\mathbb{Q}_p$ contained in L, and $\mathcal{O}_M = \mathbb{Z}_p[\alpha]$. Since the degrees of M and $\mathbb{Q}_p(\zeta_p)$ are coprime, the degree of L over $\mathbb{Q}_p$ is equal to $p(p-1)$, and $\mathrm{Gal}(L/\mathbb{Q}_p) = \mathbb{F}_p \ltimes \mathbb{F}_p^\times$ where $\sigma = (x,y) \in \mathbb{F}_p \ltimes \mathbb{F}_p^\times$ acts by $\sigma(\zeta_p) = \zeta_p^y$ and $\sigma(\sqrt[p]{2}) = \zeta_p^x \sqrt[p]{2}$. Finally, in general it is not true that the compositum of two totally ramified extensions is totally ramified; however in case of L, we know that the valuation of $v_L(p)$ is divisible by p (look at the intermediate extension $\mathbb{Q}_p(\zeta_p)$) and also divisible by $p-1$ (look at the intermediate extension $\mathbb{Q}_p(\sqrt[p]{2})$). Thus $p(p-1)|v_L(p)$; since we also know that $v_L(p) \leq p(p-1)$, we must have $v_L(p) = p(p-1)$, *i.e.* the extension $L/\mathbb{Q}_p$ is totally ramified.

At this point we already know two steps of the ramification filtration on $\mathrm{Gal}(L/\mathbb{Q}_p)$:

$$G_{-1} = \mathrm{Gal}(L/\mathbb{Q}_p) = \mathbb{F}_p \ltimes \mathbb{F}_p^\times \subset G_0 = I(L/\mathbb{Q}_p) = \mathbb{F}_p \ltimes \mathbb{F}_p^\times \subset G_1 = I(L/\mathbb{Q}_p)^{\mathrm{wild}} = \mathbb{F}_p,$$

simply because the wild inertia is the pro-p-part of the inertia group. There must be one more jump in the filtration, and we want to compute in the straightforward way where this jump happens.

Let's first find a uniformizer of L. Note that $v_L(\alpha) = p-1$ since L/M is totally ramified of degree $p-1$, and α is a uniformizer of M. Similarly, put $\beta = 1-\zeta_p$, then β is a uniformizer of $\mathbb{Q}_p(\zeta_p)$, and hence $v_L(\beta) = p$. Consequently, for $\gamma = \beta/\alpha$, we have $v_L(\gamma) = p-(p-1) = 1$, and hence γ is a uniformizer of L and $\mathcal{O}_L = \mathbb{Z}_p[\gamma]$.

Let $\sigma \in I(L/\mathbb{Q}_p)^{\mathrm{wild}}$. Then $\sigma(\zeta_p) = \zeta_p$ and $\sigma(\sqrt[p]{2}) = \zeta_p^x \sqrt[p]{2}$ for some $x \in \mathbb{F}_p$. We compute

$$\begin{aligned} v_L(\sigma(\gamma)-\gamma) &= v_L(\sigma(\beta/\alpha) - \beta/\alpha) \\ &= v_L(\beta) + v_L(1/\sigma(\alpha) - 1/\alpha) \\ &= p - v_L(\alpha\sigma(\alpha)) + v_L\left(\sigma(\alpha)-\alpha\right) \\ &= p - 2(p-1) + v_L\left(\sigma(\alpha)-\alpha\right) \\ &= -p+2 + v_L(\zeta_p^x \sqrt[p]{2} - \sqrt[p]{2}) \\ &= -p+2+p \\ &= 2, \end{aligned}$$

(unless $x=0$ of course). Hence the ramfication filtration on $\mathrm{Gal}(L/\mathbb{Q}_p)$ is

i	-1	0	1	2
G_i	$\mathbb{F}_p \ltimes \mathbb{F}_p^\times$	$\mathbb{F}_p \ltimes \mathbb{F}_p^\times$	$\mathbb{F}_p$	0

For the primes $p = 1093$ and $p = 3511$ we used the computer program Pari and saw that actually $\sqrt[1093]{2} \in \mathbb{Q}_{1093}$ and $\sqrt[3511]{2} \in \mathbb{Q}_{3511}$. In particular the extension $\mathbb{Q}_p(\zeta_p, \sqrt[p]{2})$ simply equals $\mathbb{Q}_p(\zeta_p)$. After quite some discussions with Maarten Derickx, he finally found that this is the what happens in general:

Lemma 2.37. *If p is a prime number such that $p^2 | 2^{p-1}-1$, then $\sqrt[p]{2} \in \mathbb{Q}_p$.*

Proof. Since $p^2|2^{p-1}-1$ we have for $a_0 = 2$ that $a_0^p \equiv 2 \mod p^2$. We now consider $(a_0+pb)^p - 2$ modulo p^3, and solve for b:

$$(a_0+pb)^p - 2 \equiv a_0^p + \binom{p}{1} a_0^{p-1} pb - 2 \equiv (a_0^p - 2) + p^2 a_0^{p-1} b \mod p^3.$$

Since a_0 is coprime to p, and $a_0^p - 2$ is divisible by p^2, there exists a b such that the last equation is $0 \mod p^3$. Take this b and put $a_1 = a_0 + pb$, so a_1 is a solution modulo p^3. Since $v_p(f'(a_1)) = v_p(pa_1^{p-1}) = 1$ (a_1 is a unit), and $v_p(f(a_1)) = v_p(a_1^p - 2) \geq 3$, we have $2v_p(f'(a_1)) = 2 < 3 = v_p(f(a_1))$, and hence the following variant of Hensel's lemma applies. □

Lemma 2.38. *Let $f \in \mathbb{Z}_p[X]$ be a monic polynomial such that for some $a \in \mathbb{Z}_p$ we have $2v_p(f'(a)) < v_p(f(a))$, then there exists an $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$.*

Remark 2.39. After working through the example we found on Wikipedia a page about "Wieferich primes", *i.e.* prime numbers such that $p^2|2^{p-1}-1$. Currently, there are precisely 2 of these numbers known, namely 1093 and 3511. It is known that any other prime p with this property is at least 10^{17}, which we also confirmed up to 10^6. Silverman showed that the *abc*-conjecture implies that there are infinitely many. Moreover, if p is an odd prime, $x, y, z \in \mathbb{Z}$ are integers such that $x^p + y^p + z^p = 0$, and p does not divide xyz, then p is a Wieferich prime (this result is proved by Wieferich in 1901, so long before modularity of elliptic curves, hence also the name for these numbers. Using modularity, the authors also proudly know an alternative proof).

2.4 Algebraic number theory for infinite extensions

In this section, we will recall some concepts and results from algebraic number theory and generalise them to infinite algebraic extensions of $\mathbb{Q}$. The most important ones are the *ring of integers* and *Frobenius elements*.

Number fields and infinite algebraic extensions

Recall that a field extension L/K is *algebraic* if every $\alpha \in L$ is a zero of some non-zero polynomial in $K[X]$. If α is algebraic, there exists a unique monic polynomial $f_\alpha \in K[X]$ of minimal degree having α as a zero; this f_α is the *minimal polynomial* of α.

We recall that a *number field* is a finite, and hence algebraic, extension F of $\mathbb{Q}$. Any number field has a *primitive element* $\alpha \in F$ such that α generates F over $\mathbb{Q}$.

The *ring of integers* $\mathcal{O}_F$ of F is the set of $\alpha \in F$ whose minimal polynomial f_α has coefficients in $\mathbb{Z}$. One checks that sums and products of integral elements are again integral, so $\mathcal{O}_F$ is a subring of F. The ring $\mathcal{O}_F$ turns out to be a *Dedekind domain*, *i.e.* a noetherian, integrally closed integral domain in which any non-zero prime ideal is maximal.

Remark 2.40. There are two other ways to characterize $\mathcal{O}_F$:

- The ring $\mathcal{O}_F$ is the smallest among all subrings $R \subset F$ with $\mathrm{Frac}(R) = F$ such that R is a Dedekind domain.
- The ring $\mathcal{O}_F$ is the largest subring of F that is finitely generated as a $\mathbb{Z}$-module.

Any non-zero ideal $I \subset \mathcal{O}_F$ admits a *factorization* into prime ideals

$$I = \prod_{i=1}^{t} \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_t^{e_t} \quad \text{in } \mathcal{O}_F,$$

where the $\mathfrak{p}_i$ are pairwise distinct prime ideals of $\mathcal{O}_F$ and where the e_i are positive integers. This factorization is unique up to permutation.

Let M/F be an extension of number fields. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$. Then $\mathcal{O}_M\mathfrak{p}$ is an ideal in $\mathcal{O}_M$ which is no longer a prime ideal in general. The decomposition of $\mathcal{O}_M\mathfrak{p} = \prod_{i=1}^{t} \mathfrak{P}_i^{e_i}$ is the *splitting behaviour* of $\mathfrak{p}$. The integer e_i is called the *ramification index* of $\mathfrak{P}_i$ over $\mathfrak{p}$, and the degree $f_i = [k(\mathfrak{P}_i) : k(\mathfrak{p})]$ of the extension of residue fields is called the *residue field degree*. We say furthermore that

- $\mathfrak{p}$ is *ramified* if $e_i > 1$ for some $i \in \{1, 2, \ldots, t\}$, and *unramified* otherwise.

- $\mathfrak{p}$ is *totally ramified* if $t = 1$ and $e_1 = [M : F]$.
- $\mathfrak{p}$ is *inert* if $\mathcal{O}_M\mathfrak{p}$ is prime, or equivalently $t = 1$ and $e_1 = 1$.
- $\mathfrak{p}$ is *totally split* if $t = [M : F]$.

In any extension M/F of number fields, there are only finitely many primes ramified; by contrast, there are infinitely many primes that are totally split. More precise results on the splitting of primes can be deduced from Chebotarev's density theorem (see Theorem 2.47 below).

Example 2.41. The ring of integers of the quadratic extension $\mathbb{Q}(i)/\mathbb{Q}$ is $\mathbb{Z}[i]$; it is called the ring of *Gauss numbers*. The ring $\mathbb{Z}[i]$ is a principal ideal domain, and its primes are given by

- $\pi = 1 + i$,
- $\pi = a + bi$ with $a^2 + b^2 = p$, $p \equiv 1 \pmod 4$, $a > b > 0$,
- $\pi = p$ if $p \equiv 3 \pmod 4$.

The prime numbers $p \equiv 1 \pmod 4$ split in $\mathbb{Z}[i]$ into $p = (a+bi)(a-bi)$. The prime number 2 is equal to $(1 + i)(1 - i)$. Since $1 + i$ and $1 - i$ differ by the unit i, we have as ideals $(2) = (1 + i)^2$, so the prime 2 ramifies in $\mathbb{Q}(i)/\mathbb{Q}$.

Example 2.42. Recall that even though we have ideal factorization in $\mathcal{O}_F$, in general the element factorization into irreducible elements is not unique. Typical example:

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5}) \in \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$$

Rings of integers of algebraic extensions of $\mathbb{Q}$

Now let F be any (not necessarily finite) algebraic extension of $\mathbb{Q}$. As in the case where F is a number field, we define the *ring of integers* $\mathcal{O}_F$ as the ring of elements $x \in F$ that are integral over $\mathbb{Q}$. If F is infinite over $\mathbb{Q}$, the ring $\mathcal{O}_F$ is not noetherian, and hence is not a Dedekind domain. In general, $\mathcal{O}_F$ equals the union of all rings $\mathcal{O}_L$, where L runs over the number fields contained in F, and hence is a 'limit' of Dedekind domains.

Lemma 2.43. *Let F be an algebraic extension of $\mathbb{Q}$, and let M be an algebraic extension of F.*

(i) For any prime ideal $\mathfrak{p}$ in $\mathcal{O}_F$ there exists a prime ideal $\mathfrak{P} \subset \mathcal{O}_M$ such that $\mathfrak{P} \cap \mathcal{O}_F = \mathfrak{p}$.

(ii) Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_F$ above the prime number p. Then $\mathcal{O}_F/\mathfrak{p}$ is an algebraic extension of $\mathbb{F}_p$.

(iii) If M/F is a Galois extension, then the action of the Galois group $G = \mathrm{Gal}(M/F)$ on the set of primes of M lying above a prime $\mathfrak{p}$ of F is transitive.

Proof. Exercise 2.36. □

In contrast to the finite case, unique factorization of ideals fails for infinite algebraic extensions of $\mathbb{Q}$.

Example 2.44. Consider the ring of integers $\overline{\mathbb{Z}}$ of $\overline{\mathbb{Q}}$. We will show that all prime ideals $\mathfrak{p}$ of $\overline{\mathbb{Z}}$ satisfy $\mathfrak{p}^2 = \mathfrak{p}$.

Let $p \in \mathbb{Z}$ be the prime under $\mathfrak{p}$, and $v\colon \overline{\mathbb{Q}} \to \mathbb{R} \cup \{\infty\}$ the valuation corresponding to $\mathfrak{p}$, normalized so that $v(p) = 1$. We will prove that the image of v equals $\mathbb{Q} \cup \{\infty\} \subset \mathbb{R} \cup \{\infty\}$. For each number field L, let $\mathfrak{p}_L = \mathfrak{p} \cap \mathcal{O}_L$, and $v_L = v|_L$. Then v_L is a non-normalized valuation corresponding to $\mathfrak{p}_L$. Write e_L for the ramification index of $\mathfrak{p}_L$ over p. Then the image of v equals the union, over all number fields L, of the images of the maps v_L; we note that this equals $\{\infty\} \cup \bigcup_L \frac{1}{e_L}\mathbb{Z} = \{\infty\} \cup \mathbb{Q}$. The square of $\mathfrak{p}$ can be computed locally at $\mathcal{O}_\mathfrak{p}$. But locally we have $\mathfrak{p}\mathcal{O}_\mathfrak{p} = \{x \in \overline{\mathbb{Q}} \mid v(x) \geq 0\} = \{x \in \overline{\mathbb{Q}} \mid v(x) \in \{\infty\} \cup \mathbb{Q}_{\geq 0}\}$. This implies

$$\begin{aligned}\mathfrak{p}^2\mathcal{O}_\mathfrak{p} &= \{x \in \overline{\mathbb{Q}} \mid v(x) \in \{\infty\} \cup 2 \cdot \mathbb{Q}_{\geq 0}\} \\ &= \{x \in \overline{\mathbb{Q}} \mid v(x) \in \{\infty\} \cup 2 \cdot \mathbb{Q}_{\geq 0}\} \\ &= \mathfrak{p}\mathcal{O}_\mathfrak{p}.\end{aligned}$$

Frobenius elements

Let F be a number field, let M be a (possibly infinite) Galois extension of F, and let $\mathcal{O}_M$ be its ring of integers. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_M$ lying over a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, and let $k(\mathfrak{P}) = \mathcal{O}_M/\mathfrak{P}$ and $k(\mathfrak{p}) = \mathcal{O}_F/\mathfrak{p}$ be the residue fields. Then $k(\mathfrak{p})$ is a finite field, say of cardinality q. By Lemma 2.43(ii), $k(\mathfrak{P})$ is an algebraic extension of $k(\mathfrak{p})$. Let $D_\mathfrak{P} = \{\sigma \in \mathrm{Gal}(M/F) \mid \sigma\mathfrak{P} = \mathfrak{P}\}$ be the decomposition group of $\mathfrak{P}$. By reduction to the case of finite extensions, one sees that every algebraic extension of a finite field is Galois, and that we have a surjective continuous group homomorphism

$$r\colon D_\mathfrak{P} \longrightarrow \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})).$$

The right-hand side is a pro-cyclic group (either a finite cyclic group of a topological group isomorphic to $\widehat{\mathbb{Z}}$), topologically generated by the Frobenius element $\mathrm{Frob}_q\colon x \mapsto x^q$. The kernel of r is called the *inertia group* of $\mathfrak{P}$ over $\mathfrak{p}$, and any element in $D_\mathfrak{P} \subseteq \mathrm{Gal}(M/F)$ mapping to Frob_q is called a *Frobenius element* at $\mathfrak{P}$ and denoted by $\mathrm{Frob}_\mathfrak{P}$.

Let $\mathfrak{p}$ be a prime of F such that the extension M/F is unramified at $\mathfrak{p}$. Then any prime $\mathfrak{P}$ of M lying over $\mathfrak{p}$ determines a unique element $\mathrm{Frob}_\mathfrak{P} \in \mathrm{Gal}(M/F)$. Any other prime of M over $\mathfrak{p}$ has the form $\sigma\mathfrak{P}$ with $\sigma \in \mathrm{Gal}(M/F)$, and we have $D_{\sigma\mathfrak{P}} = \sigma D_\mathfrak{P} \sigma^{-1}$ and $\mathrm{Frob}_{\sigma\mathfrak{P}} = \sigma\mathrm{Frob}_\mathfrak{P}\sigma^{-1}$. The set of all $\mathrm{Frob}_\mathfrak{P}$ with $\mathfrak{P}$ a prime of M over $\mathfrak{p}$ is therefore a conjugacy class in $\mathrm{Gal}(M/F)$, called the *Frobenius conjugacy class* at $\mathfrak{p}$. When no confusion is possible, any element of this conjugacy class (or even the conjugacy class itself) is denoted by $\mathrm{Frob}_\mathfrak{p}$.

Example 2.45. Assume $\mathfrak{p}$ is unramified in F. Then $\mathfrak{p}$ is totally split in M if and only if the Frobenius conjugacy class at $\mathfrak{p}$ equals the trivial conjugacy class $\{\mathrm{id}\} \subseteq \mathrm{Gal}(M/F)$.

Example 2.46. Let l be a prime number, and take $F = \mathbb{Q}$ and $M = \mathbb{Q}(\zeta_{l^\infty}) = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_{l^n})$. We have a canonical isomorphism

$$\begin{aligned}\mathbb{Z}_l^\times &\xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_{l^\infty})/\mathbb{Q}) \\ a &\longmapsto (\zeta_{l^n} \mapsto \zeta_{l^n}^{a \bmod l^n}).\end{aligned}$$

For every prime number $p \neq l$, the element $p \in \mathbb{Z}_l^\times$ is mapped to the Frobenius element at p. (Note that this Frobenius element is unique because the extension is Abelian.)

Densities of sets of primes; Chebotarev's theorem

Let F be a number field, and let P be the set of all prime ideals of $\mathcal{O}_F$. For any subset $S \subseteq P$, the *natural density* of S is defined by the following limit (provided it exists):

$$d_0(S) = \lim_{X\to\infty} \frac{\#\{\mathfrak{p} \in S \mid N(\mathfrak{p}) \leq X\}}{\#\{\mathfrak{p} \in P \mid N(\mathfrak{p}) \leq X\}}.$$

The *Dirichlet density* of S is defined by

$$d(S) = \lim_{s\to 1} \frac{\sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in P} N(\mathfrak{p})^{-s}},$$

where the limit is taken over positive real numbers s tending to 1 from above. One can show that the Dirichlet density always exists, and if the naïve density exists, then it is equal to the Dirichlet density.

Theorem 2.47. *Let F be a number field, and let M be a finite Galois extension of F that is unramified outside a finite set Σ of places of F. Let X be a subset of $G = \mathrm{Gal}(M/F)$ that is stable under conjugation. Let S_X be the set of primes $\mathfrak{p}$ of F such that $\mathfrak{p} \notin \Sigma$ and such that the Frobenius conjugacy class at $\mathfrak{p}$ is contained in X. Then the naïve density of S_X exists and equals $\#X/\#G$.*

There also exists a version for infinite extensions.

Theorem 2.48. *Let F be a number field, and let M be a (possibly infinite) Galois extension of F that is unramified outside a finite set Σ of places of F. Let μ be the unique Haar measure on the compact group $G = \mathrm{Gal}(M/F)$ such that $\mu(G) = 1$. Let X be a subset of G that is stable under conjugation and such that the boundary $\bar{X} \setminus X^\circ$ has measure 0. Let S_X be the set of primes $\mathfrak{p}$ of F such that $\mathfrak{p} \notin \Sigma$ and such that the Frobenius conjugacy class at $\mathfrak{p}$ is contained in X. Then the naïve density of S_X exists and equals $\mu(X)$.*

2.5 Adèles

We will now "unify" the various completions of a number field F by introducing the *adèle ring* of F. This is a topological ring $\mathbb{A}_F$ that admits every completion F_v as a quotient, but behaves in a more civilised way than the product $\prod_v F_v$ of topological rings. For example, $\mathbb{A}_F$ is locally compact, while $\prod_v F_v$ is not.

The unit group $\mathbb{A}_F^\times$ of $\mathbb{A}_F$ deserves a careful study of its own. It is a fundamental object in the modern formulation of class field theory. Likewise, its non-commutative generalisations $\mathrm{GL}_n(\mathbb{A}_F)$ (note that $\mathbb{A}_F^\times = \mathrm{GL}_1(\mathbb{A}_F)$) play a central role in the modern theory of automorphic forms, and hence in the Langlands programme.

The adèle ring of $\mathbb{Q}$

We start by looking at the case $F = \mathbb{Q}$. We define the ring of *finite adèles* $\mathbb{A}^\infty = \mathbb{A}_\mathbb{Q}^\infty$ as the tensor product $\mathbb{A}^\infty \stackrel{\text{def}}{=} \mathbb{Q} \otimes_\mathbb{Z} \widehat{\mathbb{Z}}$, where we view $\mathbb{Q}$ and $\widehat{\mathbb{Z}}$ as $\mathbb{Z}$-modules. Like any tensor product of commutative rings, $\mathbb{A}^\infty$ inherits a multiplication map, given explicitly by

$$\left(\sum_{i=1}^n q_i \otimes z_i\right) \cdot \left(\sum_{j=1}^m q'_j \otimes z'_j\right) = \sum_{i,j} q_i q'_j \otimes z_i z'_j$$

for all $\sum_{i=1}^{n} q_i \otimes z_i$ and $\sum_{j=1}^{m} q'_j \otimes z'_j$ in $\mathbb{A}^\infty$.

The ring $\mathbb{A}^\infty$ is equipped with the strongest topology such that the map

$$\begin{aligned} \mathbb{Q} \times \widehat{\mathbb{Z}} &\longrightarrow \mathbb{A}^\infty \\ (x, z) &\longmapsto x + z \end{aligned}$$

is continuous, where $\mathbb{Q}$ is given the discrete topology. More concretely, the subsets of the form

$$U_{x,y} = x \cdot \widehat{\mathbb{Z}} + y \subset \mathbb{A}^\infty \quad \text{with } x \in \mathbb{Q}^\times \text{ and } y \in \mathbb{Q}$$

form a basis for the topology on $\mathbb{A}^\infty$. This definition implies that $\mathbb{A}^\infty$ is a locally profinite topological ring containing $\widehat{\mathbb{Z}}$ as an open subring.

Definition 2.49. The *adèle ring* $\mathbb{A} = \mathbb{A}_\mathbb{Q}$ is the product ring $\mathbb{A}^\infty \times \mathbb{R}$, equipped with the product topology.

The adèle ring as a restricted product

In many texts the ring $\mathbb{A}$ is introduced as a "restricted product" ranging over all prime numbers p, of the fields $\mathbb{Q}_p$ with respect to the subrings $\mathbb{Z}_p \subset \mathbb{Q}_p$. This restricted product arises from the following computation. Observe first that we can view $\mathbb{Q}$ as the inductive limit $\mathbb{Q} = \varinjlim_{N \in \mathbb{Z}_{\geq 1}} \mathbb{Z}[1/N]$.

Using this, we compute

$$\left(\varinjlim_{N \in \mathbb{Z}_{\geq 1}} \mathbb{Z}[1/N] \right) \otimes \widehat{\mathbb{Z}} = \varinjlim_{N \in \mathbb{Z}_{\geq 1}} \left(\mathbb{Z}[1/N] \otimes \widehat{\mathbb{Z}} \right) = \varinjlim_{N \in \mathbb{Z}_{\geq 1}} \left(\prod_{p \mid N} \mathbb{Q}_p \times \prod_{p \nmid N} \mathbb{Z}_p \right). \tag{2.4}$$

For each N, we embed $\prod_{p|N} \mathbb{Q}_p \times \prod_{p \nmid N} \mathbb{Z}_p \subset \prod_{p \text{ prime}} \mathbb{Q}_p$. Hence, $\mathbb{A}^\infty$ equals the so called *restricted product*

$$\prod_{p \text{ prime}}{}' (\mathbb{Q}_p, \mathbb{Z}_p) = \left\{ (\alpha_p) \in \prod_{p \text{ prime}} \mathbb{Q}_p \mid \text{ for almost all primes } p \text{ we have } \alpha_p \in \mathbb{Z}_p \right\}.$$

A basis for the topology on the restricted product is given by the sets

$$U_{x,y} = \{ (\alpha_p) \in \mathbb{A}^\infty \mid v_p(\alpha_p - y) \geq v_p(x) \}$$

with $x \in \mathbb{Q}^\times$ and $y \in \mathbb{Q}$.

The full adèle ring is obtained from $\mathbb{A}^\infty$ by attaching a component for the infinite place as well. As a restricted product, we have

$$\mathbb{A} = \prod_{\mathbb{Q}\text{-places } v}{}' (\mathbb{Q}_v : \mathbb{Z}_v)$$

where for $v = \infty$, we take by definition $\mathbb{Z}_v = \mathbb{Q}_v = \mathbb{R}$.

The adèle ring of a number field

If F is a number field, the analogue of $\widehat{\mathbb{Z}}$ is the ring of *profinite F-integers*,

$$\widehat{\mathcal{O}}_F = \widehat{\mathbb{Z}} \otimes \mathcal{O}_F = \varprojlim_{N \in \mathbb{Z}_{\geq 1}} \mathcal{O}_F/N\mathcal{O}_F = \varprojlim_{I \subset \mathcal{O}_F} \mathcal{O}_F/I,$$

where I ranges over all the non-zero ideals of $\mathcal{O}_F$. As before, we define the ring of *finite adèles* of F by $\mathbb{A}_F^\infty = F \otimes_{\mathcal{O}_F} \widehat{\mathcal{O}}_F$, where the topology is the strongest such that the map

$$\begin{aligned} F \times \widehat{\mathcal{O}}_F &\longrightarrow \mathbb{A}_F^\infty \\ (x, z) &\longmapsto x + z \end{aligned}$$

is continuous. Then $\mathbb{A}_F^\infty$ is a locally profinite topological ring containing $\widehat{\mathcal{O}}_F$ as an open subring. The *adèle ring* of F is then defined by

$$\mathbb{A}_F \stackrel{\text{def}}{=} (F \otimes_{\mathbb{Q}} \mathbb{R}) \times \mathbb{A}_F^\infty.$$

In the same way as for the adèle ring of $\mathbb{Q}$, we can write $\mathbb{A}_F$ as a restricted direct product

$$\mathbb{A}_F = \prod_{v \in \Omega_F}{}' (F_v : \mathcal{O}_{F_v}),$$

where Ω_F is the set of all places of F.

Lemma 2.50. *Let G be a totally disconnected topological group. Then G is Hausdorff.*

Proof. Let e be the identity element of G. In any topological space, the connected components are closed, so $\{e\}$, which by assumption is a connected component of G, is closed. The diagonal in $G \times G$ is the inverse image of $\{e\}$ under the continuous map $G \times G \to G$ defined by $(g, h) \mapsto gh^{-1}$, so it is closed in $G \times G$. We conclude that G is Hausdorff. □

Lemma 2.51. *Let F be a number field.*

1. *The topological ring $\mathbb{A}_F$ is a locally compact Hausdorff space.*
2. *The topology on F induced from $\mathbb{A}_F$ is the discrete topology.*
3. *The subgroup F is closed in $\mathbb{A}_F$.*
4. *The quotient group $\mathbb{A}_F/F$ is a compact Hausdorff space.*

Proof. For simplicity, we do the case $F = \mathbb{Q}$; the general case is left as an exercise.

To prove (1), we note that $\mathbb{A}^\infty$ is totally disconnected and therefore Hausdorff by Lemma 2.50. Since $\mathbb{R}$ is also Hausdorff, the space $\mathbb{A} = \mathbb{R} \times \mathbb{A}^\infty$ is a product of two Hausdorff spaces and is therefore Hausdorff. Similarly, $\mathbb{A}^\infty$ and $\mathbb{R}$ are both locally compact, so $\mathbb{A}$ is a product of two locally compact spaces and is therefore locally compact.

For (2), we observe that $U = (-1, 1) \times \widehat{\mathbb{Z}} \subset \mathbb{A}$ is open and $U \cap \mathbb{Q} = \{0\}$. Hence the point 0 is open for the topology on $\mathbb{Q}$ induced from $\mathbb{A}_\mathbb{Q}$. By translating U by elements of $\mathbb{Q}$, we see similarly that every point in $\mathbb{Q}$ is open for the topology induced from $\mathbb{A}_\mathbb{Q}$.

Claim (3) follows from (2) and the (easily verified) fact that every discrete subspace of a Hausdorff space is closed.

Finally, to prove (4), we first note that a quotient of a Hausdorff topological group by a closed subgroup is again Hausdorff. To show compactness, consider the compact subset $[-1, 1] \times \widehat{\mathbb{Z}} \subset \mathbb{A}$. It is left as an exercise to show that this surjects onto $\mathbb{A}/\mathbb{Q}$ (Exercise 2.51). □

Partial adèle rings: omitting a set of places

It is often convenient to look at adèle rings where certain places are excluded from the products. A fairly standard notation is the following. Let Σ_1, Σ_2 be two sets of places of F. Then we define

$$\mathbb{A}_{F,\Sigma_1} \stackrel{\text{def}}{=} \prod_{v\in\Sigma_1}{}' (F_v : \mathcal{O}_{F_v}),$$
$$\mathbb{A}_F^{\Sigma_2} \stackrel{\text{def}}{=} \prod_{v\notin\Sigma_2}{}' (F_v : \mathcal{O}_{F_v}),$$

so sets in the superscript denote "excluded places" and sets in the subscript denote "included places". For instance, this explains the notation $\mathbb{A}_{\mathbb{Q}}^{\infty}$ for the finite adèles of $\mathbb{Q}$.

Example 2.52. Let q be a prime number. Then $\mathbb{A}_{\mathbb{Q}}^{\infty,q}$ denotes the ring of finite adèles away from the prime number q. It is canonically isomorphic to the quotient of $\mathbb{A}_{\mathbb{Q}}$ by the ideal $\mathbb{R}\times\mathbb{Q}_q$ (note: not a subring of $\mathbb{A}_{\mathbb{Q}}$).

2.6 Idèles

The idèle group

If $(R,\mathcal{T})$ is a topological ring, its unit group $R^\times$ is equipped with a canonical topology $\mathcal{T}^\times$ making $R^\times$ into a topological group. One way to define $\mathcal{T}^\times$ is as the subspace topology induced from the injection

$$R^\times \to R\times R,$$
$$x \mapsto (x, x^{-1}),$$

where $R\times R$ is equipped with the product topology. Equivalently, $\mathcal{T}^\times$ is the weakest topology on $R^\times$ for which both the inclusion $R^\times\to R$ and the inversion map $R^\times\to R^\times$ are continuous.

Remark 2.53. The topology $\mathcal{T}^\times$ is a refinement of the subspace topology from R; it may or may not be a strict refinement. If F is a local field, then the topology on $F^\times$ is just the subspace topology from F; see Exercise 2.53. On the other hand, the topology on $\mathbb{A}_F^\times$ (see below) is strictly finer than the subspace topology from $\mathbb{A}_F$.

Definition 2.54. The group of *finite idèles* of a number field F is defined as the unit group $\mathbb{A}_F^{\infty,\times}$ of $\mathbb{A}_F^{\infty}$. Similarly, the group of *idèles*, or *idèle group*, of F is defined as the unit group $\mathbb{A}_F^\times$ of $\mathbb{A}_F$.

We view $\mathbb{A}_F^{\infty,\times}$ and $\mathbb{A}_F^\times$ as topological groups equipped with the topology defined above. As a restricted product, we have (putting $\mathcal{O}_v^\times = F_v^\times$ for every infinite place v)

$$\mathbb{A}_F^{\infty,\times} = \prod_{\text{finite } F\text{-places } v}{}' (F_v^\times : \mathcal{O}_{F_v}^\times),$$
$$\mathbb{A}_F^\times = \prod_{F\text{-places } v}{}' (F_v^\times : \mathcal{O}_{F_v}^\times)$$
$$\cong (F\otimes_{\mathbb{Q}}\mathbb{R})^\times \times \mathbb{A}_F^{\infty,\times}.$$

Recall that for every place v of F we have a local norm

$$|\cdot|_{F_v} : F_v^\times \to \mathbb{R}_{>0}.$$

The *adèlic norm* $|\cdot|_{\mathbb{A}_F^\times}$ on $\mathbb{A}_F^\times$ is the product over all the local norms:

$$\begin{aligned} |\cdot|_{\mathbb{A}_F^\times} \colon \mathbb{A}_F^\times &\to \mathbb{R}_{>0} \\ (x_v) &\mapsto \prod_v |x_v|_{F_v}, \end{aligned}$$

where v runs over the set of all places of F. Note that this product is well defined because $|x_v|_{F_v} = 1$ for all but finitely many v; it is a continuous group homomorphism.

In Exercise 2.54, you will prove the *product formula* for the adèlic norm $|\cdot|_{\mathbb{A}_F^\times}$, *i.e.* $|x|_{\mathbb{A}_F^\times} = 1$ for all principal idèles $x \in F^\times \subset \mathbb{A}_F^\times$.

The following lemma is an analogue of Lemma 2.51.

Lemma 2.55. *Let F be a number field.*

1. *The topological group $\mathbb{A}_F^\times$ is a locally compact Hausdorff space.*
2. *The topology on $F^\times$ induced from $\mathbb{A}_F^\times$ is the discrete topology.*
3. *The subgroup $F^\times$ is closed in $\mathbb{A}_F^\times$.*

However, as we will see below, $\mathbb{A}_F/F^\times$ is *not* compact.

Class groups and idèle class groups

Recall from algebraic number theory the notion of *fractional $\mathcal{O}_F$-ideals*. By definition these are the non-zero $\mathcal{O}_F$-submodules $I \subset F$ such that for some $x \in F^\times$ we have $xI \subset \mathcal{O}_F$. The *principal fractional ideals* are then those submodules that are generated by an element of $F^\times$. The *class group of F* is then the group Cl_F of fractional $\mathcal{O}_F$-ideals modulo principal ideals. This group is finite for all F. In Exercise 2.59, you will show that there is a canonical isomorphism

$$\mathbb{A}_F^{\infty,\times}/F^\times \widehat{\mathcal{O}}_F^\times \cong \mathrm{Cl}_F\,. \tag{2.5}$$

In the modern formulation of class field theory, one introduces the *idèle class group*, which is the locally compact topological group

$$C_F = F^\times \backslash \mathbb{A}_F^\times.$$

The isomorphism (2.5) describes the class group as a quotient of the idèle class group C_F by a closed subgroup of finite index.

Remark 2.56. In the notation for the quotient $F^\times\backslash\mathbb{A}_F^\times$, we have written the quotient by $F^\times$ on the left. Because $\mathbb{A}_F^\times$ is commutative, we could just as well have written this quotient as $\mathbb{A}_F^\times/F^\times$. However, writing the subgroup on the left is more consistent in the non-commutative setting; there one encounters quotients such as $\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A}_F)$, in which there is a difference with the corresponding quotient on the right.

By the product formula, the adèlic norm $|\cdot|_{\mathbb{A}_F^\times}$ induces a surjective continuous group homomorphism

$$|\cdot|_{C_F} \colon C_F \to \mathbb{R}_{>0}.$$

The kernel of $|\cdot|_{C_F}$ is a compact subgroup of C_F and is denoted by C_F^1.

Hecke characters

We will now take a closer look at Dirichlet characters in the adèlic setting. This will motivate the definition of Hecke characters.

By Exercise 2.60, there is a canonical isomorphism

$$\mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times \xrightarrow{\sim} \mathbb{Q}^\times \backslash \mathbb{A}^\times \tag{2.6}$$

of topological groups. If $\chi\colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ is a Dirichlet character modulo some positive integer n, then χ induces a continuous group homomorphism

$$\begin{aligned} \widehat{\mathbb{Z}}^\times &\to \mathbb{C}^\times \\ u &\mapsto \chi(u \bmod n). \end{aligned}$$

In view of the isomorphism (2.6), it is natural to extend this to a continuous group homomorphism

$$\begin{aligned} \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times &\to \mathbb{C}^\times \\ (t, u) &\mapsto t^s \cdot \chi(a \bmod n) \end{aligned}$$

where $s \in \mathbb{C}$ can be chosen freely. Finally, we can use (2.6) to identify this with a homomorphism

$$\omega_{\chi,s}\colon \mathbb{A}^\times \to \mathbb{C}^\times$$

that is trivial when restricted to $\mathbb{Q}^\times$.

Definition 2.57. Let F be a number field. A *Hecke character* for F is a continuous group homomorphism

$$\omega\colon \mathbb{A}_F^\times \to \mathbb{C}^\times$$

that is trivial on the subgroup $F^\times$ of $\mathbb{A}_F^\times$.

Unfortunately, general Hecke characters are not as easy to describe explicitly as are Dirichlet characters. It is already a lot simpler for number fields of class number 1.

Example 2.58. Let $F = \mathbb{Q}(\sqrt{-1})$. In §1.2.4, we considered the character χ of the group I of fractional ideals of $\mathcal{O}_F = \mathbb{Z}[\sqrt{-1}]$ defined by

$$\begin{aligned} \chi\colon I &\to F^\times \\ \mathfrak{a} &\mapsto a^4, \end{aligned}$$

where a is a generator of the fractional $\mathcal{O}_F$-ideal $\mathfrak{a}$. Embedding F into $\mathbb{C}$, we can "translate" the character χ into a Hecke character ω of F as follows (explaining why this is the correct "translation" would require more details about the relationship between the classical and adèlic language):

$$\begin{aligned} \omega\colon \mathbb{A}_F^\times &\longrightarrow \mathbb{C}^\times \\ (x_v)_{v\in\Omega_F} &\longmapsto x_\infty^4 \cdot \prod_{\mathfrak{p}} \pi_{\mathfrak{p}}^{-4v_{\mathfrak{p}}(x_{\mathfrak{p}})}. \end{aligned}$$

Here $\mathfrak{p}$ runs over all prime ideals of $\mathbb{Z}[\sqrt{-1}]$ and $\pi_{\mathfrak{p}}$ is any generator of $\mathfrak{p}$. Note that the result does not depend on the choice of the $\pi_{\mathfrak{p}}$ because the exponent is a multiple of 4.

2.7 Class field theory

Let $\mathbb{Q}(\mu_\infty) = \varinjlim_{n\geq 1} \mathbb{Q}(\mu_n)$ be the (infinite) algebraic extension of $\mathbb{Q}$ obtained by adjoining all roots of unity. Recall that there exist canonical isomorphisms

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \quad \text{for all } n \geq 1,$$

and hence a canonical isomorphism

$$\widehat{\mathbb{Z}}^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q}).$$

In particular, $\mathbb{Q}(\mu_\infty)$ is an Abelian extension of $\mathbb{Q}$. By the famous *Kronecker–Weber theorem*, every Abelian extension of $\mathbb{Q}$ can be embedded into $\mathbb{Q}(\mu_\infty)$. It turns out that for general number fields, the description of all Abelian extensions is much more involved; for this reason, class field theory was developed.

Let F be a field, let $\bar{F}$ be an separable closure of F, and let $G = \mathrm{Gal}(\bar{F}/F)$. The *commutator subgroup* of G is the *closed* subgroup $[G, G] \subseteq G$ (topologically) generated by all commutators $[g, h] = ghg^{-1}h^{-1}$ with $g, h \in G$. The *Abelianisation* of G is the quotient

$$G^{\mathrm{ab}} = G/[G, G]$$

of topological groups. There is a unique maximal extension F^{ab} of F inside $\bar{F}$ that is Abelian over F; it is called the *maximal Abelian extension of* F and equals the fixed field of $[G, G]$ inside $\bar{F}$. Galois theory gives an isomorphism

$$G^{\mathrm{ab}} \xrightarrow{\sim} \mathrm{Gal}(F^{\mathrm{ab}}/F).$$

In the case where F is a local or global field, the aim of class field theory is to describe F^{ab} and G^{ab} in terms of "data coming from F". In the case where F is a local field, the relevent object is just the unit group $F^\times$. In the case of number fields, the relevant object is the idèle class group C_F introduced earlier.

Theorem 2.59 (Main theorem of local class field theory)**.** *Let F be a local field.*

1. *There is a canonical inclusion-reversing bijection between the partially ordered set of finite Abelian extensions of F (inside $\bar{F}$) and the partially ordered set of closed subgroups of finite index in $F^\times$.*

2. *If L is a finite Abelian extension of F and N_L is the corresponding closed subgroup of finite index in $F^\times$, then there is a canonical isomorphism*

$$F^\times/N_L \xrightarrow{\sim} \mathrm{Gal}(L/F).$$

As a consequence, the above isomorphisms induce an isomorphism

$$\widehat{F^\times} \xrightarrow{\sim} \mathrm{Gal}(F^{\mathrm{ab}}/F) \tag{2.7}$$

of topological groups, where $\widehat{F^\times}$ is the profinite completion of $F^\times$.

Theorem 2.60 (Main theorem of global class field theory)**.** *Let F be a number field.*

1. *There is a canonical inclusion-reversing bijection between the partially ordered set of finite Abelian extensions of F (inside $\bar{F}$) and the partially ordered set of closed subgroups of finite index in C_F.*

2. *If L is a finite Abelian extension of F and N_L is the corresponding closed subgroup of finite index in C_F, then there is a canonical isomorphism*

$$C_F/N_L \xrightarrow{\sim} \mathrm{Gal}(L/F).$$

As a consequence, one obtains a canonical isomorphism

$$C_F/U_F \xrightarrow{\sim} \mathrm{Gal}(F^{\mathrm{ab}}/F)$$

of topological groups, where U_F is the intersection of all closed subgroups of finite index in C_F.

One possible choice for a closed subgroup of finite index is the image of $(F\otimes_{\mathbb{Q}}\mathbb{R})^\times \times \widehat{\mathcal{O}}_F^\times$ in C_F. The corresponding finite Abelian extension of F is the *Hilbert class field* H_F of F. This is the maximal *unramified* Abelian extension of F (where the extension $\mathbb{C}/\mathbb{R}$ is regarded as being ramified for this purpose). The Galois group $\mathrm{Gal}(H_F/F)$ is canonically isomorphic to the ideal class group of F; see Exercise 2.64. Another choice is the smaller subgroup where at the real places one only takes the the subgroup of positive elements; this gives rise to the *narrow Hilbert class field* of F, the maximal Abelian extension that is unramified at all finite places.

Example 2.61. The imaginary quadratic field $K = \mathbb{Q}(\sqrt{-15})$ has discriminant $-15 = -3\cdot 5$. The field $H = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$ is an unramified quadratic extension of K, and can in fact be shown to be the Hilbert class field of K.

Example 2.62. The Hilbert class field of $K = \mathbb{Q}(\sqrt{-23})$ is $H_K = K(\alpha)$, where $\alpha^3 - \alpha - 1 = 0$. In this example the description of H_K is harder to "guess" than in the previous example. However, there exists a general method to determine Hilbert class fields (and other Abelian extensions) of imaginary quadratic fields, namely the theory of *complex multiplication*.

Example 2.63. Let K be the cubic field $\mathbb{Q}(\alpha)$ of discriminant -3299, where $\alpha^3 - \alpha^2 + 9\alpha - 8 = 0$. The Hilbert class field of K is $H_K = K(\beta)$, where $\beta^3 - (\alpha+1)\beta - 1 = 0$. To "guess" H_K in cases of this kind, one can use the (as yet unproved) *Stark conjectures*.

2.8 Appendix: Weak and strong approximation

Let Ω be the set of all places of $\mathbb{Q}$.

Let X be an (affine or projective) algebraic variety over $\mathbb{Q}$ (or more generally a global field). We have injective maps

$$X(\mathbb{Q}) \subseteq X(\mathbb{A}) \subseteq \prod_{v\in\Omega} X(\mathbb{Q}_v)$$

of topological spaces; here $X(\mathbb{Q})$ is equipped with the discrete topology, $X(\mathbb{Q}_v)$ with the v-adic topology, $X(\mathbb{A})$ with the restricted product topology, and $\prod_{v\in\Omega} X(\mathbb{Q}_v)$ with the product topology. (Defining the topology on $X(\mathbb{A})$ for general varieties X requires

discussing integral models. We will not do this here, since in the particular cases that we are interested in, there is an "obvious" notion of integral points.)

Note that both of the above inclusions are continuous, but the topology on $X(\mathbb{A})$ is in general finer than the subspace topology inherited from $\prod_{v\in\Omega} X(\mathbb{Q}_v)$. However, if the variety X is projective, then $X(\mathbb{Z}_v)$ is equal to $X(\mathbb{Q}_v)$ for every finite place v, and consequently the topological spaces $X(\mathbb{A})$ and $\prod_{v\in\Omega} X(\mathbb{Q}_v)$ can be identified.

We say that X satisfies *weak approximation* if (the image of) $X(\mathbb{Q})$ is a dense subspace of $\prod_{v\in\Omega} X(\mathbb{Q}_v)$. In other words X satisfies weak approximation if and only if every non-empty open subset of $\prod_{v\in\Omega} X(\mathbb{Q}_v)$ contains a rational point. Because of the definition of the product topology, this is equivalent to saying that for every finite subset $S \subset \Omega$, the subset $X(\mathbb{Q})$ is dense in $\prod_{v\in S} X(\mathbb{Q}_v)$.

We say that X satisfies *strong approximation* if $X(\mathbb{Q})$ is dense in $X(\mathbb{A})$ equipped with the restricted product topology.

Note that if X satisfies strong approximation, then X also satisfies weak approximation because the inclusion map from $X(\mathbb{A})$ to $\prod_{v\in\Omega} X(\mathbb{Q}_v)$ is continuous with dense image. However, the converse does not hold; since the topology on $X(\mathbb{A})$ is finer than the subspace topology inherited from $\prod_{v\in\Omega} X(\mathbb{Q}_v)$, the closure of $X(\mathbb{Q})$ in $X(\mathbb{A})$ is in general smaller than the intersection of $X(\mathbb{A})$ with the closure of $X(\mathbb{Q})$ in $\prod_{v\in\Omega} X(\mathbb{Q}_v)$.

Example 2.64. The affine line satisfies weak approximation but not strong approximation: $\mathbb{Q}$ is dense in $\prod_{v\in\Omega} \mathbb{Q}_v$ (Exercise 2.66), but is discrete as a subspace of $\mathbb{A}$. For example, there are no rational numbers x satisfying $|x|_v \leq 1$ for all finite places v and $|x - 1/2|_\infty < 1/2$. However, the affine line does satisfy strong approximation outside any non-empty set of places of $\mathbb{Q}$; see Exercise 2.67.

There are analogous notions "away from a fixed set of places". If Σ is any subset of Ω, then X satisfies *weak approximation away from* Σ if $X(\mathbb{Q})$ is dense in $\prod_{v\in\Omega\setminus\Sigma} X(\mathbb{Q}_v)$, and X satisfies *strong approximation away from* Σ if $X(\mathbb{Q})$ is dense in $X(\mathbb{A}^\Sigma)$ (defined in the same way as $X(\mathbb{A})$ but using the set of places $\Omega \setminus \Sigma$ instead of Ω).

2.9 Exercises

Profinite groups

Exercise 2.1. Show that a group object in the category of groups Grp is an abelian group, in the following sense. Let A be an abelian group. Then, notice that, $m\colon A \times A \to A$ and $i\colon A \to A$ are morphisms of groups, and hence (A, m, i) is a group object in Grp. Show that all group objects in Grp are of this form.

Exercise 2.2. Let Y be a projective limit of a projective system of topological spaces $(Y_i)_{i\in I}$. Let X be a topological space, and $f\colon X \to Y$ be a continuous morphism. Show that if for every $i \in I$ the composition $X \to Y \to Y_i$ is surjective, then f has dense image.

Exercise 2.3. Show that in the category of topological spaces, a projective limit of compact Hausdorff spaces is non-empty.

Exercise 2.4. Let X be a topological space. Show that X is homeomorphic to a projective limit of finite discrete spaces if and only if X is Hausdorff, compact and totally disconnected.

Exercise 2.5. Let G be a topological group. Show that G is totally disconnected and locally compact (*i.e.* "locally profinite") if and only if there exists an open profinite subgroup $K \subset G$.

Exercise 2.6. (a) Show that the only continuous group homomorphism from $\widehat{\mathbb{Z}}$ to the additive group of $\mathbb{C}$ is the trivial homomorphism.

(b) Show that every continuous group homomorphism $\widehat{\mathbb{Z}} \to \mathbb{C}^\times$ has finite image.

(c) Let p be a prime number. Show that the only continuous group homomorphism from $\mathbb{Q}_p$ to the additive group of $\mathbb{C}$ is the trivial homomorphism.

(d) Let p be a prime number. Show that the image of a continuous group homomorphism $\mathbb{Q}_p \to \mathbb{C}^\times$ is either trivial or infinite, and give an example of the second case.

Exercise 2.7. (a) Give the $\mathbb{C}$-algebra R over $\mathbb{C}$ such that $\operatorname{spec} R = \mathbb{G}_{\mathrm{m},\mathbb{C}} \times_{\mathbb{C}} \mathbb{G}_{\mathrm{m},\mathbb{C}}$.

(b) The multiplication mapping $m\colon \operatorname{spec} R \to \mathbb{G}_{\mathrm{m},k}$ induces on global sections a mapping $\mathbb{C}[X^{\pm 1}] \to R$; describe this map explicitly.

(c) Compute the endomorphism ring $\operatorname{End}_{\mathbb{C}\text{-Grp}}(\mathbb{G}_{\mathrm{m},\mathbb{C}})$.

Exercise 2.8. Let G be a topological group.

(a) Let $H \subset G$ be an open subgroup. Show that H is also closed.

(b) Show that the converse does not hold by giving an example of a closed subgroup that is not open.

(c) Assume G is compact. Show that any open subgroup H of G contains an open normal subgroup.

Now assume that G is profinite.

(a) Show that any open subgroup has finite index.

(b) Show that any continuous morphism $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$ has finite image.

Exercise 2.8.$\frac{1}{2}$. Let ρ be as in the previous exercise. Show that any $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$ has up to conjugation image in $\mathrm{GL}_n(F)$ where $F \subset \mathbb{C}$ is some number field.

Exercise 2.9. Let G be locally profinite group.

(a) Let $\mathcal{C}_c^\infty(G)$ be the space of locally constant functions $f\colon G \to \mathbb{C}$ that are compactly supported. Show that there exists an, up to scalar unique, non-trivial linear functional $\mu\colon \mathcal{C}_c^\infty(G) \to \mathbb{C}$ that is invariant under left translation by G, *i.e.* $\mu \in \mathcal{C}_c^\infty(G)^* = \operatorname{Hom}_{\mathbb{C}}(\mathcal{C}_c^\infty(G), \mathbb{C})$ is such that for all $f \in \mathcal{C}_c^\infty(G)$ and all $g \in G$ we have $\mu(f) = \mu({}^g f)$ where ${}^g f$ is the function $x \mapsto f(g^{-1}x)$.

(b) The functional μ is the *left Haar measure* of G. We write $\int_G f \, \mathrm{d}\mu$ for $\mu(f)$. The group G is called *unimodular* if μ is invariant under right translations. Give an example of a locally profinite group which is unimodular, and one which is not.

Exercise 2.10. Let G be a profinite group and $\rho\colon G \to \mathrm{GL}_n(\mathbb{Q}_\ell)$ be a continuous morphism. Show that ρ has up to conjugation image in the group $\mathrm{GL}_n(\mathbb{Z}_\ell)$.

Exercise 2.11. Let G be a profinite group of pro-order prime to ℓ, *i.e.* G is isomorphic to a projective limit of finite groups that are of order prime to ℓ. Show that any continuous morphism $G \to \mathrm{GL}_n(\mathbb{Q}_\ell)$ has finite image.

Exercise 2.12. Let G be a profinite group and $\rho\colon G \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ be a continuous morphism. Show that ρ has, up to conjugation, image in $\mathrm{GL}_n(F)$ where $F \subset \overline{\mathbb{Q}}_\ell$ is a finite extension of $\mathbb{Q}_\ell$.

Exercise 2.13. Let p be a prime number. Consider the group $\mathrm{SL}_2(\mathbb{Z}_p)$ of invertible 2×2-matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with coefficients in $\mathbb{Z}_p$, such that $ad-bc=1$. We give $\mathrm{SL}_2(\mathbb{Z}_p)$ a topology by pulling back the product topology on $\mathrm{M}_2(\mathbb{Z}_p)^2 \cong \mathbb{Z}_p^8$, via the injection $\mathrm{SL}_2(\mathbb{Z}_p) \rightarrowtail \mathrm{M}_2(\mathbb{Z}_p)^2$, $g \mapsto (g, g^{-1})$.

(a) Show that the group $\mathrm{SL}_2(\mathbb{Z}_p)$ is profinite.

(b) Show that we have an isomorphism $\mathrm{SL}_2(\mathbb{Z}_p) \xrightarrow{\sim} \varprojlim_{n\in\mathbb{Z}_{\geq 1}} \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

(c) Show that the mapping $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}_p)$ has dense image. Show that the mapping $\mathrm{GL}_2(\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}_p)$ does not have dense image.

Exercise 2.14. Let $\{G_i, i\in I, \leq\}$ be a filtered projective system of groups, so where I is an index set that is partially ordered by $\leq$, and where for each $i\in I$ we have a finite group G_i, and for each pair of indices $i,j\in I$ with $i\leq j$ we have a surjection $f_{ji}\colon G_j \twoheadrightarrow G_i$. We require that for all inequalities of the form $i\leq j\leq k$ in I we have that $f_{ki} = f_{ji}\circ f_{kj}$, and for all $i\in I$ that $f_{ii} = \mathrm{Id}_{G_i}$.

(a) Show that the projective limit $G = \varprojlim_{i\in I} G_i$ is either finite or uncountably infinite.

(b) Show that as a topological space, $\mathbb{Z}_2$ is isomorphic to the Cantor set.

Infinite Galois theory

Exercise 2.15. Show that any profinite group G arises as the Galois group of some, possibly infinite, Galois extension L/F of fields.

Exercise 2.16. Consider the set S of formal products $x = \prod_{p \text{ prime}} p^{n_p}$, where $n_p \in \mathbb{Z}_{\geq 0}\cup\{\infty\}$.

(a) Show that the set S parametrizes naturally the (algebraic) extensions $M\subset\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$.

(b) Let $x,y\in S$ and $M_x, M_y \subset \overline{\mathbb{F}}_q$ be the corresponding fields. Express in terms of x,y when M_x is a subfield of M_y, and determine in this case the profinite group $\mathrm{Gal}(M_y/M_x)$.

Exercise 2.17. Show that the topologies defined in (2.2) and (2.3) are equivalent.

Exercise 2.18. Let $L/M/F$ be (possibly infinite) Galois extensions of the number field F. Show that the mapping $\mathrm{Gal}(L/F) \to \mathrm{Gal}(M/F)$ is surjective.

Exercise 2.19. In the spirit of Grothendieck, there is a more categorical way to formulate Galois theory (Theorem 2.15): Let F be an algebraic field with absolute Galois group $G = \mathrm{Gal}(\overline{F}/F)$. Define

$\mathcal{C}_F =$ The category of F-algebras M such that every element $x \in M$ satisfies $f(x) = 0$ for some separable polynomial $f \in F[X]$.

G-spaces= The category of compact, totally disconnected topological spaces X that are equipped with a continuous G-action, and the space of orbits X/G is finite.

Let X be a G-space. Write $\mathrm{Map}(X, \overline{F})$ for the F-algebra of continuous functions $X \to \overline{F}$ with pointwise addition and pointwise multiplication. The group G acts on $\mathrm{Map}(X, \overline{F})$ by translation on the functions $g(f) = (x \mapsto f(g^{-1}x))$ $(g \in G, f \in \mathrm{Map}(X, \overline{F}))$. Use Theorem 2.15 to show that the functor $\mathcal{C}_F \to G$-spaces, $M \mapsto \mathrm{Hom}_F(M, \overline{F})$ is quasi-inverse to the functor that assigns the algebra of invariant functions $\mathrm{Map}(X, \overline{F})^G$ to the G-set X.

Exercise 2.20. Let $p_1, p_2, p_3, \ldots \in \mathbb{Z}_{\geq 1}$ be the (infinite) list of all the (positive) prime numbers in $\mathbb{Z}$. Consider the extension $M = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots)$ of $\mathbb{Q}$ obtained by adjoining square roots $\sqrt{p_1}$, $\sqrt{p_2}$, ..., of the prime numbers.

(a) Explain that M is an infinite Galois extension and determine its Galois group $\mathrm{Gal}(M/\mathbb{Q})$ as a profinite group. (Hence, also determine its topology!).

(b) Show that the group $\mathrm{Gal}(M/\mathbb{Q})$ has uncountably many subgroups of index 2 that are not closed for its topology.

(c) Explain that in the statement of infinite Galois theory, one cannot remove the condition that the subgroups are closed.

Local fields

Exercise 2.21. Prove Theorem 2.35.(ii).

Exercise 2.22. Let L/F be a finite Galois extension of p-adic fields. Show that for all $x \in L$ and all $\sigma \in \mathrm{Gal}(L/F)$ we have $|\sigma(x)| = |x|$.

Exercise 2.23. Consider the power series ring $R = \mathbb{R}[[T]]$. Show that there exist an element $\sqrt{1+T} \in R$ whose square is $1 + T \in R$.

Exercise 2.24. Let F be a topological field of characteristic 0 with non-discrete topology. Show that F is a p-adic field if and only if it is locally profinite.

Exercise 2.25. Let v be a (finite or infinite) place of $\mathbb{Q}$. Show that any field automorphism $\sigma \in \mathrm{Aut}_{\mathrm{fields}}(\mathbb{Q}_v)$ is automagically continuous. Deduce that $\mathrm{Aut}_{\mathrm{fields}}(\mathbb{Q}_v) = 1$.
Hint: Try to characterize the topology by some algebraic property. For the p-adic fields $\mathbb{Q}_p$ show that $|\alpha|_p = 1$ if and only if α has an m-th root in $\mathbb{Q}_p$ for all positive integers m prime to $p(p-1)$.

Exercise 2.26. Show that Theorem 2.28 implies Proposition 2.27.

Exercise 2.27. On page 39 we computed the higher ramification groups $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p, \sqrt[p]{2})/\mathbb{Q}_p)_i$ for all (odd) prime numbers p. The goal of this exercise is to generalize this computation to $\mathbb{Q}_p(\zeta_p, \sqrt[p]{c})$ for all $c \in \mathbb{Z}_p$, $c \neq 0$.

(a) Assume $v_p(c) = 0$ and $[\mathbb{Q}_p(\zeta_p, \sqrt[p]{c}) : \mathbb{Q}_p] = p(p-1)$. Show that the ramification filtration on $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p, \sqrt[p]{c})/\mathbb{Q}_p)$ is

$$\begin{array}{cccccc} i & & -1 & & 0 & 1 & 2 \\ G_i & \mathbb{F}_p \ltimes \mathbb{F}_p^\times & & \mathbb{F}_p \ltimes \mathbb{F}_p^\times & & \mathbb{F}_p & 0 \end{array}$$

(b) Assume $0 < v_p(c) < p$. Show that the ramification filtration on $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p, \sqrt[p]{c})/\mathbb{Q}_p)$ is

$$\begin{array}{cccccccc} i & & -1 & & 0 & 1 & 2 & \cdots & p & p+1 \\ G_i & \mathbb{F}_p \ltimes \mathbb{F}_p^\times & & \mathbb{F}_p \ltimes \mathbb{F}_p^\times & & \mathbb{F}_p & \mathbb{F}_p & \cdots & \mathbb{F}_p & 0 \end{array}$$

(c) Give an explicit necessary and sufficient condition on p, similar to the one we found when $c = 2$ that predicts when $[\mathbb{Q}_p(\zeta_p, \sqrt[p]{c}) : \mathbb{Q}_p] = p - 1$.

Exercise 2.28. Give an example of a prime number p such that $\sqrt[p]{15} \in \mathbb{Q}_p$.
Hint: You may want to use a computer for this, because the smallest such prime number p is larger than 25000.

Exercise 2.29. Let $p = 3$. Find a uniformizer of the field $\mathbb{Q}_p(\zeta_{p^2}, \sqrt[p^2]{p})$.

Exercise 2.30. Recall the conjecture that any finite group arises as a Galois group of a Galois extension of $\mathbb{Q}$. In contrast, explain that over $\mathbb{Q}_p$ the Galois group of a finite Galois extension is always solvable and moreover give an example of a finite solvable group G such that for all prime numbers p and all finite Galois extensions $F/\mathbb{Q}_p$ we have $G \ncong \mathrm{Gal}(F/\mathbb{Q}_p)$.

Exercise 2.31. Determine all prime numbers p such that $\mathbb{Q}_p$ has a finite Galois extension $F/\mathbb{Q}_p$ whose Galois group is the symmetric group $\mathfrak{S}_4$. You may use the fact that the polynomial $f = X^4 - 2x + 2$ has Galois group $\mathfrak{S}_4$ over $\mathbb{Q}_2$.

Exercise 2.32. Give an example of a prime number p, two totally ramified extensions M_1, M_2 of $\mathbb{Q}_p$ both contained in a fixed algebraic closure $\overline{\mathbb{Q}}_p$, such that the compositum $M_1M_2 \subset \overline{\mathbb{Q}}_p$ is not totally ramified.

Exercise 2.33. Compute the Galois group of the splitting field of $x^5 + x + 1$ over $\mathbb{Q}_3$.

Algebraic number theory for infinite extensions

Exercise 2.34. (a) Give an example of an infinite algebraic extension $M/\mathbb{Q}$ and a prime p that is totally split in M.

(b) Give an example of an infinite algebraic extension $M/\mathbb{Q}$ and a prime p that is inert in M.

Exercise 2.35. Let $f_1, \ldots, f_n \in \mathbb{Z}[X]$ be monic polynomials of degree at least 2. Prove that there exists a prime p such that all the f_i are reducible modulo p.

Exercise 2.36. Prove Lemma 2.43. Make for each of the items a reduction to the finite case. For the finite cases you may refer to any standard text on algebraic number theory, such as the book of Neukirch [10].

Exercise 2.37. Let F be a number field. Let G be a finite group, equipped with the discrete topology. Let $\varphi\colon \mathrm{Gal}(\overline{F}/F) \to G$ be a continuous homomorphism. For every prime $\mathfrak{p}$ of F and every prime $\mathfrak{P}$ of $\overline{F}$ over $\mathfrak{p}$, let $I_{\mathfrak{P}}$ denote the inertia group at $\mathfrak{P}$. Show that φ is unramified at almost all primes of F, *i.e.* for almost all primes $\mathfrak{p}$ of F we have $\varphi(I_{\mathfrak{P}}) = \{1\}$ for all primes $\mathfrak{P}$ of $\overline{F}$ over $\mathfrak{p}$.

Exercise 2.38. Let v be a finite place of F and choose an embedding $\iota\colon \overline{F} \to \overline{F}_v$. Show that the induced mapping $\psi_\iota\colon \mathrm{Gal}(\overline{F}_v/F_v) \to \mathrm{Gal}(\overline{F}/F)$ is injective.
Hint: look up *Krasner's lemma* (you may use this lemma in your solution).

Exercise 2.39 (The ring of integers of $\mathbb{Q}(\mu_{\ell^n})$)**.** Let ℓ^n be a power of a prime number ℓ in $\mathbb{Z}$. Let $\mu_{\ell^n} \subset \overline{\mathbb{Q}}^\times$ be the roots of unity of order dividing ℓ^n. We show in this exercise that $\mathbb{Z}[\mu_{\ell^n}]$ is the ring of integers of $\mathbb{Q}(\mu_{\ell^n})$.

(a) Let $p \in \mathbb{Z}$ be a prime number different from ℓ. Show that p is unramified in $\mathbb{Q}(\mu_{\ell^n})$.

(b) Use Minkowski's theorem to show that ℓ ramifies in $\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}$.

(c) Show that the principal ideal $\ell \cdot \mathbb{Z}[\mu_{\ell^n}]$ decomposes into the $\ell^{n-1}(\ell-1)$-th power of a principal prime ideal.

(d) Deduce that $\mathbb{Z}[\mu_{\ell^n}]$ is regular at all prime numbers, and therefore integrally closed.

(e) Conclude that $\mathbb{Z}[\mu_{\ell^n}]$ is the ring of integers of $\mathbb{Q}(\mu_{\ell^n})$.

Exercise 2.40. Let n be a positive integer, and let $\mathbb{Q}(\mu_n)$ be the n-th cyclotomic field. Prove that the ring of integers of $\mathbb{Q}(\mu_n)$ equals $\mathbb{Z}[\mu_n]$.

Exercise 2.41 (The cyclotomic character)**.** We write $\mathbb{Q}(\mu_{\ell^\infty})$ for the extension of $\mathbb{Q}$ obtained by adjoining for each positive integer $n \in \mathbb{Z}_{\geq 1}$ the ℓ^n-th roots of unity to $\mathbb{Q}$. Let p be a prime number different from ℓ.

(a) Recall that for each $n \in \mathbb{Z}_{\geq 1}$, there exists a unique isomorphism $\chi_{\ell,n}\colon \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^n})) \xrightarrow{\sim} (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ such that $\sigma(\zeta) = \zeta^{\chi_{\ell,n}(\sigma)}$ for all ℓ^n-th roots of unity $\zeta \in \mathbb{Q}(\zeta_{\ell^n})$. Show that the collection of maps $\{\chi_{\ell,n}\}_{n\in\mathbb{Z}}$ induces an isomorphism $\chi_\ell\colon \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}_\ell^\times$.

(b) Explain that for all $x \in \mathbb{Z}_\ell^\times$ and all roots of unity $\zeta \in \mu_{\ell^\infty}$ of ℓ-power order, the exponentiation ζ^x is well-defined. Then show that χ_ℓ is characterized by the property that for all $\zeta \in \mu_{\ell^\infty}$ we have $\sigma(\zeta) = \zeta^{\chi_\ell(\sigma)}$.

(c) Let p be a prime number different from ℓ. Let $\mathfrak{p}$ be an $\mathbb{Q}(\zeta_{\ell^n})$-prime dividing p. Show that the composition $\mu_{\ell^n} \subset \mathbb{Z}[\mu_{\ell^n}] \to \mathbb{Z}[\mu_{\ell^n}]/\mathfrak{p}$ is injective.

(d) Deduce that $\chi_\ell(\mathrm{Frob}_p) = p$ for all roots of unity $\zeta \in \mu_{\ell^n}$ of ℓ-power order and all prime numbers p different from ℓ.

(e) Let $I_\ell \subset \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q})$ be the inertia group. What is the image of I_ℓ under χ_ℓ?

Exercise 2.42. This exercise is a continuation of Exercise 2.20

1. Compute for every prime ideal $\mathfrak{p} \subset \mathcal{O}_M$ the algebraic extension $M_\mathfrak{p}$ of $\mathbb{Q}$ contained in M corresponding to inertia group $I(\mathfrak{p}/p) \subset \mathrm{Gal}(M/\mathbb{Q})$. So $M_\mathfrak{p} = M^{I(\mathfrak{p}/p)}$.

2. Prove that there exists a morphism $\varphi\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$ of abstract groups that is ramified at infinitely many prime numbers.
   Note: By Exercise 2.37, the morphism φ cannot be continuous.

Exercise 2.43. Let p be a prime number. Show that there are infinitely many prime ideals $\mathfrak{q}$ of $\mathbb{Z}[\zeta_p]$ such that 2 is a p-th power in the finite field $\mathbb{Z}[\zeta_p]/\mathfrak{q}$.

Exercise 2.44. [1] The exact sequence $\{\pm 1\} \to \overline{F}^\times \to \overline{F}^\times$ is equivariant for the Galois action of $\mathrm{Gal}(\overline{F}/F)$ on $\overline{F}^\times$. Taking the long exact sequence of Galois cohomology, we obtain

$$\overline{F}^{\times,\mathrm{Gal}(\overline{F}/F)} \to \overline{F}^{\times,\mathrm{Gal}(\overline{F}/F)} \to \mathrm{H}^1(\mathrm{Gal}(\overline{F}/F), \{\pm 1\}) \to \mathrm{H}^1(\mathrm{Gal}(\overline{F}/F), \overline{F}^\times). \tag{2.8}$$

(a) Show that $\mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\overline{F}/F), \{\pm 1\}) = \mathrm{H}^1(\mathrm{Gal}(\overline{F}/F), \{\pm 1\})$.

(b) Show using Hilbert 90 and the result from previous exercise, that Sequence (2.8) induces an isomorphism $F^\times/F^{\times,2} \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\overline{F}/F), \{\pm 1\})$.

(c) Assume that $F = \mathbb{Q}$. Let $\chi\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$ be a non-trivial, continuous morphism that corresponds to the element $\alpha \in \mathbb{Q}^\times/\mathbb{Q}^{\times,2}$ from the previously found bijection. Consider the field of invariants, $E = \overline{\mathbb{Q}}^{\ker(\chi)}$, *i.e.* E is the set of $x \in \overline{\mathbb{Q}}$ such that for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with $\chi(\sigma) = 1$ we have $\sigma(x) = x$. Explain that $E/\mathbb{Q}$ is a quadratic extension and give a generator of this field in terms of α.

Adèles

Exercise 2.45. (a) Determine the prime ideals $P \subset \mathbb{A}$ that are open for the topology on $\mathbb{A}$.

(b) Prove that there are uncountably many prime ideals P of $\mathbb{A}$ that are not open.

Exercise 2.46. Consider the canonical inclusion map $f\colon \mathbb{A} \to \prod_{v \text{ place of } \mathbb{Q}} \mathbb{Q}_v$. Prove or disprove the following statements.

1. The map f is continuous.

2. The map f is open.

3. The map f is a homeomorphism onto its image.

Exercise 2.47. (a) Explain that in $\mathbb{Q} \otimes \prod_{p \text{ prime}} \mathbb{Z}_p$ the tensor product does not commute with the product.

(b) Explain that in $\mathbb{Z}[1/N] \otimes \prod_{p \text{ prime}} \mathbb{Z}_p$ the tensor product does commute with the product (cf. equation (2.4)).

[1] This exercise is for students who know, or are willing to learn, some basic Galois cohomology. A good reference for this is Serre's book [13].

Exercise 2.48. Let F be a number field. Show that $\mathbb{A}_F$ is canonically isomorphic to $F \otimes \mathbb{A}_{\mathbb{Q}}$.

Exercise 2.49. Let L/F be a finite extension of number fields. Show that there is an induced ring homomorphism $\mathbb{A}_F \to \mathbb{A}_L$, and that this is a homeomorphism of $\mathbb{A}_F$ onto a closed subring of $\mathbb{A}_L$.

Exercise 2.50. (a) Let $(\mathbb{R} \times \widehat{\mathbb{Z}})/\mathbb{Z}$ be the quotient of $\mathbb{R} \times \widehat{\mathbb{Z}}$ by the group $\mathbb{Z}$ that is diagonally embedded in $\mathbb{R} \times \widehat{\mathbb{Z}}$, *i.e.* the image of the map $\mathbb{Z} \to (\mathbb{R} \times \widehat{\mathbb{Z}})$, $x \mapsto (x, x)$. Show that the mapping

$$\begin{aligned}(\mathbb{R} \times \widehat{\mathbb{Z}})/\mathbb{Z} &\longrightarrow (\mathbb{R} \times \mathbb{A}^\infty)/\mathbb{Q} \\ (x, y) \bmod \mathbb{Z} &\longmapsto (x, y) \bmod \mathbb{Q}\end{aligned}$$

is an isomorphism of topological groups.

(b) Show that the mapping

$$\begin{aligned}\varprojlim_{N \in \mathbb{Z}_{\geq 1}} \mathbb{R}/N\mathbb{Z} &\longrightarrow (\mathbb{R} \times \widehat{\mathbb{Z}})/\mathbb{Z} \\ (x_N \bmod N\mathbb{Z})_{N \geq 1} &\longmapsto (x_1, (x_1 - x_N \bmod N\mathbb{Z})_{N \geq 1}) \bmod \mathbb{Z}\end{aligned}$$

is an isomorphism of topological groups, and give a description of its inverse.

(c) Conclude that $\mathbb{A}/\mathbb{Q}$ is isomorphic to the solenoid $\mathbb{S} = \varprojlim_{N \in \mathbb{Z}_{\geq 1}} \mathbb{R}/N\mathbb{Z}$.

Exercise 2.51. Prove the identity

$$\mathbb{A} = \mathbb{Q} + ([-1, 1] \times \widehat{\mathbb{Z}}).$$

(In other words, any adèle $\alpha \in \mathbb{A}$ can be written, not necessarily uniquely, as $x + \beta$ with $x \in \mathbb{Q}$ and $\beta \in [-1, 1] \times \widehat{\mathbb{Z}}$.)

Idèles

Exercise 2.52. Let R be a topological ring, and let $R^\times$ be the unit group of R equipped with the topology defined in the text. Prove that the standard action of $R^\times$ on R (*i.e.* the map $R^\times \times R \to R$ defined by $(a, b) \mapsto ab$) is continuous.

Exercise 2.53. Prove that if F is a local field, then the topology on $F^\times$ defined in the text is the subspace topology induced from the inclusion $F^\times \to F$.

Exercise 2.54. Let F be a number field. Show that $|x|_{\mathbb{A}_F^\times} = 1$ for all $x \in F^\times \subset \mathbb{A}_F^\times$ (the "product formula").
Hint: First do the case where $F = \mathbb{Q}$.

Exercise 2.55. Prove Lemma 2.55.

Exercise 2.56. Let F be a number field. Show that the subset $\mathbb{A}_F^\times \subset \mathbb{A}_F$ (equipped with the subspace topology) is closed but not open.

Exercise 2.57. Consider the set $S = \{p\}$, where p is a prime number.

(a) Construct an explicit isomorphism from the quotient $\mathbb{A}_{\mathbb{Q}}^{S,\times}/\mathbb{Q}^\times\widehat{\mathbb{Z}}^{S,\times}$ to the circle $\mathbb{R}/\mathbb{Z}$. (In particular, $\mathbb{Q}^\times\widehat{\mathbb{Z}}^{S,\times}$ is closed in $\mathbb{A}_{\mathbb{Q}}^{S,\times}$.)

(b) Conclude that $\mathbb{Q}^\times$ is not dense in $\mathbb{A}_{\mathbb{Q}}^{S,\times}$.

(c) Show that $\mathbb{Q}^\times\widehat{\mathbb{Z}}^{\{p,q\},\times}$ is dense in $\mathbb{A}^{\{\infty,p,q\},\times}$.

Exercise 2.58. Let F be a number field. Let S be a finite set of places of F. Show that the subset $F^\times \subset \mathbb{A}_{F,S}^\times = \prod_{v\in S} F_v^\times$ is dense.

Exercise 2.59. Let F be a number field. Consider the group $\mathrm{Frac}(\widehat{\mathcal{O}}_F)$ consisting of those $\mathcal{O}_F$-submodules $I \subset \mathbb{A}_F$ such that $I \otimes \mathcal{O}_{F_v}$ is non-trivial for every v, and for some $x \in \mathbb{A}_F^\times$ we have $xI \subset \widehat{\mathcal{O}}_F$.

(a) Show that the mapping $\mathrm{Frac}(\mathcal{O}_F) \to \mathrm{Frac}(\widehat{\mathcal{O}}_F)$, $I \mapsto \widehat{\mathcal{O}}_F \otimes_{\mathcal{O}_F} I$ is a bijection.

(b) Show that there is a canonical isomorphism $\mathrm{Frac}(\widehat{\mathcal{O}}_F) \cong \mathbb{A}_F^{\infty,\times}/\widehat{\mathcal{O}}_F^\times$.

(c) Deduce that there is a canonical isomorphism $\mathrm{Cl}_F = \mathrm{Frac}(\mathcal{O}_F)/F^\times \xrightarrow{\sim} \mathbb{A}_F^{\infty,\times}/\widehat{\mathcal{O}}_F^\times F^\times$.

Exercise 2.60. (a) Prove (without using Exercise 2.61) that the idèle class group $C_\mathbb{Q} = \mathbb{Q}^\times\backslash\mathbb{A}^\times$ of $\mathbb{Q}$ is canonically isomorphic to $\mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times$.

(b) Let $U_\mathbb{Q}$ be the intersection of all closed subgroups of finite index in $C_\mathbb{Q}$ (cf. Section 2.7). Prove (without using the main theorem of class field theory) that $U_\mathbb{Q}$ equals the image of $\mathbb{R}_{>0}$ under the isomorphism $\mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times \xrightarrow{\sim} C_\mathbb{Q}$ from part (a).

Exercise 2.61. Let F be a number field. Prove that there exists a canonical long exact sequence

$$1 \longrightarrow \mathcal{O}_F^\times \longrightarrow \widehat{\mathcal{O}}_F^\times \times (F\otimes\mathbb{R})^\times \longrightarrow C_F \longrightarrow \mathrm{Cl}_F \longrightarrow 1.$$

Exercise 2.62. Show that every continuous homomorphism $\mathbb{A}^\times \to \mathbb{C}^\times$ that is trivial on $\mathbb{Q}^\times$ is of the form $\omega_{\chi,s}$ (see Section 2.6), where $\chi\colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ is a Dirichlet character modulo some positive integer n and $s \in \mathbb{C}$.

Exercise 2.63. Let F be a number field, and let V be a finite-dimensional vector space over F. Let X_F be the set of $\mathcal{O}_F$-lattices in V, and let $\widehat{X}_F$ be the set of $\widehat{\mathcal{O}}_F$-lattices in the $\mathbb{A}_F^\infty$-module $\widehat{V} = \mathbb{A}_F^\infty \otimes_F V$.

(a) Show that the mapping $X_F \to \widehat{X}_F$, $\Lambda \mapsto \widehat{\Lambda} = \widehat{\mathcal{O}}_F \otimes_{\mathcal{O}_F} \Lambda$ is a bijection.

(b) Fix a lattice $\Lambda_0 \in V$. Show that the map $\mathrm{GL}_F(V) \to X_F$, $g \mapsto g\Lambda_0$ induces a bijection $\mathrm{GL}_F(V)/\mathrm{GL}_{\mathcal{O}_F}(\Lambda_0) \xrightarrow{\sim} X_F$. And similarly, $\mathrm{GL}_{\mathbb{A}_F^\infty}(\widehat{V})/\mathrm{GL}_{\widehat{\mathcal{O}}_F}(\widehat{\Lambda}_0) \xrightarrow{\sim} \widehat{X}_F$.

(c) Deduce that the mapping $\mathrm{GL}_F(V)/\mathrm{GL}_{\mathcal{O}_F}(\Lambda_0) \to \mathrm{GL}_{\mathbb{A}_F^\infty}(\widehat{V})/\mathrm{GL}_{\widehat{\mathcal{O}}_F}(\widehat{\Lambda}_0)$, $g \mapsto \mathbb{A}_F^\infty \otimes_F g$, is a bijection.

Class field theory

Exercise 2.64. Let F be a number field, let $C_F = F^\times \backslash \mathbb{A}_F^\times$ be the idèle class group of F, and let U be the image of $(F \otimes_{\mathbb{Q}} \mathbb{R})^\times \times \widehat{\mathcal{O}}_F^\times \subset \mathbb{A}_F^\times$ in C_F.

(a) Show that U is an open subgroup of C_F.

(b) Show that the finite Abelian extension of F associated to U by the main theorem of class field theory is the maximal unramified extension of F. (Here the extension $\mathbb{C}/\mathbb{R}$ of Archimedean local fields is regarded as being ramified.)

Exercise 2.65. Let F be a number field.

(a) Assume that F has two ℓ-adic places λ_1, λ_2 whose inertial degree and ramification degree over $\mathbb{Q}$ are the same. Show that any continuous character $\chi\colon \mathrm{Gal}(\overline{F}_{\lambda_1}/F_{\lambda_1}) \to \overline{\mathbb{Q}}_\ell^\times$ globalizes to a character of the absolute Galois group of F, *i.e.* there exists a continuous character $\widetilde{\chi}\colon \mathrm{Gal}(\overline{F}/F) \to \overline{\mathbb{Q}}_\ell^\times$ such that $\widetilde{\chi}|_{\mathrm{Gal}(\overline{F}_{\lambda_1}/F_{\lambda_1})} = \chi$.

(b) Now assume that ℓ is inert in F. Let λ be the F-place above ℓ. Give a necessary and sufficient condition for a character $\chi\colon \mathrm{Gal}(\overline{F}_\lambda/F_\lambda) \to \overline{\mathbb{Q}}_\ell^\times$ to globalize.

Approximation

Exercise 2.66. Prove that weak approximation holds for the affine line over $\mathbb{Q}$, *i.e.* $\mathbb{Q}$ is dense in $\prod_{v\in\Omega} \mathbb{Q}_v$.

Exercise 2.67. Let S be a finite set of places of $\mathbb{Q}$. The goal of this exercise is to prove strong approximation for the adèles of $\mathbb{Q}$ outside S, *i.e.* the statement that $\mathbb{Q}$ is dense in $\mathbb{A}^S$, holds if and only if $S \neq \emptyset$.

(a) Prove that $\mathbb{Q}$ is not dense in $\mathbb{A}$ (*i.e.* strong approximation fails for $S = \emptyset$).

(b) Prove that $\mathbb{Q}$ is dense in $\mathbb{A}^\infty$ (*i.e.* strong approximation holds for $S = \{\infty\}$).

(c) Let p be a prime number. Show that for all $\gamma \in \mathbb{A}$, all $\varepsilon > 0$, and every finite set Σ of places of $\mathbb{Q}$ with $p \notin \Sigma$ and $\infty \in \Sigma$, the open subset $\prod_{v\in\Sigma} B(\gamma_v, \varepsilon) \times \prod_{v\notin\Sigma, v\neq p} \mathbb{Z}_v$ of $\mathbb{A}^{\{p\}}$ contains a rational number.

(d) Conclude that $\mathbb{Q}$ is dense in $\mathbb{A}^S$ for every non-empty finite set S of places of $\mathbb{Q}$.

Exercise 2.68. (a) Prove that $\mathbb{Q}^\times$ is not dense in $\mathbb{A}^\times$ (*i.e.* strong approximation fails for the multiplicative group over $\mathbb{Q}$).

(b) Let v be a place of $\mathbb{Q}$. Show that $\mathbb{Q}^\times$ is not dense in $\mathbb{A}^{\{v\},\times}$ (*i.e.* strong approximation outside $\{v\}$ fails for the multiplicative group over $\mathbb{Q}$).

(c) Does there exist a finite set S of places of $\mathbb{Q}$ such that $\mathbb{Q}^\times$ is dense in $\mathbb{A}^{S,\times}$ (*i.e.* such that strong approximation outside S holds for the multiplicative group over $\mathbb{Q}$)?

Chapter 3

Galois representations

In this chapter, we will develop the basic theory of *Galois representations*. We have already seen one type of Galois representations in §1.4.1, namely *Artin representations* $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$. In modern number theory and arithmetic geometry, it turns out to be indispensable to consider representations with coefficients in fields other than $\mathbb{C}$. In this way, one obtains a much more intricate theory. From the point of view of number theory, the representations of Galois groups of number fields are the most interesting ones. However, in studying these, one is led to representations of Galois groups of local fields.

3.1 Basic representation theory

The purpose of this section is to give a brief overview of the most important concepts from representation theory. We recommend the reader to also have a look on Serre's book [14]

Let G be a group, and let A be a commutative ring. An *A-linear representation* of G consists of a free A-module V together with a group morphism $\rho_V\colon G \to \mathrm{Aut}_A(V)$. It is very useful to introduce the *group algebra* $A[G] = \bigoplus_{g\in G} A$ consisting of finite formal A-linear combinations of elements of G. The group algebra has the structure of a ring with point-wise addition, and with multiplication given by

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} a_g b_h gh = \sum_{g\in G}\left(\sum_{h\in G} a_{gh^{-1}} b_h\right) g.$$

Note that $A[G]$ is commutative if and only if either G is Abelian or A is the zero ring.

In the terminology of group rings, an A-linear representation of G is the same as a left $A[G]$-module V that is free as an A-module; the group homomorphism ρ is then part of the $A[G]$-module structure. It is customary to still write $\rho(g)v$ instead of gv to denote the image of $v \in V$ under the action of $g \in G$ when there is a possibility of confusion. In other words, the category of A-linear representations of G is isomorphic to the category of left $A[G]$-modules V that are free over A.

Remark 3.1. Note that to give a representation of a group G is to give two pieces of information. First an A-module V and then a morphism $\rho_V\colon G \to \mathrm{GL}_A(V)$. We will often suppress ρ_V from the notation, and say V is the representation (so making the map ρ_V implicit). Note that different authors with different backgrounds have different preferences. Some authors write the map $\rho\colon G \to \mathrm{GL}(V)$ and suppress the A-module V

from the notation. Yet other authors do not want to suppress anything and write (V, ρ) to denote a representation.

Remark 3.2. In the previous chapter we spoke about group objects in arbitrary categories. Using this language a representation of G is nothing but a G-set object in the category of A-modules (for which the underlying A-module is free).

Let V and W be two A-linear representations of G. A *morphism* from V to W is by definition an $A[G]$-linear map $V \to W$. Equivalently, a morphism $V \to W$ is an A-linear map that is compatible with the G-actions on both sides. The representations V and W are called *isomorphic* or *equivalent* if they are isomorphic as left $A[G]$-modules. The A-linear representations of G with morphisms between them form a category, which we identify with the category ${}_{A[G]}\mathrm{Mod}$ of left $A[G]$-modules. Like any category of modules of a ring, this is an Abelian category.

Example 3.3. Let $G = S_n$ be the symemtric group on n symbols. Then we have the permutation of representation S_n acting on $\mathbb{C}^n$: If $\sigma \in S_n$, $(x_i) \in \mathbb{C}^n$, then we put $\sigma \cdot (x_i) = (x_{\sigma^{-1}i})$.

Example 3.4. Consider the additive group $\mathbb{R}$ and let $L^2(\mathbb{R})$ be the space of square integrable functions $f\colon \mathbb{R} \to \mathbb{C}$, *i.e.* these are functions such that the integral $\int_{\mathbb{R}} |f(x)|^2 \mathrm{d}x$ converges. Two such functions are considered equivalent if their difference is supported on a set of measure 0. Then $L^2(\mathbb{R})$ is a Hilbert space. Moreover the group $\mathbb{R}$ acts on $L^2(\mathbb{R})$ by translating functions.

From now on we will restrict ourselves to the case where A is a field K. Let V be a K-linear representation of G. We say that V is *simple* or *irreducible* if V is simple as a $K[G]$-module, i.e. if V has exactly two $K[G]$-submodules, namely 0 and V. In particular, the zero representation is not regarded as irreducible. Furthermore, we say that V is *semi-simple* if V is a direct sum of simple $K[G]$-modules.

Theorem 3.5 (Maschke)**.** *Let G be a finite group, let K be a field such that $\#G$ is not divisible by the characteristic of K, and let V be a $K[G]$-module of finite K-dimension. Then V is a direct sum of simple $K[G]$-modules.*

In other words, every finite-dimensional K-linear representation of G is a direct sum of irreducible representations. We will not give a proof; the idea is to show that every short exact sequence of $K[G]$-modules splits.

Remark 3.6. The assumption that $\#G$ is not divisible by the characteristic of K is necessary, as the following example shows. Let K be a field of characteristic $p > 0$, let G be a cyclic group of order p, and let g be a generator of G. Let $V = K^2$, made into a $K[G]$-module by letting g act as $g(x, y) = (x + y, y)$. Then $V' = K \oplus \{0\}$ is a $K[G]$-submodule of V (with trivial G-action), and G also acts trivially on the quotient $V'' = V/V'$. However, the short exact sequence $[V' \rightarrowtail V \twoheadrightarrow V'']$ of $K[G]$-modules does not split. This can be viewed as an manifestation of the fact that the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$ is not diagonalisable.

Lemma 3.7 (Schur)**.** *Let K be a field, and let G be a group*

(i) Let V and W be two simple $K[G]$-modules, and let $f\colon V \to W$ be a $K[G]$-linear map. Then f is either the zero map or an isomorphism.

(ii) Let V be a simple $K[G]$-module. Then the K-algebra $\mathrm{End}_{K[G]}V$ of $K[G]$-linear endomorphisms of V is a division algebra.

(iii) Let V be a simple $K[G]$-module, where K is algebraically closed and V is finite-dimensional. Then $\mathrm{End}_{K[G]}(V) = K$.

Proof. If $f\colon V \to W$ is a morphism between simple $K[G]$-modules, then $\ker f$ and $\operatorname{im} f$ are submodules of V and W, respectively, so either $\ker f = 0$ and $\operatorname{im} f = W$, or $\ker f = V$ and $\operatorname{im} f = 0$. This proves (i), and (ii) follows by taking $W = V$. For (iii) let $X \in \mathrm{End}_{K[G]}(V)$. Choose $V \cong K^n$, then X induces an $n \times n$-matrix, and since we are over an algebraically closed field, X will have an eigenvalue λ with corresponding eigenvector v. Then $X - \lambda \in \mathrm{End}_{K[G]}(V)$, and since $(X - \lambda)(v) = 0$ the endomorphism $X - \lambda$ can't be invertible, and we must have $X = \lambda$. □

We now restrict to *complex* representations.

Proposition 3.8. *Let G be a finite group. Then the group ring $\mathbb{C}[G]$, viewed as a left module over itself, is the direct sum of all irreducible $\mathbb{C}$-linear representations V of G, with each V occurring $\dim_{\mathbb{C}} V$ times.*

The $\mathbb{C}$-linear representation $\mathbb{C}[G]$ of G is called the *(left) regular representation of G*. As it "contains" all irreducible representations of G, the regular representation is apparently a useful representation to consider. In a similar vein, we will see later that for more general (infinite topological) groups G, such as $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$, it will be essential to study representations of G via suitable spaces of continuous functions $G \to \mathbb{C}$.

We finish this section with a very useful result on constructing representations of a group G from representations of a subgroup H.

Theorem 3.9 (Frobenius reciprocity)**.** *Let G be a group, let H be a subgroup of G, and let A be a commutative ring. Let $\mathrm{Res}^G_H\colon {}_{A[G]}\mathrm{Mod} \to {}_{A[H]}\mathrm{Mod}$ denote the forgetful functor sending every $A[G]$-module V to itself viewed as an $A[H]$-module.*

(i) The functor

$$\begin{aligned} \mathrm{cInd}^G_H\colon {}_{A[H]}\mathrm{Mod} &\longrightarrow {}_{A[G]}\mathrm{Mod} \\ V &\longmapsto A[G] \underset{A[H]}{\otimes} V \end{aligned}$$

(where $A[G]$ is viewed as a right $A[H]$-module) is a left adjoint of Res^G_H.

(ii) The functor

$$\begin{aligned} \mathrm{Ind}^G_H\colon {}_{A[H]}\mathrm{Mod} &\longrightarrow {}_{A[G]}\mathrm{Mod} \\ V &\longmapsto {}_{A[H]}\mathrm{Hom}(A[G], V) \end{aligned}$$

(where $A[G]$ is viewed as a left module over its subalgebra $A[H]$ and $\mathrm{Ind}^G_H V$ is viewed as a left $A[G]$-module through the right action of $A[G]$ on itself) is a right adjoint of Res^G_H.

By the above theorem, we have functorial isomorphisms

$${}_{A[G]}\mathrm{Hom}(\mathrm{cInd}^G_H V, W) \cong {}_{A[H]}\mathrm{Hom}(V, \mathrm{Res}^G_H W)$$

and

$$ {}_{A[H]}\mathrm{Hom}(\mathrm{Res}^G_H W, V) \cong {}_{A[G]}\mathrm{Hom}(W, \mathrm{Ind}^G_H V) $$

In particular, there are canonical maps

$$ \begin{aligned} V &\to \mathrm{Res}^G_H \,\mathrm{cInd}^G_H V, \\ \mathrm{cInd}^G_H \,\mathrm{Res}^G_H W &\to W, \\ W &\to \mathrm{Ind}^G_H \,\mathrm{Res}^G_H W, \\ \mathrm{Res}^G_H \,\mathrm{Ind}^G_H V &\to V. \end{aligned} $$

The proof is left as an exercise.

Remark 3.10. The abbreviations Ind and cInd stand for "induction" and "compact induction", respectively. In the wider literature on representation theory, the left adjoint of Res^G_H is often denoted by Ind^G_H instead of cInd^G_H, and the right adjoint of Res^G_H is often denoted by Coind^G_H instead of Ind^G_H. Our usage conforms to the usual convention in the theory of automorphic forms.

We will mostly need a variant of the Frobenius reciprocity theorem when G is a *topological* group and H is a closed subgroup. In that context it is harder to define the induced representation using group algebras. Instead, one notes that there is a canonical isomorphism $\mathrm{Ind}^G_H V \cong {}_H\mathrm{Hom}(G, V)$ where the right-hand side is the set of morphisms of left H-sets, and the G-action on it is defined through the right action of G on itself. This characterisation of the induced representation is easier to generalise to topological groups.

3.2 Galois representations

Artin representations

In section 1.4.1 we discussed Artin representations. These representations are the first examples of Galois representations and in some sense also the most difficult ones. Let F be a number field. An *Artin representation* of F is a finite-dimensional representation $V/\mathbb{C}$ of its absolute Galois group $\mathrm{Gal}(\overline{F}/F)$, such that the mapping $\mathrm{Gal}(\overline{F}/F) \times V \to V$, $(\sigma, x) \mapsto \sigma \cdot x$ is continuous for the complex topology on V the profinite topology on $\mathrm{Gal}(\overline{F}/F)$ and the product topology on $\mathrm{Gal}(\overline{F}/F) \times V$. We have seen in Exercise 2.8 that any such representation has finite image and factors over the Galois group $\mathrm{Gal}(L/F)$ of some finite Galois extension L of F with $L \subset \overline{F}$. Let v be a finite F-place. The representation V is called *unramified* at v, if for every, equivalently for some (cf. Exercise 3.6), embedding of $\iota_v \colon \overline{F} \to \overline{F}_v$ the restriction of V to $\mathrm{Gal}(\overline{F}_v/F_v)$ is trivial on the inertia subgroup $I(\overline{F}_v/F_v) \subset \mathrm{Gal}(\overline{F}_v/F_v)$. Since almost all finite F-places are unramified in L/F, any Artin representation is unramified at almost all F-places v.

Let F be a number field and let V be an Artin representation of $\mathrm{Gal}(\overline{F}/F)$. Let S be the set of finite F-places v where V ramifies. Let v be a finite F-place that is not in S. For any $v \notin S$ we have the Frobenius element Frob_v in the group $\mathrm{Gal}(\overline{F}^{\ker(\rho_V)}/F) = \mathrm{Gal}(\overline{F}/F)/\ker(\rho_V)$, which is well-defined up to conjugation. Hence its characteristic polynomial

$$ \mathrm{charpol}(\mathrm{Frob}_v, V) = \det(1 - \rho_V(\mathrm{Frob}_v)X) \in \mathbb{C}[X], $$

is well-defined (and in particular the trace $\mathrm{Tr}(\mathrm{Frob}_v, V)$ is well-defined as well). In fact it is easy to see that $\mathrm{charpol}(\rho_V(\mathrm{Frob}_V)) \in \overline{\mathbb{Q}}[X]$.

The partial L-function of V outside S is defined by the infinite product

$$L^{S\cup\{v|\infty\}}(V,s) := \prod_{v\notin S\cup\{v|\infty\}} L_v(V,s) \tag{3.1}$$

where for every place $v \notin S\cup\{v|\infty\}$ the function $L_v(V,s)$ (the *Euler factor* at v) is defined in terms of $\mathrm{charpol}(\mathrm{Frob}_v, V)$ and the cardinality q_v of the residue field $\kappa(v)$ as

$$L_v(V,s) = \frac{1}{\mathrm{charpol}(\mathrm{Frob}_v, V)|_{X=q_v^{-s}}}. \tag{3.2}$$

Theorem 3.11 (Artin)**.** *The infinite product $L^{S\cup\{v|\infty\}}(V,s)$ converges absolutely and uniformly for s in sets of the form $\{s \in \mathbb{C} \mid \Re s \geq a\}$ with $a > 1$. Moreover $L^{S\cup\{v|\infty\}}(V,s)$ has a unique extension to a meromorphic function on $\mathbb{C}$.*

The main ingredient in the proof of this result is the following theorem by Brauer.

Theorem 3.12 (Brauer)**.** *Suppose that r is a finite-dimensional complex representation of a finite group G. Then there are subgroups $H_i \subset G$, one-dimensional representations ψ_i of the H_i and integers n_i such that*

$$\mathrm{Tr}\, r(\sigma) = \sum_i n_i \cdot \mathrm{Tr}(\mathrm{Ind}_{H_i}^G \psi_i)(\sigma) \quad \textit{for all } \sigma \in G.$$

The L-factors at the remaining (ramified) finite F-places v are given by

$$L_v(V,s) := \frac{1}{\mathrm{charpol}(\mathrm{Frob}_v, V^{I_v})|_{X=q_v^{-s}}} \in \mathbb{C}(p^{-s}), \tag{3.3}$$

where $I_v \subset \mathrm{Gal}(\overline{F}/F)$ is the inertia group at v (which is well defined up to conjugation). Note that since I_v is normal in the local decomposition group D_v, the quotient D_v/I_v has a natural action on the space V^{I_v}, and hence taking the characteristic polynomial of Frob_v acting on V^{I_v} is a well-defined operation. Note moreover that, in case v is unramified, (3.2) and (3.3) coincide.

To obtain the correct functional equation, the local L-factors at the infinite places have to be defined. In this course we will not pay too much attention to these local factors, but this does not mean they are unimportant. Thus, let us take the effort to write down the formulas here. For the infinite places $v|\infty$ the Artin L-function is obtained by multiplying Γ factors, as follows. First recall that the Gamma function Γ is defined by analytic continuation in z of the integral $\Gamma(z) = \int_0^\infty x^{z-1}e^{-x}\mathrm{d}x$, which converges for numbers $z \in \mathbb{C}$ with positive real part. The function Γ can then be extended to all complex numbers, except the non-positive integers (where Γ has simple poles). Define now $\Gamma_{\mathbb{R}}(s) := \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)$ and $\Gamma_{\mathbb{C}}(s) := \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1) = 2(2\pi)^{-s}\Gamma(s)$. Then for v an infinite F-place,

$$L_v(V,s) := \begin{cases} \Gamma_{\mathbb{R}}(s)^{\dim V^{D_v}}\Gamma_{\mathbb{R}}(s+1)^{\mathrm{codim} V^{D_v}} & \text{if } v \text{ is real} \\ \Gamma_{\mathbb{C}}(s)^{\dim(V)} & \text{if } v \text{ is complex,} \end{cases}$$

where D_v is the decomposition group at v (so $D_v = 1$ if v is complex and $D_v \cong \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ if v is real). This defines the Euler factors at the infinite places.

A discussion about why these definitions for the L-factors are what they are can be found in Cogdell's paper [4]. Very roughly, one could say that the definitions come from the desire that the L-functions are compatible with sums and induced representations, and definitions that were already known from the abelian case.

With the $L_v(V,s)$ defined for all F-places v the L-function $L(V,s)$ is defined at the product over all v of $L_v(V,s)$. This function is known to have meromorphic continuation (see above), and is in fact expected to be holomorphic unless V contains the trivial representation:

Conjecture 3.13 (Artin Conjecture)**.** *Let V be an irreducible Artin representation of $\mathrm{Gal}(\overline{F}/F)$. Then $L(V,s)$ is holomorphic if and only if V is non-trivial.*

Langlands has shown that this conjecture would follow if enough of the Langlands program were shown. Explaining this is one of the main goals of this course. More precisely, according to Langlands's conjecture there should exist for every algebraic automorphic representation π of $\mathrm{GL}_n(\mathbb{A}_F)$ a corresponding Galois representation $\rho\colon \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$, and also conversely. The correspondence should be such that the L-function of π matches the L-function of ρ. We will understand later that actually most ρ have infinite image, but for those that do have finite image, we can choose an isomorphism $\iota\colon \mathbb{C} \xrightarrow{\sim} \overline{\mathbb{Q}}_\ell$, and obtain a complex representation $\iota\rho$ whose L-function does not depend on ι (see Exercise 3.21). The Artin conjecture follows then immediately from the known properties of L-functions of automorphic representations.

Conductor of an Artin representation

As we have seen at local places the Galois groups are filtered by the higher ramification groups. These groups can be used to measure 'how ramified' your representation is. More precisely, let V be a continuous representation of $\mathrm{Gal}(\overline{F}/F)$ in a complex vector space, where now F is a local p-adic field. Write $G = \mathrm{Gal}(\overline{F}/F)/\ker(\rho_V)$, then G is a finite group and the induced action of G on V is faithful. Note also that G is the Galois group of some finite extension L/F. Let v be a finite F-place. We define the conductor exponent of V by

$$n_V = \underbrace{\dim(V/V^{G_0})}_{\text{tame exponent}} + \underbrace{\sum_{i=1}^{\infty} \frac{1}{[G_0 : G_i]} \dim(V/V^{G_i})}_{\text{wild exponent}} \tag{3.4}$$

As indicated, the conductor exponent n_V breaks up into a sum two components, the *wild exponent* and the *tame exponent*.

Theorem 3.14 (Artin)**.** *We have $n_V \in \mathbb{Z}$.*

With the conductor exponent defined, the *conductor* of V is the ideal $N_V = (\varpi_F^{n_V})$. Finally, if F is a number field, then the conductor of V is defined by

$$n_V = \prod_{v \text{ finite } F\text{-place}} \mathfrak{p}_v^{n_{V,v}} \subset \mathcal{O}_F,$$

where $\mathfrak{p}_v \subset \mathcal{O}_F$ is the prime ideal corresponding to the place v, and $N_{V,v}$ is the local conductor exponent from (3.4).

Functional equation

Theorem 3.15 (Artin?)**.** *Let V be an Artin representation of* $\mathrm{Gal}(\overline{F}/F)$*, where F is a number field. Then the L-function of V satisfies the following functional equation*

$$L(V,s) = w\left(|\mathcal{O}_L/N_V| \cdot \sqrt{|\Delta_F|}^{\dim(V)}\right)^{\frac{1}{2}-s} L(V^*, 1-s),$$

where $V^* = \mathrm{Hom}_{\mathbb{C}}(V,\mathbb{C})$ is the dual representation, Δ_F is the discriminant of F, w is the root number.

ℓ-adic representations

Let $\ell \in \mathbb{Z}$ be a prime number and $\overline{\mathbb{Q}}_\ell$ be an algebraic closure of $\mathbb{Q}_\ell$. A finite-dimensional $\mathbb{Q}_\ell$-vector space has a, up to equivalence unique, norm compatible with the norm on $\mathbb{Q}_\ell$. In particular, any finite extension E of $\mathbb{Q}_\ell$ contained in $\overline{\mathbb{Q}}_\ell$ has a unique norm extending the norm on $\mathbb{Q}_\ell$. We normalize the norm on E so that $|\ell|_E = \ell^{-1}$. Then, for any pair $E, E' \subset \mathbb{Q}_\ell$ the restriction of the norm on E' down to E, agrees with the norm on E. Hence the norms $(|\cdot|_E)_{E\subset\overline{\mathbb{Q}}_\ell}$ define a norm on $\overline{\mathbb{Q}}_\ell$. Using this norm we equip $\overline{\mathbb{Q}}_\ell$ with a topology. Note that, in exercise 3.16 we will see that $\overline{\mathbb{Q}}_\ell$ is not complete for this norm.

Let E be a topological ring, M a topological E-module and G a topological group. A continuous G-representation in M is an $E[G]$-module structure on M such that the action $G \times M \to M$ is continuous. A morphism of continuous representations is a continuous morphism of $E[G]$-modules. Assume E is a subfield of $\overline{\mathbb{Q}}_\ell$ containing $\mathbb{Q}_\ell$. In this case, we call a continuous, finite-dimensional representation of a topological group G in an E-vector space an *ℓ-adic* representation of G. We will mainly look at the case where the group G is the Galois group of some (infinite) Galois extension of algebraic fields in $\overline{\mathbb{Q}}$ or of closed subfields in $\overline{\mathbb{Q}}_p$ for some prime number p, but of course in principle one could study ℓ-adic representations of any topological group.

Example 3.16. In the exercises we have seen that there is a unique continuous morphism of groups, $\chi_\ell\colon \mathrm{Gal}(\overline{F}/F) \to \mathbb{Z}_\ell^\times \subset \overline{\mathbb{Q}}_\ell^\times$, such that for all ℓ^n-power roots of unity $\zeta \in \mu_{\ell^\infty}$ and all $\sigma \in \mathrm{Gal}(\overline{F}/F)$ we have $\sigma(\zeta) = \zeta^{\chi_\ell(\sigma)}$. This morphism is the *cyclotomic character*. Through the character χ_ℓ we may let $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ act on $\overline{\mathbb{Q}}_\ell$ via $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \times \overline{\mathbb{Q}}_\ell \to \overline{\mathbb{Q}}_\ell$, $(\sigma, x) \mapsto \chi(\sigma)\cdot x$. This is an example of a one-dimensional ℓ-adic $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representation. Another fundamental example is given by the Tate module of elliptic curves, we will study these in the next section.

Let F be some subfield of $\overline{\mathbb{Q}}$ or a closed subfield of $\overline{\mathbb{Q}}_p$ for some prime number p. Let E be a subfield of $\overline{\mathbb{Q}}_\ell$ containing $\mathbb{Q}_\ell$. Suppose $\psi\colon \mathrm{Gal}(\overline{F}/F) \to E^\times$ is a continuous morphism. We write $E(\psi)$ for the $\mathrm{Gal}(\overline{F}/F)$-representation with space E and $\mathrm{Gal}(\overline{F}/F)$-action given by ψ. If $\psi = \chi^k$ for some $k \in \mathbb{Z}$ then we will write $E(k) := E(\chi^k)$. More generally, if V is an arbitrary ℓ-adic $\mathrm{Gal}(\overline{F}/F)$-representation, then we write $V(\psi) := V \otimes_E E(\psi)$ and $V(k) = V \otimes_E E(k)$. The $\mathrm{Gal}(\overline{F}/F)$-representation $V(\psi)$ is called a *twist* of V by ψ.

We call an ℓ-adic representation *irreducible*, or *simple*, if it has precisely two invariant subspaces. An ℓ-adic representation is *semi-simple* if it is a direct sum of simple representations. An ℓ-adic representation V can be made semi-simple in a functorial manner in the following way. In Exercise 3.1 we will see that any ℓ-adic representation V has a canonical filtration $0 = V_0 \subset V_1 \subset \cdots V_n = V$ where the successive quotients V_i/V_{i+1} are

all semi-simple; this is called the *socle filtration* of V. The representation V is irreducible if and only if $V_1 = V$.

Proposition 3.17. *Let Λ be an algebra over a field K of characteristic zero, and let ρ_1, ρ_2 be two Λ-modules of finite K-dimension. Assume that ρ_1 and ρ_2 are semi-simple and $\mathrm{Tr}_K(\rho_1(\lambda))$ equals $\mathrm{Tr}_K(\rho_2(\lambda))$ for all $\lambda \in \Lambda$. Then ρ_1 is isomorphic to ρ_2.*

Proof. [**?**, chapter 8, sect. 12, n° 1, prop. 3]. □

Proposition 3.17 has a variant for characteristic p coefficients.

Theorem 3.18 (Brauer-Nesbitt)**.** *Let G be a finite group, E a perfect field of characteristic p and ρ_1, ρ_2 two semi-simple $E[G]$-modules, of finite dimension over E. Then $\rho_1 \cong \rho_2$ if and only if the characteristic polynomials of $\rho_1(g)$ and $\rho_2(g)$ coincide for all $g \in G$.*

Proof. [**?**, theorem 30.16]. □

ℓ-adic Galois representations

Let ℓ be a prime number. Let G be a profinite group and $E \subset \overline{\mathbb{Q}}_\ell$ a closed subfield. We call an *ℓ-adic representation* a continuous representation of G in a finite-dimensional E-vector space. We will be mostly looking at the case where either E is a finite extension of $\mathbb{Q}_\ell$ or $E = \overline{\mathbb{Q}}_\ell$.

Assume now that G is the absolute Galois group of some number field F. Then a *Galois representation* of $\mathrm{Gal}(\overline{F}/F)$ (or of F) is by definition an ℓ-adic representation V over E of $\mathrm{Gal}(\overline{F}/F)$ such that V is unramified at almost all F-places v. More precisely, we require that for almost all F-places v, and all (equivalently: one) embedding of $\overline{F}$ in an algebraic closure $\overline{F}_v$ of F_v, the restriction of $\rho_V \colon \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_E(V)$ down to $\mathrm{Gal}(\overline{F}_v/F_v)$ is trivial on the inertia subgroup $I(\overline{F}_v/F_v) \subset \mathrm{Gal}(\overline{F}_v/F_v)$. (cf. Exercise 3.6).

Theorem 3.19. *Let $V, V'/E$ be two semi-simple Galois representations of $\mathrm{Gal}(\overline{F}/F)$. Let S be a finite set finite of F-places v such that S contains all finite F-places where V or V' is ramified. Assume $\mathrm{Tr}(\mathrm{Frob}_v, V) = \mathrm{Tr}(\mathrm{Frob}_v, V')$ for all finite F-places v such that $v \notin S$. Then $V \cong V'$.*

Proof. The field $K = \overline{\mathbb{Q}}^{\ker(\rho_V) \cap \ker(\rho_{V'})}$ is a Galois extension of F which is unramified at almost all F-places. By the Chebotarev density theorem the set of Frobenius elements in $\mathrm{Gal}(K/F)$ is dense subset. Hence the equality $\mathrm{Tr}(\mathrm{Frob}_v, V) = \mathrm{Tr}(\mathrm{Frob}_v, V')$ extends to an equality $\mathrm{Tr}(\sigma, V) = \mathrm{Tr}(\sigma, V')$ for all $\sigma \in \mathrm{Gal}(\overline{F}/F)$. Hence the theorem follows from Proposition 3.17. □

L-factors and L-functions

Let F be a local p-adic field with absolute Galois group $\mathrm{Gal}(\overline{F}/F)$ and inertia subgroup $I \subset \mathrm{Gal}(\overline{F}/F)$. Let (V, ρ) be an ℓ-adic $\mathrm{Gal}(\overline{F}/F)$-representation, where ℓ is not p. The L-factor of (V, ρ) is defined by

$$L_v(V, s) := \frac{1}{\det(1 - \rho|_{V^I}(\mathrm{Frob}_v) \cdot q_v^{-s})} \in \overline{\mathbb{Q}}_\ell(q_v^{-s}), \tag{3.5}$$

where for now we view the symbol "q_v^{-s}" as a transcendental variable over $\overline{\mathbb{Q}}_\ell$, and with the notation $\rho|_{V^I}$ we mean the representation ρ restricted to the space of invariants V^I under the action of the inertia group I on V. To obtain from (3.5) an L-factor with complex coefficients we choose an isomorphism $\iota\colon \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$ (see Exercise 3.20), and apply ι to (3.5), to obtain $\iota L_v(V,s) \in \mathbb{C}(q_v^{-s})$. If we have an ℓ-adic Galois representation of a number field, we get in this way local factors for all places that do not divide ℓ. For the places dividing ℓ it is also possible to define local L-factors, but the definition is more involved, and we will not go into this question during this course. The (partial) L-function of V is then defined as the product

$$L^{\ell,\iota}(V,s) = \prod_{v\nmid\ell} \iota(L_v(V,s)) \in \mathbb{C}(p^{-s}).$$

In general the function $L^{\ell,\iota}(V,s)$ depends in a bad way on the isomorphism ι (and in particular also the prime ℓ!). But, as we will hopefully see, for many interesting Galois representations (those that come from geometry), the function $L^{\ell,\iota}(V,s)$ is nicely behaved and depends only on its restriction of ι to the algebraic number $\overline{\mathbb{Q}}$ (which is contained both in $\overline{\mathbb{Q}}_\ell$ and $\mathbb{C}$).

3.3 Elliptic curves

Let F be a field. An *elliptic curve* over F is a variety that can be given by a smooth equation in projective coordinates x, y, z of the form

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

called the *Weierstrass equation*. If the characteristic of F is not 2 or 3, the variables can be changed, and the equation can always be simplified to an equation of the form $y^2z = x^3 + axz^2 + bz^3$. The smoothness condition translates to an explicit condition on the coefficients. For the second equation, it simply states $4a^3 + 27b^2 \neq 0$. In the language of varieties over F, and elliptic curve is a connected projective smooth curve E of genus 1, that is equipped with the structure of a commutative group variety, so it has a natural addition operation $E \times E \to E$, satisfying the usual group axioms (see also the section on group objects).

Elliptic curves over the complex numbers

In case $F = \mathbb{C}$, you can use the Weierstrass equation to view E as a complex manifold, which we denote by E_{an}. Then E_{an} is a connected compact Lie group of dimension 1. The objects that you get in this way are precisely the 1-dimensional complex tori, *i.e.* a space of the form V/Λ, where V is a 1-dimensional complex vector space and $\Lambda \subset V$ is a free $\mathbb{Z}$-submodule with $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \xrightarrow{\sim} V$, $\lambda \otimes x \mapsto \lambda x$. The module Λ is then the first homology group $H_1(E,\mathbb{Z})$ of E. In fact, we have an equivalence of categories

$$\begin{aligned} \{\text{Complex elliptic curves}\} &\xrightarrow{\sim} \{\text{pairs } (V,\Lambda) \text{ with } V \text{ a 1-dim } \mathbb{C}\text{-vsp, } \Lambda \subset V \text{ a lattice}\} \\ E &\longrightarrow (\Omega^1(E)^\vee, \mathrm{H}_1(E,\mathbb{Z})) \\ V/\Lambda &\longleftarrow (V,\Lambda). \end{aligned}$$

Tate modules

The Tate module is a canonical way to attach to an elliptic curve E over a field F an ℓ-adic Galois representation of $\mathrm{Gal}(\overline{F}/F)$. The Tate module is an analogue over more general fields F of the module $\Lambda = \mathrm{H}_1(E, \mathbb{Z})$ from complex elliptic curves. However, if you are over a field F different from $\mathbb{C}$ it is not clear how to attach a free $\mathbb{Z}$-module Λ of rank 2 to elliptic curves E/F. If $F = \mathbb{Q}$ you can base change to $\mathbb{C}$ and take the $H_1(E, \mathbb{C})$ but then the Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ does not respect the geometry, and hence does not pass to an action on $H_1(E, \mathbb{Z})$. Thus you won't get a Galois representation out of the construction, which is our main goal. Furthermore, if F is a finite field $\mathbb{F}_q$ and you have an elliptic curve $E/\mathbb{F}_q$ the situation is even worse as there is no 'reasonable' way to extend the scalars to $\mathbb{C}$.

The first attempt to solving the problem is to, instead of trying to attach to E/F the module Λ, to try to attach to E the profinite completion $\widehat{\Lambda}$ of Λ. Let N be an integer, and $E(\mathbb{C}) = V/\Lambda$ an elliptic curve over $\mathbb{C}$. Let $E_N \subset E(\mathbb{C})$ be the subset of N torsion, *i.e.* the set of $x \in E(\mathbb{C})$ such that $N \cdot x = 0$. In terms of the equality $E(\mathbb{C}) = V/\Lambda$, it is easy to see that $E_N = \frac{1}{N}\Lambda/\Lambda$, and hence

$$\widehat{\Lambda} = \varprojlim_{N \in \mathbb{Z}_{\geq 1}} \Lambda/N\Lambda = \varprojlim_{N \in \mathbb{Z}_{\geq 1}} \tfrac{1}{N}\Lambda/\Lambda = \varprojlim_{N \in \mathbb{Z}_{\geq 1}} E_N$$

where the transition morphisms in the projective system on the right hand side are the maps $E_N \to E_{N'}$, $x \mapsto (N/N') \cdot x$. Now notice that on the right hand side the N-torsion E_N of E can be defined over arbitrary base fields F. In concrete terms, the addition law $+ \colon E \times E \to E$ is given by an polynomial in the coordinates. Hence the N-torsion of E is the space of solutions of the polynomial law applied N-times to itself, which shows that E_N is the solution space of some polynomial. Thus indeed E_N is a subvariety of E. More formally, E_N fits in a Cartesian diagram

$$\begin{array}{ccc} E_N & \longrightarrow & E \\ \downarrow & & \downarrow{\scriptstyle [N]} \\ \mathrm{spec}(F) & \xrightarrow[e]{} & E \end{array}$$

where $E_N = \mathrm{spec}(F) \times_{e,E,[N]} E$. Since fibre products exist in the category of varieties over F, the space E_N is indeed a variety over $\mathrm{spec}(F)$. Its dimension is 0 and has at most N^2-points over an algebraic closure $\overline{F}$ of F. In case the characteristic of F divides N, the cardinality $\#E_N(\overline{F})$ will however be strictly smaller than N^2. For instance, if F has characteristic p and $N = p$, then either $\#E_p(\overline{F}) = p$ (E is *ordinary*), or $\#E_p(\overline{F}) = 1$ (E is *supersingular*).

We are now ready to define the Tate module. Let F be a field field algebraic closure $\overline{F}$ and let E be an elliptic curve over F. We define $T(E) = \varprojlim E_N(\overline{F})$, where the projective limit ranges over all $N \in \mathbb{Z}_{\geq 1}$. The Galois group $\mathrm{Gal}(\overline{F}/F)$ acts on the finite sets $E_N(\overline{F})$, and since the multiplication by N-maps $E \to E$ are defined over F, this Galois action passes in the limit to a Galois action on $T(E)$. Similarly, the addition law is defined by polynomials over F, so the Galois action commutes with this additional law, which means that the Galois action on $T(E)$ is linear. Similar to the decomposition $\widehat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$, we can decompose $T(E)$ into a product $T(E) = \prod_\ell T_\ell(E)$ where the product ranges over all

primes numbers ℓ and $T_\ell(E)$ is the projective limit of the finite groups $E_{\ell^n}(\overline{F})$. Let p be the characteristic of F (so possibly $p = 0$). For all primes ℓ different from p the module $T_\ell(E)$ is free of rank 2 over $\mathbb{Z}_\ell$. For $\ell = p$, so when F has positive characteristic, the module $T_p(E)$ is in many ways not the right object (for instance its rank is at most 1), and even though it does carry a Galois action, it is (for our purposes) better to discard it.

Good reduction

Let E be an elliptic curve over a p-adic field F. We say that E has *good reduction* if there exists an elliptic curve $\mathcal{E}$ over $\mathcal{O}_F$ such that $\mathcal{E} \otimes F \cong E$. To make this notion precise, one would need to define what an elliptic curve over $\mathcal{O}_F$ is (which we did not do). Fortunately, the definition of good reduction can also be stated without referring to schemes, using Weierstrass equations, but since multiple Weierstrass equations can define the same curve, some care is needed to formulate the notion of good reduction in the correct manner. Let E be an elliptic curve over a p-adic field F, given by the (affine) Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.6}$$

with discriminant Δ with $v_F(\Delta) = e$. Like we said, several Weierstrass equations can give rise to the same elliptic curve. In fact, for any $u \in F$ we can replace (x, y) by $(u^{-2}x, u^{-3}y)$, the coefficients a_i of the equation then get replaced by $u^i a_i$. Thus, for i large enough we will have $a_i \in \mathcal{O}_F$. Moreover, we can take u such that $v_F(\Delta)$ is as small as possible. In this case we call our Weierstrass equation *minimal*. In terms of a minimal Weierstrass equation E has good reduction if and only if (3.6) defines an elliptic curve over $\mathbb{F}_q$, *i.e.* $v_F(\Delta) = 0$.

Theorem 3.20 (Néron-Ogg-Tate-Shafarevich)**.** *Let E be an elliptic curve over a p-adic field F with p different from ℓ. Then the curve E has* good reduction *if and only if the Galois representation $V_\ell(E) = \mathbb{Q} \otimes_{\mathbb{Z}} T_\ell(E)$ of $\mathrm{Gal}(\overline{F}/F)$ is unramified.*

Note that the above discussion gives meaning also to the reduction of elliptic curves E over number fields F. Namely, if v is a finite F-place, then F_v is a p-adic local field. The coefficients of the Weierstrass equation of E lie in F and hence also in F_v. When over F_v we have the uniformizer ϖ_{F_v}, and use this uniformizer to replace our Weierstrass equation with one that is minimal, say of discriminant $\Delta_v(E)$. The elliptic curve E then has good reduction at v if and only if $v_{F_v}(\Delta_v(E)) = 0$. Moreover, if we choose an embedding $\iota\colon \overline{F} \to \overline{F}_v$ we obtain an isomorphism

$$T_\ell(E/F) = \varprojlim_{\ell^n} E_{\ell^n}(\overline{F}) \xrightarrow{\sim} \varprojlim_{\ell^n} E_{\ell^n}(\overline{F}_v) = T_\ell(E/F_v)$$

which is equivariant for the $\mathrm{Gal}(\overline{F}_v/F_v)$-action if we restrict the $\mathrm{Gal}(\overline{F}/F)$-action to $\mathrm{Gal}(\overline{F}_v/F_v)$ along the inclusion $\mathrm{Gal}(\overline{F}_v/F_v) \to \mathrm{Gal}(\overline{F}/F)$ induced by ι.

Elliptic curves over finite fields

The Tate module $T_\ell(E)$ of an elliptic curve E over a finite field $\mathbb{F}_q$ can be used to count the number of rational points $E(\mathbb{F}_q)$. The set $\overline{\mathbb{F}}_q$-points $E(\overline{\mathbb{F}}_q)$ is the set of triples $(x, y, z) \in \overline{\mathbb{F}}_q^3$ that satisfy the Weierstrass equation taken up to the equivalence $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$

for $\lambda \in \overline{\mathbb{F}}_q^\times$, *i.e.* the equivalence from the projective space. Similarly, the set of $\mathbb{F}_q$-rational points $E(\mathbb{F}_q)$ on E would be the set of triples (x, y, z) such that, for some $\lambda \in \overline{\mathbb{F}}_q^\times$, we have $(\lambda x, \lambda y, \lambda z) \in \mathbb{F}_q^3$.

Theorem 3.21. *Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then we have the formula*

$$\mathrm{Tr}(\mathrm{Frob}_q, T_\ell(E)) = 1 - \#E(\mathbb{F}_q) + q. \tag{3.7}$$

Sketch. We would like prove this formula, but unfortunately we do not have enough time to go in all the details. We recommend the reader to have a look in Silverman's book [15], where the theory is properly built up, and the above theorem can be proved. However, we will give the main ideas that go into (3.7).

Consider again E over $\mathbb{F}_q$. Concretely this means that E is given by a Weierstrass equation where the coefficients of the equation lie in $\mathbb{F}_q$. A morphism of elliptic curves is a morphism of group varieties which can be defined over $\mathbb{F}_q$ (or equivalently, they are morphisms over $\overline{\mathbb{F}}_q$ that are invariant under the Galois action).

Consider a point $(x, y, z) \in \mathbb{P}^2(\overline{\mathbb{F}}_q)$ on E, *i.e.*

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Raising this equality to the q-th power, we obtain

$$\begin{aligned}(y^2z + a_1xyz + a_3yz^2)^q &= (x^3 + a_2x^2z + a_4xz^2 + a_6z^3)^q \\ (y^q)^2z^q + a_1^qx^qy^qz^q + a_3y^qz^q &= (x^q)^3 + a_2^q(x^q)^2(z^q) + a_4^qx^q(z^q)^2 + a_6^q(z^q)^3.\end{aligned}$$

Since, moreover $a_1, \ldots, a_6 \in \mathbb{F}_q$ we have $a_i^q = a_i$ for all i. Thus (x^q, y^q, z^q) defines another point on E. We obtain the Frobenius endomorphism,

$$\phi_q \colon E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q), \quad (x, y, z) \mapsto (x^q, y^q, z^q).$$

We only defined ϕ_q on the geometric points, but it can be defined on the elliptic curve E.

Lemma 3.22. *The set of rational points $E(\mathbb{F}_q) \subset E(\overline{\mathbb{F}}_q)$ is precisely the set of points $(x, y, z) \in E(\overline{\mathbb{F}}_q)$ that are fixed under the action of ϕ_q.*

Proof. Assume that (x, y, z) is a fixed point under Frobenius. There exists some $\lambda \in \overline{\mathbb{F}}_q^\times$ such that $\mathrm{Frob}_q(x, y, z) = (x^q, y^q, z^q) = (\lambda x, \lambda y, \lambda z)$. One of the coordinates of (x, y, z) must be non-zero; say it is z (the other cases are the same). Then we can normalize so that $z = 1$, then λ must be 1 as well, and we find $x^q = x$, $y^q = y$ and $z^q = z$ in $\overline{\mathbb{F}}_q$. By Galois theory: $x, y, z \in \mathbb{F}_q$. □

Consider the morphism

$$f = (\mathrm{id}_E - \phi_q) \colon E \to E, \quad (x, y, z) \mapsto (x, y, z) - (x^q, y^q, z^q).$$

The kernel of f is then precisely the set $\#E(\mathbb{F}_q)$.

Fact 1: A non-constant morphism $h \colon E \to E'$ is called an *isogeny*. Any isogeny has a *degree*, which is defined to be the degree of the corresponding extension $F(E)/F(E')$ of

function fields. More concretely, if E is given by the affine equation $y^2 = x^3 + ax + b$ and E' is given by the equation $y^2 = x^3 + cx + d$, then h induces a morphism of fields

$$h^*\colon \operatorname{Frac}\left(\frac{\mathbb{F}_q[x,y]}{y^2-(x^3+cx+d)}\right) \to \operatorname{Frac}\left(\frac{\mathbb{F}_q[x,y]}{y^2-(x^3+ax+b)}\right)$$

For the isogenies h where this extension is separable, the degree is also the cardinality $\#\ker(h)(\overline{\mathbb{F}}_q)$ of the kernel. For the non-separable morphisms $h\colon E \to E$, the degree of h is still the size of its kernel, but the kernel might not be reduced, and one can not simply use the $\overline{\mathbb{F}}_q$-points to measure its size. The degree of our isogeny f is equal to $\#E(\mathbb{F}_q)$ (since this f is separable), and in case of ϕ_q the degree is q (even though $\phi_q\colon E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ is injective, it's not separable and its degree is q).

Fact 2: Any non-zero morphism $h\colon E \to E$ has a unique *dual* $h^\vee\colon E \to E$ such that $h \circ h^\vee$ and $h^\vee \circ h$ equal to are equal to multiplication by the degree of h.

In particular, due to our particular choice of f, $f = \mathrm{id}_E - \phi_q$, we have

$$[\#E(\mathbb{F}_q)] = f \circ f^\vee = (1-\phi_q)\circ(1-\phi_q^\vee) = 1 - (\phi_q + \phi_q^\vee) + q \in \operatorname{End}_{\overline{\mathbb{F}}_q}(E). \tag{3.8}$$

Thus ϕ_q is a root of the polynomial

$$\begin{aligned}(X-\phi_q)(X-\phi_q^\vee) &= X^2 - (\phi_q+\phi_q^\vee)\cdot X + \phi_q \circ \phi_q^\vee \\ &= X^2 - (1 - \#E(\mathbb{F}_q) + q)\cdot X + q \in \operatorname{End}_{\overline{\mathbb{F}}_q}(E)[X].\end{aligned}$$

Put $a_E = 1 - \#E(\mathbb{F}_q) + q$. The polynomial $X^2 - a_E X + q$ is the characteristic polynomial of ϕ_q. Since the Tate module $T_\ell(E)$ is a functor in E, the Frobenius Frob_q acting on $T_\ell(E)$ is a root of the same quadratic polynomial, and $\operatorname{Tr}(\mathrm{Frob}_q, T_\ell(E)) = 1 - \#E(\mathbb{F}_q) + q$. □

The L-function of an elliptic curve at unramified places

At this point we have

Theorem 3.23. *Let E be an elliptic curve over a number field F, given by a Weierstrass equation, whose discriminant is Δ. Fix a prime number $\ell \in \mathbb{Z}$. Let v be a finite F-place with $v(\Delta) = 0$ and $v \nmid \ell$, then*

$$L_p^{(\iota)}(V_\ell(E), s) = \frac{1}{1 - a_v(E) q_v^{-s} + q_v q_v^{-2s}} \in \mathbb{C}(p^{-s})$$

where $E(\kappa(v))$ denotes the set of solutions of the fixed Weierstrass equation for E over the residue field $\kappa(v)$ of F at v, $q_v = \#\kappa(v)$, and $a_v(E) = 1 - \#E(\kappa(v)) + q_v$.

3.4 Elliptic curves with complex multiplication

Elliptic curves with CM

Let F be a number field and E and elliptic curve over F. Embed $F \subset \overline{\mathbb{Q}}$ and consider the algebra of $\overline{\mathbb{Q}}$-endomorphisms $\operatorname{End}_{\overline{\mathbb{Q}}}(E)$. For many elliptic curves E this algebra is equal to $\mathbb{Z}$, so the only endomorphisms of E are the multiplication by N maps $[N]\colon E \to E$. The second, and only other possibility, is that the ring $\operatorname{End}_{\overline{\mathbb{Q}}}(E)$ is an order R in a quadratic

imaginary field K. We recall, an *order* in a number field K is a subring $R \subset K$, which is of finite type as Z-module, and whose fraction field is K. Such rings R only contain elements that are integral over $\mathbb{Z}$, and hence $R \subset \mathcal{O}_K$, but the inclusion may be strict.

Example 3.24. The elliptic curve $E : y^2 = x^3 + x$. Observe that $I \colon (x, y) \mapsto (-x, i \cdot y)$ is an endomorphism of E that is defined over $\mathbb{Q}(i)$ (hence also over $\overline{\mathbb{Q}}$). Observe that I^2 is the endomorphism $(x, y) \mapsto (x, -y)$, which is the endomorphism -1. Consequently $\mathbb{Z}[I] \subset \mathrm{End}_{\overline{\mathbb{Q}}}(E)$. Since we know that $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ is an order, and $\mathbb{Z}[I]$ is the largest order inside $\mathbb{Q}(i)$, we must have $\mathbb{Z}[I] = \mathrm{End}_{\overline{\mathbb{Q}}}(E)$ in this case.

Example 3.25. The elliptic curve $E : y^2 + y = x^3$ has CM by $\mathbb{Z}[\zeta_3]$, via $(x, y) \mapsto (x, \zeta_3 y)$, where ζ_3 is a primitive 3-rd root of unity.

It is insightful to also look what CM elliptic curves look like over $\mathbb{C}$. Over $\mathbb{C}$ we can construct such curves as follows. Suppose that $K/\mathbb{Q}$ is quadratic imaginary and that $R \subset \mathcal{O}_K$ is a subring which is free of rank 2 as $\mathbb{Z}$-module (*i.e.* R is an *order* in K). For instance, we could have $R = \mathcal{O}_K$. Any fractional ideal $I \subset R$ is then also free of rank 2 as $\mathbb{Z}$-module. Moreover $I \subset \mathbb{C}$ is a lattice, since $\mathbb{R} \otimes I$ has an action by $\mathbb{R} \otimes K \cong \mathbb{C}$. Thus $E = \mathbb{C}/I$ is a complex elliptic curve. Any element $r \in R$ maps the fractional ideal I into itself, therefore r acts on $\mathbb{C}/I = E$ and we obtain the mapping $R \to \mathrm{End}_{\mathbb{C}}(E)$. In general $\mathrm{End}_{\mathbb{C}}(E)$ is an order in K too, but it may be larger than R (the multiplier ring of I in K may be larger than R).

Tate module of a CM elliptic curve

Let F be a number field and E an elliptic curve over F and complex multiplications by an order R in the quadratic imaginary field $K \subset \mathbb{C}$. We have two actions on the Tate module

$$\mathrm{Gal}(\overline{F}/F) \circlearrowright V_\ell(E) \circlearrowleft \mathbb{Q}_\ell \otimes \mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Q}_\ell \otimes K.$$

These actions need not commute, but if we assume that the complex multiplications R are defined over F, then the actions do commute. Since $V_\ell(E)$ is a free $K_\ell = \mathbb{Q}_\ell \otimes K$-module of rank 1, the action is given by a continuous morphism $\mathrm{Gal}(\overline{F}/F) \to K_\ell^\times$, and hence comes via class field theory from a continuous morphism

$$\chi_\ell \colon \mathbb{A}_F^\times / \overline{F^\times (F \otimes \mathbb{R})^{\times,+}} \cong \mathrm{Gal}(\overline{F}/F)^{\mathrm{ab}} \to K_\ell^\times, \tag{3.9}$$

uniquely characterized by the property that the morphism χ_ℓ is unramified at the finite F-place $v \nmid \ell$ if and only if E has good reduction at v, in which case

$$\mathrm{Tr}_{K_\ell/\mathbb{Q}_\ell}(\chi_\ell(\varpi_{F_v})) = 1 - \#E(\kappa_v) + q_v \in \mathbb{Z},$$

i.e.

$$\chi_\ell(\varpi_{F_v}) + \overline{\chi_\ell(\varphi_{F_v})} = 1 - \#E(\kappa_v) + q_v \in \mathbb{Z},$$

where $\bar{\cdot}$ denotes the non-trivial automorphism of K.

The Hecke characters we obtained in (3.9) take values in an ℓ-adic field. Observe that in (3.9) the prime number ℓ is arbitrary. More precisely, for every pair of prime numbers (ℓ, ℓ') we have maps

$$\chi_\ell \colon \mathbb{A}_F^\times / \overline{F^\times (F \otimes \mathbb{R})^{\times,+}} \cong \mathrm{Gal}(\overline{F}/F)^{\mathrm{ab}} \to K_\ell^\times$$
$$\chi_{\ell'} \colon \mathbb{A}_F^\times / \overline{F^\times (F \otimes \mathbb{R})^{\times,+}} \cong \mathrm{Gal}(\overline{F}/F)^{\mathrm{ab}} \to K_{\ell'}^\times,$$

such that for all $v \nmid \ell, \ell'$ where E has good reduction, we have that

$$\mathbb{Z}_\ell \ni \chi_\ell(\varpi_{F_v}) + \overline{\chi_\ell(\varphi_{F_v})} = 1 - \#E(\kappa_v) + q_v = \chi_{\ell'}(\varpi_{F_v}) + \overline{\chi_{\ell'}(\varphi_{F_v})} \in \mathbb{Z}_{\ell'}. \tag{3.10}$$

Remark 3.26. By (3.10) we call the family of characters $(\chi_\ell)_{\text{primes } \ell}$ is a *compatible* family of Galois representations. In fact general conjectures predict that, any ℓ-adic Galois representation arising from geometry should fit in such a family. We have seen this for elliptic curves, and again here for the abelian character attached to CM elliptic curves, but it should hold in general for geometric Galois representations. Next week when Peter will discuss étale cohomology, he might say some more about these compatible families of Galois representations.

Apart from characters χ_ℓ for ℓ finite, we will see that it is also possible to attach to E/F an 'infinite' character χ_∞. This χ_ℓ takes values in $\mathbb{C}^\times$. It is however *not* a character of the Galois group $\mathrm{Gal}(\overline{F}/F)^{\mathrm{ab}}$, but of the extension

$$\mathbb{A}_F^\times/F^\times \to \mathbb{A}_F^\times \Big/ \overline{F^\times (F \otimes \mathbb{R})^{\times,+}} \cong \mathrm{Gal}(\overline{F}/F)^{\mathrm{ab}} ,$$

of the Galois group $\mathrm{Gal}(\overline{F}/F)^{\mathrm{ab}}$. (Recall that any continuous morphism from $\mathrm{Gal}(\overline{F}/F)$ to $\mathbb{C}^\times$ must have finite image; in particular $\mathrm{Gal}(\overline{F}/F)$ does not have 'enough' maps to $\mathbb{C}^\times$.)

Algebraic Hecke characters

Let F be a number field. An *algebraic Hecke character* χ is a continuous morphism $\mathbb{A}_F^\times/F^\times \to \mathbb{C}^\times$ such that for each embedding φ of $F \to \mathbb{C}$ and corresponding infinite place $v|\infty$ of F the restriction $\chi|_{F_v^\times}$ is given, on an open subgroup U of $F_v^\times$, by a morphism of the form $U \ni z \mapsto \varphi(z^{a_v})\overline{\varphi}(z^{b_v})$ where $\overline{\varphi}$ is the complex conjugate of φ. If T is the $\mathbb{R}$-torus given by $\mathrm{Res}_{F\otimes\mathbb{R}/\mathbb{R}}\mathbb{G}_{\mathrm{m}}$, the requirement is equivalent to the existence of an algebraic morphism $t\colon T \to \mathrm{Res}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_{\mathrm{m}}$, such that $t(\mathbb{R})|_U = \chi$.

We say that χ is unramified at a finite F-place v if χ_v is trivial on $\mathcal{O}_{F_v}^\times$. In this case $\chi_v(\varpi_{F_v})$ does not depend on the choice of a local uniformizer $\varpi_{F_v} \in F_v$, and we can define the local L-factor at v by $L_v(\chi, s) := (1 - \chi_v(\varpi_{F_v})q_v^{-1})^{-1} \in \mathbb{C}(p^{-s})$. If χ ramifies at v the L-factor is set to be 1. There is also a definition of the L-factors at infinity, but we do not discuss them. The L-function (which is the product over all places of the local L-factors) of these algebraic Hecke characters is known to converge in a right half plane, have analytic continuation and satisfies a functional equation (Tate's thesis).

Theorem 3.27. *Let E/F be an CM elliptic curve with complex multiplications that are defined over F. There exists an algebraic Hecke character $\chi\colon \mathbb{A}_F^\times/F^\times \to \mathbb{C}^\times$ such that for all places v where E is unramified we have*

$$\chi(\varpi_{F_v}) + \overline{\chi(\varpi_{F_v})} = 1 - \#E(\kappa(v)) + \#\kappa(v),$$

where $\kappa(v)$ is the residue field of F at v.

In terms of L-functions, the above means that the L-function of E can be identified as the product of the L-function of χ with the L-function of $\overline{\chi}$. In particular the sought-after analytic properties of $L(E, s)$ follows from those properties of $L(\chi, s)$ (and $L(\overline{\chi}, s)$).

3.5 Étale cohomology

Generally speaking, *homology* and *cohomology* are collective names for certain types of functors from varieties to suitable Abelian categories. The philosophy is that many interesting properties of varieties can be captured in a "linear" way. In our case, we will be interested in the case where the "linear" objects are Galois representations.

Historically, the first example of a (co)homology theory is *singular* (or *Betti*) (co)homology of ordinary topological spaces. This already gives a useful theory for complex algebraic varieties equipped with the complex analytic topology. Later, *sheaf cohomology* was introduced. This also gives a nice theory for coherent sheaves with respect to the Zariski topology, i.e. for algebraic varieties over fields other than $\mathbb{C}$. However, for more advanced applications, one needs various other cohomology theories.

Étale cohomology was initially developed by Grothendieck and Artin to prove the *Weil conjectures* on zeta functions of varieties over finite fields.

Let X be a smooth projective variety over a finite field $k = \mathbb{F}_q$ of q elements. We define a power series $\zeta_X \in \mathbb{Q}[[t]]$ by

$$\zeta_X = \exp\left(\sum_{m=1}^{\infty} \frac{\#E(\mathbb{F}_{q^m})}{m} t^m\right).$$

Theorem 3.28 (Weil conjectures; Dwork, Grothendieck, Deligne)**.** *Let X be a smooth projective variety of dimension n over $\mathbb{F}_q$.*

(i) There exist polynomials $P_0, \ldots, P_{2n} \in \mathbb{Z}[t]$ with constant coefficient 1 such that ζ_X can be written as the rational function

$$\zeta_X = \frac{P_1 P_3 \ldots P_{2n-1}}{P_0 P_2 \ldots P_{2n}}$$

(ii) The rational function ζ_X satisfies

$$\zeta_X\left(\frac{1}{q^n t}\right) = \eta_X t^e \zeta_X(t)$$

for some $e \in \mathbb{Z}$ and $\eta_X \in \mathbb{Q}^\times$.

(iii) The polynomial P_i factors over $\mathbb{C}$ as $\prod_{j=1}^{b_i}(1 - \alpha_{i,j}t)$ where all the $\alpha_{i,j}$ have absolute value $q^{i/2}$.

Example 3.29. In Exercise 3.60, you will show that

$$\zeta_{\mathbb{P}^1_{\mathbb{F}_q}} = \frac{1}{(1-t)(1-qt)}$$

and more generally

$$\zeta_{\mathbb{P}^n_{\mathbb{F}_q}} = \frac{1}{(1-t)(1-qt)\ldots(1-q^n t)}.$$

Basic properties

We first state some of the basic results from étale cohomology from a "black box" point of view, without any proofs.

We fix a base field k with separable closure $\bar{k}$, and a prime number ℓ different from the characteristic of k.

It will be useful to introduce the notations

$$\mathbb{Q}_\ell(1) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \varprojlim_r \mu_{\ell^r}(\bar{k})$$

which is the one-dimensional representation of $\mathrm{Gal}(\bar{k}/k)$ corresponding to the cyclotomic character, and more generally

$$\mathbb{Q}_\ell(n) = \begin{cases} \mathbb{Q}_\ell(1)^{\otimes n} & \text{if } n \geq 0, \\ \mathrm{Hom}(\mathbb{Q}_\ell(1)^{\otimes(-n)}, \mathbb{Q}_\ell) & \text{if } n < 0. \end{cases}$$

If X is a smooth projective variety over a field k and ℓ is a prime number, we have étale cohomology groups

$$\mathrm{H}^i(X_{\bar{k},\text{ét}}, \mathbb{Q}_\ell) \quad (i \in \mathbb{Z}).$$

These groups vanish unless $0 \leq i \leq 2n$, where n is the dimension of X. Each of them is a finite-dimensional $\mathbb{Q}_\ell$-vector space.

The construction gives a contravariant functor from the category of smooth projective varieties over k. This means that given a morphism of smooth projective varieties

$$f\colon X_{\bar{k}} \to Y_{\bar{k}},$$

we have induced $\mathbb{Q}_\ell$-linear maps

$$f^*\colon \mathrm{H}^i(Y_{\bar{k},\text{ét}}, \mathbb{Q}_\ell) \longrightarrow \mathrm{H}^i(X_{\bar{k},\text{ét}}, \mathbb{Q}_\ell).$$

In particular, we can apply this to the automorphisms

$$\sigma^\#\colon X_{\bar{k}} \xrightarrow{\sim} X_{\bar{k}} \quad \text{for } \sigma \in \mathrm{Gal}(\bar{k}/k)$$

obtained by base change from the automorphisms $\sigma^\#\colon \operatorname{spec} \bar{k} \xrightarrow{\sim} \operatorname{spec} \bar{k}$ (note, however, that $\sigma^\#$ is actually not a morphism of varieties over $\bar{k}$, but the construction works anyway). This gives $\mathbb{Q}_\ell$-linear maps

$$\sigma_* = (\sigma^\#)^* \in \mathrm{Aut}_{\mathbb{Q}_\ell} \mathrm{H}^i(X_{\bar{k},\text{ét}}, \mathbb{Q}_\ell).$$

This shows that the étale cohomology groups are equipped with a natural continuous action of $\mathrm{Gal}(\bar{k}/k)$.

If X and Y are two smooth projective varieties over K, there are canonical *Künneth isomorphisms*

$$\mathrm{H}^i((X \times Y)_{\bar{k},\text{ét}}, \mathbb{Q}_\ell) \xrightarrow{\sim} \bigoplus_{a+b=i} \mathrm{H}^a(X_{\bar{k},\text{ét}}, \mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} \mathrm{H}^b(Y_{\bar{k},\text{ét}}, \mathbb{Q}_\ell).$$

Now assume (in addition to the above hypotheses) that X is geometrically connected. Then one has canonical isomorphisms

$$\mathrm{H}^0(X_{\bar{k},\text{ét}}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$$

and

$$\mathrm{H}^{2n}(X_{\bar{k},\text{ét}}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell(-n).$$

Furthermore, one has a canonical *Poincaré duality pairing*

$$\mathrm{H}^i(X_{\bar{k},\text{ét}}, \mathbb{Q}_\ell) \times \mathrm{H}^{2n-i}(X_{\bar{k},\text{ét}}, \mathbb{Q}_\ell) \longrightarrow \mathrm{H}^{2n}(X_{\bar{k},\text{ét}}, \mathbb{Q}_\ell) \xrightarrow{\sim} \mathbb{Q}_\ell(-n).$$

inducing isomorphisms

$$\mathrm{H}^i(X_{\bar{k},\text{ét}}, \mathbb{Q}_\ell) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Q}_\ell}(\mathrm{H}^{2n-i}(X_{\bar{k},\text{ét}}, \mathbb{Q}_\ell), \mathbb{Q}_\ell(-n)),$$
$$\mathrm{H}^{2n-i}(X_{\bar{k},\text{ét}}, \mathbb{Q}_\ell) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Q}_\ell}(\mathrm{H}^{i}(X_{\bar{k},\text{ét}}, \mathbb{Q}_\ell), \mathbb{Q}_\ell(-n)).$$

Now assume that the base field k is a finite field $\mathbb{F}_q$ of cardinality q. For all $i \in \mathbb{Z}$, we define

$$V_i = \mathrm{H}^i(X_{\overline{\mathbb{F}}_q,\text{ét}}, \mathbb{Q}_\ell)$$

and

$$P_i = \det(1 - t \cdot \mathrm{Frob}_q^{-1} \mid V_i)$$

Note that we use the *inverse* of the usual Frobenius automorphism in this definition; this is called the *geometric Frobenius automorphism*. Then Grothendieck showed that the polynomials P_i are the polynomials occurring in Theorem 3.28. In particular, the P_i are independent of the choice of ℓ.

In the following sections, we will try to explain in a nutshell how one defines these étale cohomology groups for a variety X over a field k. The objects from which one constructs étale cohomology groups of X are *sheaves of Abelian groups for the étale topology on X*.

Étale morphisms

Let $f\colon U \to X$ be a morphism of varieties. We say that f is *étale* if f is smooth of relative dimension 0. (There are various other definitions, but this one is the most intuitive.) The simplest examples of étale morphisms are open immersions.

Example 3.30. Let k be a field, let X be the affine line over k, and let U be the affine variety defined by $P(x, y) = 0$ with $P \in k[x, y]$ having positive degree in y. Let $B = k[x, y]/(P)$, and let $f\colon U \to X$ be the obvious map corresponding to the ring homomorphism $k[x] \to B$ given by $x \mapsto x$. Then the module of relative differentials for $U \to X$ is

$$\begin{aligned}\Omega_{U/X}(U) &= \Omega_{B/k[x]} \\ &= \frac{B\,dy}{\frac{\partial P}{\partial y} B\,dy}\end{aligned}$$

This means that f is étale on the open subset of U where $\frac{\partial P}{\partial y}$ is invertible. To give a concrete example, if $P = x - y^n$ with n not divisible by the characteristic of k, then there is a natural isomorphism $k[y] \xrightarrow{\sim} B$, inducing an isomorphism

$$k[y]/(ny^{n-1}) \xrightarrow{\sim} \Omega_{U/X}(U).$$

This means that f is étale over the open subset $x \neq 0$ of X.

Étale sheaves

If X is a variety, we write $X_{\text{ét}}$ for the category whose objects are étale morphisms $f\colon U \to X$, and where the morphisms between two objects $f\colon U \to X$ and $g\colon V \to X$ are the morphisms of varieties $h\colon U \to V$ such that $f = g \circ h$. It is known that such an h is automatically étale itself; see Exercise 3.63.

For any variety Y, an *étale covering* of Y is a family of étale morphisms $\{f_i\colon U_i \to Y\}_{i\in I}$ satisfying $\bigcup_{i\in I} \operatorname{im}(f_i) = Y$.

Definition 3.31. A *presheaf (of Abelian groups) for the étale topology on* X is a contravariant functor

$$\mathcal{F}\colon X_{\text{ét}} \to \mathbf{Ab}$$

from $X_{\text{ét}}$ to the category of Abelian groups. We say that $\mathcal{F}$ is a *sheaf* if it satisfies the following glueing condition: for every étale morphism $U \to Y$ and every étale covering $\{f_i\colon U_i \to U\}$ of U, the sequence

$$0 \longrightarrow \mathcal{F}(U) \xrightarrow{(f_i^*)_{i\in I}} \prod_{i\in I} \mathcal{F}(U_i) \xrightarrow{g} \prod_{i,j\in I} \mathcal{F}(U_{i,j})$$

is exact. Here $U_{i,j}$ is the fibre product $U_i \times_U U_j$, and the morphism g is defined by

$$g((s_i)_{i\in I} = (p_{i,j}^* s_i - q_{i,j}^* s_j)_{i,j\in I},$$

where $p_{i,j}\colon U_{i,j} \to U_i$ and $q_{i,j}\colon U_{i,j} \to U_j$ are the projections onto the first and second coordinates.

Example 3.32. Let A be an Abelian group. For every variety U, let $A(U)$ be the group of continuous (*i.e.* locally constant) functions $U \to A$, where U has the Zariski topology and A the discrete topology. Then for every variety X, the functor $(U \to X) \longmapsto A(U)$ is a sheaf for the étale topology on X (the proof is left as an exercise). This sheaf is called the *constant sheaf* A_X.

Example 3.33. For every variety U, let $\mathbb{G}_{\text{m}}(U)$ be the group $\mathcal{O}_U(U)^\times$ of invertible regular functions on U. Then for every variety X, the functor $(U \to X) \longmapsto \mathbb{G}_{\text{m}}(U)$ is a sheaf for the étale topology on X. This sheaf is called the *multiplicative group* over X and is denoted by $\mathbb{G}_{\text{m},X}$.

Remark 3.34. The sheaves A_X and $\mathbb{G}_{\text{m},X}$ in the above examples can also be viewed as varieties over X (except that A_X is only of finite type over X if A is finite or X is empty). For our purposes this is not important, however.

Construction of étale cohomology

Let $\mathbf{Ab}(X_{\text{ét}})$ denote the category of sheaves of Abelian groups for the étale topology on X. It turns out that this is an Abelian category with enough injectives. This means that starting from the global sections functor

$$\Gamma(X_{\text{ét}}, \bullet)\colon \mathbf{Ab}(X_{\text{ét}}) \to \mathbf{Ab}$$

we obtain a sequence of right derived functors

$$\mathrm{H}^i(X_{\text{ét}}, \bullet)\colon \mathbf{Ab}(X_{\text{ét}}) \to \mathbf{Ab} \quad (i \in \mathbb{Z}).$$

For technical reasons, one does not get the correct results when one directly applies the definition to the sheaf $\mathbb{Q}_\ell$. Therefore, instead of considering $\mathbb{Q}_\ell$ as a sheaf on $X_{\bar{k},\text{ét}}$, one defines

$$\mathrm{H}^i(X_{\bar{k},\text{ét}}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \varprojlim_r \mathrm{H}^i(X_{\bar{k},\text{ét}}, \mathbb{Z}/\ell^r\mathbb{Z}).$$

Étale cohomology of a curve

Let C be a smooth, projective, connected curve over an algebraically closed field k. Let $j\colon \{\eta\} \to C$ be the inclusion of the generic point, and for each closed point $x \in C$ let $i_x\colon \{x\} \to C$ be the inclusion. We have push-forward sheaves $j_*\mathbb{G}_{\mathrm{m},\eta}$ and $i_{x,*}\mathbb{Z}_{\{x\}}$ for all closed points $x \in C$, fitting in a short exact sequence of sheaves of Abelian groups on $C_{\text{ét}}$:

$$1 \longrightarrow \mathbb{G}_{\mathrm{m},C} \longrightarrow j_*\mathbb{G}_{\mathrm{m},\eta} \xrightarrow{\text{div}} \bigoplus_{x\in C} i_{x,*}\mathbb{Z}_{\{x\}} \longrightarrow 0.$$

Taking the long exact cohomology sequence and doing various computations gives the following canonical isomorphisms:

$$\mathrm{H}^i(C, \mathbb{G}_\mathrm{m}) \cong \begin{cases} k^\times & \text{if } i = 0, \\ \operatorname{Pic} C & \text{if } i = 1, \\ 0 & \text{otherwise.} \end{cases}$$

The above example is more or less the only one in which one directly takes étale cohomology with coefficients in a non-torsion sheaf. In most other cases, étale cohomology is only well-behaved when one takes torsion coefficients. For every positive integer n that is not divisible by the characteristic of k, we consider the short exact sequence

$$1 \longrightarrow \mu_n \longrightarrow \mathbb{G}_\mathrm{m} \xrightarrow{n} \mathbb{G}_\mathrm{m} \longrightarrow 1$$

Taking étale cohomology gives a long exact sequence, which splits into

$$1 \longrightarrow \mu_n(k) \longrightarrow k^\times \longrightarrow k^\times \longrightarrow 1$$

$$1 \longrightarrow \mathrm{H}^1(C, \mu_n) \longrightarrow \operatorname{Pic} C \xrightarrow{n} \operatorname{Pic} C \longrightarrow \mathrm{H}^2(C, \mu_n) \longrightarrow 1.$$

From this we obtain canonical isomorphisms

$$\mathrm{H}^i(C, \mu_n) \cong \begin{cases} \mu_n(k) & \text{if } i = 0, \\ (\operatorname{Pic} C)[n] & \text{if } i = 1, \\ \mathbb{Z}/n\mathbb{Z} & \text{if } i = 2, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, choosing a prime number ℓ different from the characteristic of k and taking a direct limit over $n = \ell^r$ gives

$$\begin{aligned} \mathrm{H}^i(C, \mathbb{Q}_\ell(1)) &= \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \varprojlim_r \mathrm{H}^i(C, \mu_{\ell^r}) \\ &\cong \begin{cases} \mathbb{Q}_\ell(1) & \text{if } i = 0, \\ V_\ell(J) & \text{if } i = 1, \\ \mathbb{Q}_\ell & \text{if } i = 2, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Here J is the Jacobian variety of C; this is a g-dimensional Abelian variety over k, where g is the genus of C. The latter implies that $\dim_{\mathbb{Q}_\ell} \mathrm{H}^1(C, \mathbb{Q}_\ell(1)) = 2g$. If you don't know what the Jacobian variety is, you can take

$$V_\ell(J) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \varprojlim_r (\mathrm{Pic}\, C)[\ell^r]$$

as a definition.

Comparison theorem

The following fundamental theorem shows that étale cohomology gives "the same" results as ordinary (singular) cohomology for smooth projective complex varieties.

Theorem 3.35 (Comparison between singular and étale cohomology)**.** *Let X be a smooth projective variety over $\mathbb{C}$, let X_{an} be the corresponding compact complex manifold $X(\mathbb{C})$, viewed as a topological space with the analytic topology, and let ℓ be a prime number. Then there are canonical isomorphisms*

$$\mathrm{H}^i(X_{\text{ét}}, \mathbb{Z}/\ell^r\mathbb{Z}) \xrightarrow{\sim} \mathrm{H}^i(X_{\mathrm{an}}, \mathbb{Z}/\ell^r\mathbb{Z}) \quad \textit{for all } r \geq 0,$$

and hence

$$\mathrm{H}^i(X_{\text{ét}}, \mathbb{Q}_\ell) \xrightarrow{\sim} \mathbb{Q}_\ell \otimes_{\mathbb{Z}} \mathrm{H}^i(X_{\mathrm{an}}, \mathbb{Z}).$$

Galois representations

We now turn to the case where the base field is $\mathbb{Q}$ or $\mathbb{Q}_p$ (although everything generalises to number fields and their completions).

Theorem 3.36. *Let p be a prime number, let X be a smooth projective variety over $\mathbb{Q}_p$, and let ℓ be a prime number different from p. If X has good reduction at p, then for all $i \in \mathbb{Z}$, the finite-dimensional $\mathbb{Q}_\ell$-linear representation $H^i(X_{\overline{\mathbb{Q}}_p,\text{ét}}, \mathbb{Q}_\ell)$ of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is unramified.*

Corollary 3.37. *Let X be a smooth projective variety over $\mathbb{Q}$, and let ℓ be a prime number. Then for every prime number $p \neq \ell$ such that X has good reduction at p, the finite-dimensional $\mathbb{Q}_\ell$-linear representation $H^i(X_{\overline{\mathbb{Q}},\text{ét}}, \mathbb{Q}_\ell)$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is unramified at p.*

Equivalently, let N be a positive integer such that X admits a smooth projective model over $\mathbb{Z}[1/N]$. Then for all $i \in \mathbb{Z}$, the finite-dimensional $\mathbb{Q}_\ell$-linear representation $H^i(X_{\overline{\mathbb{Q}},\text{ét}}, \mathbb{Q}_\ell)$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is unramified outside $N\ell$.

We now fix a smooth projective variety X over $\mathbb{Q}$ and an integer i, and we consider the family of ℓ-adic Galois representations

$$V_\ell = \mathrm{H}^i(X_{\overline{\mathbb{Q}},\text{ét}}, \mathbb{Q}_\ell)$$

where ℓ runs over all prime numbers.

By the above results, for each prime number p, the characteristic polynomial of Frob_p on V_ℓ, which a priori has coefficients in $\mathbb{Q}_\ell$, actually has coefficients in $\mathbb{Z}$ and is independent of the choice of ℓ.

Definition 3.38. A *compatible family of ℓ-adic representations* of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a family

$$\{\rho_\ell \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{Q}_\ell} V_\ell\}_\ell$$

where V_ℓ is a finite-dimensional $\mathbb{Q}_\ell$-vector space and ρ_ℓ is a continuous representation, with the following property. There exists a finite set S of primes such that for all primes $p \notin S$ the following compatibility condition holds: for all primes $\ell \neq p$ the representation V_ℓ is unramified at p, and the characteristic polynomial of Frob_p on V_ℓ has coefficients in $\mathbb{Z}$ and is independent of ℓ.

3.6 Weil–Deligne representations

In this section, F denotes a p-adic field.

Morally speaking, the local Langlands programme links n-dimensional representations of the Galois group of F with admissible representations of $\mathrm{GL}_n(F)$. Due to the fact that we are interested in *complex* representations, it is extremely useful to formulate the Galois side of the Langlands correspondence not in terms of the Galois group, but in terms of the closely related *Weil group*.

A classical reference for Weil groups and their properties is Tate [18]. We also refer to Bushnell and Henniart [3, Chapter 7].

The Weil group

Recall that the absolute Galois group $G_F = \mathrm{Gal}(\bar{F}/F)$ fits in a short exact sequence

$$1 \longrightarrow I_F \longrightarrow G_F \longrightarrow \widehat{\mathbb{Z}} \longrightarrow 1,$$

where the map $G_F \to \widehat{\mathbb{Z}}$ sends a Frobenius element to 1.

Definition 3.39. The *Weil group* of F is the subgroup $W_F \subset G_F$ consisting of all elements whose image in $\widehat{\mathbb{Z}}$ lies in $\mathbb{Z}$. It is equipped with the coarsest topology making G_F into a topological group containing I_F as an open subgroup with the subspace topology from G_F.

Remark 3.40. Besides Weil groups (named after André Weil), there also exist *Weyl groups* (named after Hermann Weyl). Other than the fact that they both play a role in the context of the Langlands programme, these groups are not related to each other.

Thus we have a short exact sequence

$$1 \longrightarrow I_F \longrightarrow W_F \longrightarrow \mathbb{Z} \longrightarrow 1.$$

The reciprocity map from local class field theory (2.7) restricts to an isomorphism

$$\mathrm{rec}_F \colon F^\times \xrightarrow{\sim} W_F^{\mathrm{ab}}$$

of topological groups. Conversely, the isomorphism (2.7) can be obtained from the above isomorphism by taking the profinite completion on both sides.

There are two natural normalisations of the above isomorphism. We choose the one such that the image of a uniformiser $\varpi_F \in F^\times$ in W_F^{ab} is a *geometric* Frobenius element

(inducing the *inverse* of the q-th power map on the residue field of $\bar{F}$). We define a group homomorphism

$$\begin{aligned} \|\cdot\|_F \colon W_F &\longrightarrow q^{\mathbb{Z}} \subset \mathbb{Q}^\times \\ w &\longmapsto |\mathrm{rec}_F^{-1}(w)|_F. \end{aligned}$$

With this definition, the geometric Frobenius elements $\phi \in W_F$ satisfy $\|\phi\|_F = q^{-1}$, and more generally every element $w \in W_F$ acts on the residue field of $\bar{F}$ as $x \mapsto x^{\|w\|_F}$.

Grothendieck's monodromy theorem on ℓ-adic representations

In practice, many interesting representations of W_F that one encounters are continuous ℓ-adic representations, which are not necessarily smooth (*i.e.* locally constant). It turns out that the ℓ-adic representations of W_F can be transformed into *Weil–Deligne representations*. These have a purely algebraic definition (*i.e.* independent of the topology of the field of coefficients), to be given below.

We recall that the tame inertia group of F (the quotient of I_F by its maximal pro-p subgroup, the wild inertia group) is canonically isomorphic to $\prod_{\ell \neq p} \mathbb{Z}_\ell(1)$, where ℓ runs over all prime numbers different from p.

Let ℓ be a prime number different from p. By the above result, we can choose a surjective group homomorphism

$$t_\ell \colon I_F \to \mathbb{Z}_\ell.$$

This is unique up to multiplication by an element of $\mathbb{Z}_\ell^\times$, and one can show (Exercise 3.71) that t_ℓ satisfies

$$t_\ell(wxw^{-1}) = \|w\|_F t_\ell(x) \quad \text{for all } x \in I_F, w \in W_F. \tag{3.11}$$

Theorem 3.41 (Grothendieck)**.** *Let V be a finite-dimensional $\overline{\mathbb{Q}}_\ell$-vector space, and let $\sigma \colon W_F \to \mathrm{Aut}_{\overline{\mathbb{Q}}_\ell} V$ be a continuous representation of W_F. Then there exists an open subgroup $H \subseteq I_F$ such that $\sigma|_H$ is unipotent (i.e. for any $h \in H$, the matrix $\sigma(h)$ has all its eigenvalues equal to 1).*

For the next corollary, we note that if N is a nilpotent matrix over a field of characteristic 0, then $\exp(N) = \sum_{r=0}^{\infty} N^r/r!$ is well-defined since the sum is finite, and $exp(N)$ is unipotent. Conversely, if U is a unipotent matrix, then $I - U$ is nilpotent, and we can define $\log(U) = -\sum_{r=1}^{\infty} (I-U)^r/r$. These operations are mutually inverse.

Corollary 3.42. *With the above notation, there exists a unique nilpotent endomorphism $N \in \mathrm{End}_{\overline{\mathbb{Q}}_\ell} V$ such that all h in a sufficiently small open subgroup of I_F satisfy*

$$\sigma(h) = \exp(t_\ell(h)N).$$

Proof. Let H be as in the above theorem. Because H has finite index in I_F, there exists $h_0 \in H$ such that the element $t_\ell(h_0) \in \mathbb{Z}_\ell$ is non-zero. It is clear that the only choice is

$$N = t_\ell(h_0)^{-1} \log(\sigma(h_0)).$$

We have to show that the claim holds with this choice of N.

After shrinking H if necessary, the representation $\sigma|_H$ factors through t_ℓ ("only the pro-ℓ part can have infinite image"), *i.e.* there exists a continuous homomorphism $\phi \colon t_\ell(H) \to$

$\mathrm{Aut}_{\overline{\mathbb{Q}}_\ell} V$ such that $\sigma(h) = \phi(t_\ell(h))$ for all $h \in H$. The two homomorphisms $t_\ell(H) \to \mathrm{Aut}_{\overline{\mathbb{Q}}_\ell} V$ mapping x to $\phi(x)$ and $\exp(xN)$, respectively, agree on the element $t_\ell(h_0)$ and hence on the closed subgroup of $t_\ell(H)$ generated by $t_\ell(h_0)$, which is also open in $t_\ell(H)$. It follows that the homomorphisms $H \to \mathrm{Aut}_{\overline{\mathbb{Q}}_\ell} V$ mapping h to $\sigma(h)$ and $\exp(t_\ell(h)N)$, respectively, agree on an open subgroup of H, which is what we had to prove. □

Weil–Deligne representations

Definition 3.43. Let E be a field of characteristic 0. A *Weil–Deligne representation* of F is a triple (ρ, V, N) where V is a finite-dimensional E-vector space, $\rho\colon W_F \to \mathrm{Aut}_E(V)$ is a smooth (*i.e.* locally constant) representation, and $N \in \mathrm{End}_E(V)$ is a nilpotent endomorphism (*i.e.* there exists $n \geq 1$ such that $N^n = 0$) satisfying the compatibility relation

$$\rho(w) N \rho(w)^{-1} = \|w\|_F N \in \mathrm{End}_E(V) \quad \text{for all } w \in W_F.$$

Let $\sigma\colon W_F \to \mathrm{Aut}_{\overline{\mathbb{Q}}_\ell} V$ be a continuous representation. We choose a geometric Frobenius element

$$\phi \in W_F$$

(*i.e.* an element inducing the *inverse* of the q-th power map on the residue field of $\bar{F}$). Let N be the nilpotent endomorphism of V given by Corollary 3.42. We define a smooth representation ρ_σ of W_F by

$$\rho_\sigma(\phi^a h) = \sigma(\phi^a h) \exp(-t_\ell(h) N) \quad \text{for all } a \in \mathbb{Z}, h \in I_F.$$

Theorem 3.44. *With the above notation, (ρ_σ, V, N) is a Weil–Deligne representation of W_F that (up to isomorphism) is independent of the choice of ϕ and t_ℓ. This construction defines an equivalence of categories from the category of continuous finite-dimensional $\overline{\mathbb{Q}}_\ell$-linear representations of W_F to the category of Weil–Deligne representations of F.*

3.7 Exercises

In the exercises below, unless otherwise mentioned F is a number field, $\overline{F}$ is an algebraic closure and ℓ is a prime number.

Exercise 3.1. Let G be a group and C a field. Show that for any finite-dimensional G-representation V there exists a filtration of V by G-stable subspaces $0 = V_0 \subset V_1 \subset \cdots \subset V_m = V$ such that for all i the quotient V_i/V_{i+1} is semi-simple. Moreover show that this filtration can be defined in such a way that it depends functorially on V.

Exercise 3.2. Prove Theorem 3.9.

Exercise 3.3. Let V be a finite-dimensional complex representation of $\mathrm{Gal}(\overline{F}/F)$. Show that the mapping $\mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_{\mathbb{C}}(V)$ is continuous if and only if the mapping $\mathrm{Gal}(\overline{F}/F) \times V \to V$, $(\sigma, x) \mapsto \sigma x$ is continuous. Does this result also hold for representations in finite-dimensional vector spaces over $\overline{\mathbb{Q}}_\ell$?

Exercise 3.4. Let G be a finite group. Let S be the set of all isomorphism classes of irreducible complex representations of G. Pick for each $s \in S$ a V_s that represents the elements in the isomorphism class s. Show that for all $g \in G$ we have

$$\sum_{s \in S} \dim(V_s) \cdot \mathrm{Tr}(g, V_s) = \begin{cases} \#G & g = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Exercise 3.5. Show by counter example that Proposition 3.17 becomes false if the condition "semi-simple" is removed from the statement.

Exercise 3.6. Let F be a number field and v a place of F. Choose an algebraic closure $\overline{F}$ of F and choose an algebraic closure $\overline{F}_v$ of F_v.

(a) Show that there exist an F-morphism $\iota_v \colon \overline{F} \to \overline{F}_v$.

(b) Deduce that there exists a natural injection $\iota_v^* \colon \mathrm{Gal}(\overline{F}_v/F_v) \to \mathrm{Gal}(\overline{F}/F)$.

(c) Show that if ι_v' is another choice of embedding of F_v into $\overline{F}_v$, then there exists an element $\sigma \in \mathrm{Gal}(\overline{F}/F)$ such that $\iota_v^* = \sigma \circ \iota_v'^* \circ \sigma^{-1}$.

(d) Deduce that if V is a Galois representation of a number field F then the local representation $V|_{\mathrm{Gal}(\overline{F}_v/F_v)}$ is well-defined up to isomorphism.

(e) Show that if $V/\mathbb{C}$ is an Artin representation of $\mathrm{Gal}(\overline{F}/F)$ then V is unramified for almost all finite F-places v.

Exercise 3.7. Let F be a number field, let v be a finite F-place and fix an algebraic closure $\overline{F}_v$ of F_v. Show that to give an $\overline{F}$-place w above v is to give a $\mathrm{Gal}(\overline{F}_v/F_v)$-conjugacy class in $\mathrm{Hom}_F(\overline{F}, \overline{F}_v)$.

Exercise 3.7$\frac{1}{2}$. Let $O(n)$ be the group of real orthogonal matrices $g \in \mathrm{GL}_n(\mathbb{R})$ such that $g^t g = 1$. Let G be a finite group. Show that any representation $r \colon G \to \mathrm{GL}_n(\mathbb{R})$ of G on the vector space $\mathbb{R}^n$ is $\mathrm{GL}_n(\mathbb{R})$-conjugate to a morphism $G \to O(n)$.

Exercise 3.8. Let V be a Galois representation of a number field F in a vector space V over a closed subfield C of $\mathbb{C}$, $\overline{\mathbb{Q}}_\ell$, or $\overline{\mathbb{Q}}$. Let v be a finite F-place where V is unramified. Show that the element $\rho(\mathrm{Frob}_v) \in \mathrm{GL}_C(V)$ is well-defined up to conjugation.

Exercise 3.9. Does there exist a group G and a non-trivial representation V of G such that V contains no irreducible subrepresentation?

Exercise 3.10. Does there exist an irreducible 2-dimensional Galois representation $V/\mathbb{Q}_\ell$ of $\mathrm{Gal}(\overline{F}/F)$ such that $V \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ is reducible?

Exercise 3.11. Let F be a field of characteristic $p > 0$. Give an example of a finite group G such that $p | \#G$ and a 2-dimensional representation V/F of G that is not semi-simple.

Exercise 3.12. Does there exist a continuous representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in a two-dimensional $\mathbb{Q}_\ell$-vector space that is ramified at infinitely many prime numbers?

Exercise 3.13. In this exercise F is a local p-adic field. Let V_1 and V_2 be two continuous representations of $\mathrm{Gal}(\overline{F}/F)$ in finite-dimensional complex vector spaces. Use Formula 3.4 to express the conductor exponent $n_{V_1 \oplus V_2}$ of $V_1 \oplus V_2$ in terms of the conductor exponents n_{V_1} and n_{V_2} of V_1 and V_2.

Exercise 3.14. Let $V/\overline{\mathbb{Q}}_\ell$ be an ℓ-adic representation of the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$ of some number field F. Assume that $V \cong V \otimes \chi$ for some non-trivial character $\chi\colon \mathrm{Gal}(\overline{F}/F) \to \overline{\mathbb{Q}}_\ell^\times$ with finite image. Show that the representation V is reducible when restricted to an open subgroup of $\mathrm{Gal}(\overline{F}/F)$.

Exercise 3.15. Let K be the splitting field of the polynomial $f = x^3 - x - 1$ considered in Example 1.19, and let V be the Artin representation considered in that example. Compute the conductor exponent $n_{V,23}$.

Exercise 3.16. Show that the field $\overline{\mathbb{Q}}_\ell$ is not complete for the norm $|\cdot|$.

Exercise 3.17. Let V be an ℓ-adic representation of the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$ of some number field F. Show that there exists a finite extension $L/\mathbb{Q}_\ell$ such that $\mathrm{Tr}\,\rho_V(\sigma) \in \mathcal{O}_L$ for all $\sigma \in \mathrm{Gal}(\overline{F}/F)$.

Exercise 3.18. Let χ_ℓ be the cyclotomic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let p be a prime number different from ℓ. Compute $L_p^\iota(\chi, s)$ for some choice of isomorphism $\iota\colon \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$. General conjectures predict that for "nice Galois representations" (*i.e.* those that come from geometry), the Galois representations should come in families where ℓ ranges over all prime numbers. Using this, explain (without proving) what the natural definition of the factor $L_\ell(\chi, v)$ at the prime ℓ of χ_ℓ should be.

Exercise 3.19. Let $V/\overline{\mathbb{Q}}_\ell$ be an ℓ-adic representation of $\mathrm{Gal}(\overline{F}/F)$, which is not necessarily a Galois representation. Show that for almost all finite F-places v the wild inertia group $I(\overline{F}_v/F_v)^{\mathrm{wild}}$ acts trivially on V.

Exercise 3.20. Show that there exists an isomorphism of fields $\iota\colon \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$. Explain that such an isomorphism is "very far" from continuous, and that the number of such ι is uncountably infinite. Are there continuous isomorphisms $\iota\colon \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \overline{\mathbb{Q}}_{\ell'}$ if ℓ' is a prime different from ℓ?

Exercise 3.21. Let V be an Artin representation of $\mathrm{Gal}(\overline{F}/F)$. Let σ be a not necessarily continuous field automorphism of $\mathbb{C}$. Show that $V_\sigma := V \otimes_{\mathbb{C},\sigma} \mathbb{C}$ is another Artin representation of $\mathrm{Gal}(\overline{F}/F)$. Show that the Euler factors at the finite places of V_σ are conjugate to the Euler factors of V.

Exercise 3.22. Let $V/\overline{\mathbb{Q}}_\ell$ be a semi-simple Galois representation of $\mathrm{Gal}(\overline{F}/F)$, such that for all most all finite F-places v where r is unramified, the characteristic polynomial of $r(\mathrm{Frob}_v)$ has coefficients in $\overline{\mathbb{Q}}$. Let ℓ' be a prime number different from ℓ. Let $\iota\colon \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \overline{\mathbb{Q}}_{\ell'}$ be an isomorphism of fields (non-continuous).

(a) Show that there exists at most one semi-simple ℓ'-adic Galois representation (r', V') over $\overline{\mathbb{Q}}_{\ell'}$ of $\mathrm{Gal}(\overline{F}/F)$ such that for all most all finite F-places v where r and r' are unramified $\iota\mathrm{charpol}(r(\mathrm{Frob}_v))$ equals $\mathrm{charpol}(r'(\mathrm{Frob}_v))$ in $\overline{\mathbb{Q}}[X]$.

(b) Give an example of a triple (ℓ, ℓ, r') where ℓ, ℓ' are prime numbers, $(r, V)/\overline{\mathbb{Q}}_\ell$ is a Galois representation such that for any choice of $\iota\colon \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \overline{\mathbb{Q}}'_\ell$ there does not exist a Galois representation $(r', V')/\overline{\mathbb{Q}}_{\ell'}$ such that r and r' have almost everywhere matching characteristic polynomials (via ι, as in part (a)).

Exercise 3.23. Let L/F be a finite Galois extension of number fields with $L \subset \overline{F}$. Consider the 1-dimensional representation $\mathbf{1}$ of $\mathrm{Gal}(\overline{F}/L)$ with space $\mathbb{C}$ and trivial Galois action. Express the L-function of the Galois representation $\mathrm{Ind}_{\mathrm{Gal}(\overline{F}/L)}^{\mathrm{Gal}(\overline{F}/F)}(\mathbf{1})$ in terms of the Dedekind zeta functions of L and F.

Exercise 3.24. Let $E/\mathbb{Q}$ be a quadratic extension of $\mathbb{Q}$. Let $\chi\colon \mathrm{Gal}(\overline{E}/E) \to \mathbb{C}^\times$ be a non-trivial continuous morphism. Let (r, V) be the induced representation $\mathrm{Ind}_{\mathrm{Gal}(\overline{E}/E)}^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}(\chi)$. Let p be a prime number that is unramified in E and such that χ is unramified at the E-places above p. Determine the characteristic polynomial of $r(\mathrm{Frob}_p)$.

Exercise 3.25. Let $r\colon \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ be a Galois representation, and let $H_r \subset \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ be the Zariski closure of the image of r.

(a) Show that H_r is a group.

(b) Give an example of a representation r as above such that $H_r = \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ for some $n \geq 2$.

(c) Give an example of an irreducible Galois representation r such that H_r is non-connected (for the Zariski topology) and infinite.

Exercise 3.26. Let $r\colon \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ be a Galois representation. Show that there exists a finite extension $E \subset \overline{F}$ of F such that for any finite extension $L \subset \overline{F}$ of F that is linearly disjoint from E, the groups $\mathrm{Gal}(\overline{F}/F)$ and $\mathrm{Gal}(\overline{F}/E)$ have the same Zariski closure in $\mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$.

Exercise 3.27. (Place holder)

Exercise 3.28. Let r_1, r_2 be two semi-simple n-dimensional ℓ-adic Galois representations of $\mathrm{Gal}(\overline{F}/F)$, both unramified outside a finite set of F-places S. Assume that there exists an integer $k \in \mathbb{Z}_{\geq 1}$ such that $\mathrm{Tr}\, r_1(\mathrm{Frob}_v^j) = \mathrm{Tr}\, r_2(\mathrm{Frob}_v^j)$ for all integers $j \geq k$. Show that r_1 and r_2 are isomorphic.

Exercise 3.29. Let $V/\overline{\mathbb{Q}}_\ell$ be an ℓ-adic Galois representation of the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$ of some number field F where V is a finite-dimensional $\overline{\mathbb{Q}}_\ell$-vector space. Let $\Lambda \subset V$ be a stable lattice (cf. Exercise 2.10). Show that the representation of $\mathrm{Gal}(\overline{F}/F)$ on $\Lambda \otimes \mathbb{F}_\ell$ is irreducible if and only if the only Galois stable lattices in V are the lattices of the form $\ell^n \Lambda$ for $n \in \mathbb{Z}$.

Exercise 3.30. Let $V_1, V_2/\overline{\mathbb{Q}}_\ell$ be two Galois representations of $\mathrm{Gal}(\overline{F}/F)$ and $H \subset \mathrm{Gal}(\overline{F}/F)$ a normal open subgroup. Show that the space $\mathrm{Hom}_{\overline{\mathbb{Q}}_\ell[H]}(V_1, V_2)$ of vector space morphisms has a natural structure of an Artin representation of $\mathrm{Gal}(\overline{F}/F)$.

Exercise 3.31. Let F be a number field. Let $\rho\colon \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ be a Galois representation such that its restriction $\rho|_{\mathrm{Gal}(\overline{F}/L)}$ is irreducible for all extensions L of F contained in $\overline{F}$. Let $\rho'\colon \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ be another Galois representation of dimension n such that for almost all places v of F where ρ and ρ' are unramified we have $\mathrm{Tr}(\rho(\mathrm{Frob}_v)) = \pm \mathrm{Tr}(\rho'(\mathrm{Frob}_v))$ for some sign $\pm$ (that may depend on v).

(a) Show that there exists a finite extension L/F such that $\rho|_{\mathrm{Gal}(\overline{F}/L)} \cong \rho'|_{\mathrm{Gal}(\overline{F}/L)}$.

(b) Show that $\rho \cong \rho' \otimes \chi$ where $\chi\colon \mathrm{Gal}(\overline{F}/F) \to \{\pm 1\}$ is a quadratic character.

Exercise 3.32. Let $T = \mathrm{Tr}\, r$ be the trace mapping $\mathrm{Gal}(\overline{F}/F) \to \mathbb{Z}_\ell$ attached to a Galois representation $(r, V)/\mathbb{Q}_\ell$ of $\mathrm{Gal}(\overline{F}/F)$. Show that there are infinitely many F-places v such that $T(\mathrm{Frob}_v) \equiv \dim(V) \mod \ell$ and give a lower bound for the density of such v.

Exercise 3.33. Let $(r, V)/\overline{\mathbb{Q}}_\ell$ be a semi-simple ℓ-adic Galois representation of $\mathrm{Gal}(\overline{F}/F)$ and $(r', V')/\overline{\mathbb{Q}}_{\ell'}$ be a semi-simple ℓ'-adic Galois representation of $\mathrm{Gal}(\overline{F}/F)$. We assume that for almost all finite F-places v where r and r' are unramified the characteristic polynomials match (with respect to some fixed $\iota\colon \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \overline{\mathbb{Q}}_{\ell'}$, cf. Exercise 3.18). Show that the image of r is finite if and only if the image of r' is finite.

Exercise 3.34. Consider a continuous morphism $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)/\{\pm 1\}$ that is unramified almost everywhere. In this exercise we investigate the question when ρ lifts to a continuous representation $\widetilde{\rho}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$, such that $\widetilde{\rho}(\sigma) \equiv \rho(\sigma) \in \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)/\{\pm 1\}$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

(a) Show that there exists a map of topological spaces $r\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ such that $r(\sigma) \equiv \rho(\sigma) \in \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)/\{\pm 1\}$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

(b) Show that $(\sigma, \sigma') \mapsto c_{\sigma,\sigma'} = r(\sigma)r(\sigma')^{-1}$ defines a continuous 2-cocyle of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with values in $\{\pm 1\}$.

(c) Show that $\widetilde{\rho}$ exists if and only if the 2-cocycle c is cohomologous to the trivial 2-cocycle $(\sigma, \sigma') \mapsto 1$.

Exercise 3.35. Let (ρ, V) be a semi-simple ℓ-adic Galois representation of $\mathrm{Gal}(\overline{F}/F)$ such that its image contains a regular unipotent element N of $\mathrm{GL}_{\overline{\mathbb{Q}}_\ell}(V)$. Show that V is irreducible. (A *unipotent element* N of $\mathrm{GL}_{\overline{\mathbb{Q}}_\ell}(V)$ is a matrix such that $N - 1 \in \mathrm{End}_{\overline{\mathbb{Q}}_\ell}(V)$ is nilpotent; N is *regular unipotent* if furthermore $(N-1)^{\dim(V)-1} \neq 0$.)

Exercise 3.36. Let p be a prime number and $q \in {\mathbb{Q}_p}^\times$ with $|q| < 1$. Consider the group $\overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}}$ as a module of $\mathbb{Z}[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)]$. Let ℓ be a prime number different from p, and consider the module $\Lambda = \varprojlim \overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}}[\ell^n]$ where the limit ranges over $n \in \mathbb{Z}_{\geq 1}$. Compute the space of $I(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-invariants (resp. $I(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-coinvariants) $\Lambda^{I(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$ (resp. $\Lambda_{I(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$) of Λ.

Exercise 3.37. Let K be the splitting field of $x^3 - x - 1 \in \mathbb{Q}[x]$ as in Example 1.19, and put $F = \mathbb{Q}(\sqrt{-23})$, viewed as a subfield of K. Let $G = \mathrm{Gal}(K/\mathbb{Q})$, and let $H = \mathrm{Gal}(K/F) \subset G$; note that these groups are isomorphic to the symmetric group S_3 and the alternating group $A_3 \subset S_3$, respectively. Let $\chi\colon H \to \mathbb{C}^\times$ be a non-trivial character of H (sending a generator of H to a primitive third root of unity).

(a) Show that the induced representation $\mathrm{Ind}_H^G \chi$ is isomorphic to the two-dimensional representation $\rho\colon G \to \mathrm{GL}_2(\mathbb{C})$ defined in Example 1.19.

(b) Let $\mathfrak{p}$ be the unique place of F lying over 23. Compute the L-factors $L_{\mathfrak{p}}(\chi, s)$ and $L_p(\rho, s)$. (*Hint:* they should be equal.)

Exercise 3.38. (a) For each irreducible representation ρ of the group $G = S_3$, find subgroups $H_i \subseteq G$, one-dimensional representations ψ_i of the groups H_i and integers n_i as in Brauer's theorem 3.12.

(b) Same question for $G = A_4$.

(c) Same question for $G = S_4$.

(*Hint:* look up (or compute) the *character tables* of these groups, and use Frobenius reciprocity.)

Elliptic curves

Exercise 3.39. The category of complex elliptic curves *modulo isogeny* $\mathrm{Ell}(\mathbb{C}) \otimes \mathbb{Q}$ is the category whose objects are the elliptic curves E over $\mathbb{C}$ and whose morphisms are given as follows. Let E, E' be two elliptic curves over $\mathbb{C}$. The set of morphisms $\mathrm{Hom}(E, E')$ taken in the category of elliptic curves is an abelian group. We define

$$\mathrm{Hom}_{\mathrm{Ell}(\mathbb{C})\otimes\mathbb{Q}}(E, E') \stackrel{\mathrm{def}}{=} \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathrm{Ell}(\mathbb{C})}(E, E').$$

(a) Explain that $\mathrm{Ell}(\mathbb{C}) \otimes \mathbb{Q}$ is indeed a category (*i.e.* morphisms can be composed, and the axioms of a category are satisfied). Show that $F\colon \mathrm{Ell}(\mathbb{C}) \to \mathrm{Ell}(\mathbb{C}) \otimes \mathbb{Q}$ is a functor.

(b) Let $f\colon E \to E'$ be a morphism between two elliptic curves that respects the structure of group variety (*i.e.* a morphism of elliptic curves). Show that the following statements are equivalent:

(i) f is an *isogeny* (*i.e.* f is a surjection and has finite kernel);

(ii) f is surjective;

(iii) f has finite kernel;

(iv) f is non-trivial;

(v) $F(f)$ is an isomorphism.

(c) Show that the category $\mathrm{Ell}(\mathbb{C}) \otimes \mathbb{Q}$ is equivalent to the category whose objects are pairs (V, I), where V is a 2-dimensional $\mathbb{Q}$-vector space and $I \in \mathrm{End}_{\mathbb{R}}(V \otimes_{\mathbb{Q}} \mathbb{R})$ is a complex structure on the real vector space $V \otimes_{\mathbb{Q}} \mathbb{R}$, *i.e.* an element such that $I^2 = -1$. (part of the exercise is to define the correct notion of morphisms $(V, I) \to (V', I')$).

(d) Show that there exist a functor $\mathrm{Ell}(\mathbb{C}) \otimes \mathbb{Q} \to \mathbb{Q}_\ell$-vsp sending an elliptic curve E up to isogeny to the 'rational' Tate module $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \varprojlim E_{\ell^n}(\mathbb{C})$.

Exercise 3.40. Let E, E' be two elliptic curves over a number field F.

(a) Show that the following statements are all equivalent[1]

(a) $V_\ell(E)_{\mathrm{ss}} \cong V_\ell(E')_{\mathrm{ss}}$ for a single prime ℓ.

(b) $V_\ell(E)_{\mathrm{ss}} \cong V_\ell(E')_{\mathrm{ss}}$ for all prime numbers ℓ.

(c) for almost all finite places v of F where E and E' have good reduction, we have $\#E(\kappa_v) = \#E'(\kappa_v)$

(d) for all finite F-places v where E and E' have good reduction, we have $\#E(\kappa_v) = \#E'(\kappa_v)$.

A famous theorem of Faltings states that the above properties are equivalent to E and E' being isogenous.

(b) Does the equivalence of the first two items hold over a finite field $\mathbb{F}_q$?

Exercise 3.41. Let $\mathfrak{H}^\pm = \mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R})$ be the complex double half space; *i.e.* the set of complex numbers $z \in \mathbb{C}$ whose imaginary part not zero. The group $\mathrm{GL}_2(\mathbb{C})$ acts on $\mathbb{P}^1(\mathbb{C})$ via its natural action on $\mathbb{C}^2$ and its induced action on the space of lines through the origin. The subgroup $\mathrm{GL}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{C})$ fixes $\mathbb{P}^1(\mathbb{R})$ and hence its complement $\mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R})$ in $\mathbb{P}^1(\mathbb{C})$. Thus $\mathrm{GL}_2(\mathbb{R})$ acts on the space $\mathfrak{H}^\pm$.

(a) Show that the action on $\mathfrak{H}^\pm$ obtained in the above way is given by the formula $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z = \frac{az+b}{cz+d}$ for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ and all $z \in \mathfrak{H}^\pm$.

(b) Show that the set of isomorphism classes of complex elliptic curves equals $\mathrm{GL}_2(\mathbb{Z})\backslash\mathfrak{H}^\pm$.

(c) Show that the set of isogeny classes of complex elliptic curves equals $\mathrm{GL}_2(\mathbb{Q})\backslash\mathfrak{H}^\pm$.

(d) Consider the group Γ of matrices $X \in \mathrm{GL}_2(\mathbb{Z})$ such that $X \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \mod 4$. Show that for each point $x \in \mathfrak{H}^\pm$ there exists an open neighborhood $U_x \subset \mathfrak{H}^\pm$ such that for every $\gamma \in \Gamma$ we have $\gamma U_x \cap U_x \neq \emptyset \Leftrightarrow \gamma = \pm 1 \in \mathrm{GL}_2(\mathbb{Z})$. Deduce that the quotient space $\Gamma\backslash\mathfrak{H}^\pm$ has the natural structure of a complex manifold.

(e) Show that the space of isogeny classes of complex elliptic curves $\mathrm{GL}_2(\mathbb{Q})\backslash\mathfrak{H}^\pm$ is not Haussdorff and that it can't have the structure of a manifold.

Exercise 3.42. This exercise is a continuation of Exercise 3.41. Let Γ be as in 3.41.(d).

(a) Define a 2-dimensional complex manifold $\mathbb{E}$ equipped with an action of $\mathrm{GL}_2(\mathbb{Z})$ and a $\mathrm{GL}_2(\mathbb{Z})$-equivariant map $\pi\colon \mathbb{E} \to \mathfrak{H}^\pm$ such that the quotient space $\mathrm{GL}_2(\mathbb{Z})\backslash\mathbb{E}$ has the following property. For every $\tau \in \mathfrak{H}^\pm$ the fibre $\pi^{-1}(\tau)$ is isomorphic to the complex elliptic curve $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$.

(b) Show, similar to Exercise 3.41.(d), that $\Gamma\backslash\mathbb{E}$ is a complex manifold and that the map $\Gamma\backslash\mathbb{E} \to \Gamma\backslash\mathfrak{H}^\pm$ is a morphism of manifolds.

Exercise 3.43. Let K be quadratic imaginary field. Let I be a fractional $\mathcal{O}_K$-ideal. Show that the complex elliptic curve $E_I = \mathbb{C}/I$ is an elliptic curve that has extra multiplications by $\mathcal{O}_K$.

[1]Here $V_\ell(E)_{\mathrm{ss}}$ denotes the semi-simplification of $V_\ell(E)$. In fact it is known that $V_\ell(E)$ is semi-simple, but you do not need this fact to solve the exercise.

(a) Show that for two such fractional ideals I, I' we have $E_I \cong E_{I'}$ if and only if I and I' differ by a principal R-ideal.

(b) Establish a bijection between the set of isomorphism classes of complex elliptic curves E with $\mathrm{End}(E) = \mathcal{O}_K$ and the ideal class group of $\mathcal{O}_K$.

Exercise 3.44. Let E be an elliptic curve over a finite field $\mathbb{F}_q$. In this exercise we will show that $\#E(\mathbb{F}_q) \leq 2\sqrt{q}$.

(a) Let A be an abelian group and let $d\colon A \to \mathbb{Z}$ be a positive definite quadratic form, which means

- $d(x) = d(-x)$ for all $x \in A$, and $A \times A \to \mathbb{Z}$, $(x, y) \mapsto d(x + y) - d(x) - d(y)$ is bilinear. (*i.e.* d is a *quadratic form*).
- $d(x) \geq 0$ for all $x \in A$, and $d(x) = 0$ if and only if $x = 0$ (*i.e.* d is *positive definite*).

Show that for all $a, b \in A$ we have $|d(a - b) - d(a) - d(b)| \leq 2\sqrt{d(a)d(b)}$.

(b) Show that the degree mapping $d\colon \mathrm{End}_{\mathbb{F}_q}(E) \to \mathbb{Z}$ is a positive definite quadratic form.

(c) Deduce that $\#E(\mathbb{F}_q) \leq 2\sqrt{q}$.

Exercise 3.45. Let E be an elliptic curve over $\mathbb{Q}$ given by the Weierstrass equation $y^2 = x^3 + 1$. Compute the set of 2-torsion points $E[2](\overline{\mathbb{Q}})$ on E, and describe the Galois action on this set.

Exercise 3.46. Let F be a p-adic local field and E/F an elliptic curve given by a Weierstrass equation as in (3.6), with coefficients $a_i \in F$. Show that if $a_i \in \mathcal{O}_F$ and $v(\Delta) < 12$, then this equation is *minimal*.

Exercise 3.47. Let E be an elliptic curve over a number field F, and let $r\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{Q}_\ell} V_\ell(E) \simeq \mathrm{GL}_2(\mathbb{Q}_\ell)$ be the Galois representation on the Tate module of E. Show that as a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the Tate module of the n-fold product $E \times E \times \cdots \times E$ is isomorphic to the n-th tensor power of r.

Exercise 3.48. Let E be an elliptic curve over a number field F. Show that there exists a finite solvable extension L/F such that the set of points $(x, y, z) \in E(\overline{F})$ of order 3 are defined over L (*i.e.* for some $\lambda \in \overline{F}^\times$ we have $(\lambda x, \lambda y, \lambda z) \in F^3$).

Exercise 3.49. This exercise is for those students who have some familiarity with abelian varieties. Let A be an abelian variety of dimension 2 over $\mathbb{Q}$, *i.e.* an abelian surface. Let K be a totally real quadratic extension of $\mathbb{Q}$, and assume that there exists a morphism $i\colon K \to \mathbb{Q} \otimes \mathrm{End}_{\mathbb{Q}}(A)$. Assume that ℓ is split in K. Show that there exists a 2-dimensional Galois representation $V/\mathbb{Q}_\ell$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that for all prime numbers p where A has good reduction V is unramified, and $p \neq \ell$, we have $\#A(\mathbb{F}_p) = 1 - \mathrm{Tr}(\mathrm{Frob}_p, V) + p$.

Exercise 3.50. Let $E/\mathbb{F}_q$ be an elliptic curve. Show that there are two algebraic numbers $\alpha, \beta \in \overline{\mathbb{Q}}$ such that for all integers $j \geq 1$ we have $\#E(\mathbb{F}_{q^j}) = 1 + q^j - \alpha^j - \beta^j$.

Exercise 3.51. Consider the elliptic curve E given by the equation $y^2 = x^3 - 4x$ over the field $\mathbb{F}_5$.

(a) Compute the characteristic polynomial $f \in \mathbb{Z}[X]$ of the Frobenius acting on the ℓ-adic Tate module of E.

(b) Compute $\#E(\mathbb{F}_{5^5})$.

Exercise 3.52. Let E be an elliptic curve over a number field F. Let $a_E \in \mathbb{R}$ be the naive density of the set of finite F-places v where E has good reduction and such that the number of $\kappa(v)$-points $\#E(\kappa(v))$ is even. Explain that this density exists and show that either $a_E = 1/3$, $a_E = 2/3$ or $a_E = 1$.

Exercise 3.53. (a) Let G be a topological group, which is Haussdorff. Show that the space of connected components $\pi_0(G)$ is naturally a topological group as well.

Let F be a number field.

(b) Show that the surjection $\mathbb{A}_F^\times/F^\times \to \mathbb{A}_F^\times \Big/ \overline{F^\times (F \otimes \mathbb{R})^{\times +}}$ induces an isomorphism $\pi_0(\mathbb{A}_F^\times/F^\times) \xrightarrow{\sim} \mathbb{A}_F^\times \Big/ \overline{F^\times (F \otimes \mathbb{R})^{\times +}}$.

(c) Explain that the abelianized absolute Galois group $\mathrm{Gal}(\overline{F}/F)^{\mathrm{ab}}$ identifies naturally with the component group $\pi_0(\mathbb{A}_F^\times/F^\times)$ of $\mathbb{A}_F^\times/F^\times$.

Exercise 3.54. Let F be a number field, and $\chi\colon \mathbb{A}_F^\times/F^\times \to \mathbb{C}^\times$ be an algebraic Hecke character.

(a) Show that there exists a number field $E \subset \mathbb{C}$ such that $\chi(\mathbb{A}_F^{\infty,\times}) \subset E^\times$.

(b) Let λ be a finite E-place, and let ℓ be the rational prime number below λ. Show that there exists a unique continuous morphism $\chi_\lambda\colon \mathbb{A}_F^\times/F^\times \to E_\lambda^\times$ such that for all finite E-places v not dividing ℓ where χ is unramified, we have that χ_λ is unramified as well, $\chi_\lambda(\varpi_v) \in E^\times$ and $\chi_\lambda(\varpi_v) = \chi(\varpi_{F_v}) \in E^\times \subset E_\lambda^\times$.

Hodge–Tate numbers

Exercise 3.55. Let $E/\mathbb{Q}$ be an elliptic curve, and let $(r, V)/\overline{\mathbb{Q}}_\ell)$ be its associated Galois representation on its Tate module. Show that V_{ss} is not isomorphic to a direct sum of two 1-dimensional representations given by algebraic characters χ_1, χ_2 (for algebraic, see 3.59).

Exercise 3.56. Let L/F be a (possibly infinite) Galois extension of fields with (profinite) Galois group G. Let V be an L-vector space with a semi-linear action of G, *i.e.* V viewed as an F-vector space is a G-representation, and for all $\sigma \in G$, all $x \in L$ and all $v \in V$ we have $\sigma(xv) = \sigma(x)v$.

(a) Show that the natural mapping $L \otimes_F V^G \to V$ is an isomorphism.

(b) Show that the mapping $W \mapsto L \otimes_F W$ is a bijection between F-subspaces of V^G and G-invariant L-subspaces of V.

Exercise 3.57. Show that the transcendence degree of $\mathbb{C}_\ell$ over $\mathbb{Q}_\ell$ is infinite. (Hint: Consider elements $x \in \mathbb{C}_\ell$ on which the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ acts via a continuous morphism $\chi\colon \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathbb{C}_\ell^\times$ with infinite image.)

Exercise 3.58. Let ℓ be a prime number.

(a) Show that $\mathbb{Z}_\ell^\times$ is isomorphic to $\mathbb{F}_\ell^\times \times (1 + \ell\mathbb{Z}_\ell)$ if ℓ is odd, and isomorphic to $\mu_4 \times (1 + 4\mathbb{Z}_2)$ if $\ell = 2$.

(b) Show that the multiplicative group $(1 + \ell\mathbb{Z}_\ell) \subset \mathbb{Z}_\ell^\times$ is isomorphic to $\mathbb{Z}_\ell$, and has a natural structure of a free $\mathbb{Z}_\ell$-module of rank 1.

(c) Let χ_ℓ be the ℓ-adic cyclotomic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Write t for the composition $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_\ell^\times \twoheadrightarrow (1 + \ell\,\gcd(\ell, 2)\mathbb{Z}_\ell)$. Let $\chi\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \overline{\mathbb{Q}}_\ell^\times$ be a 1-dimensional Galois representation. Show that χ is of the form $\rho \cdot t^{a_\chi}$ where $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \overline{\mathbb{Q}}_\ell^\times$ has finite image and $a_\chi \in \mathbb{Z}_\ell$.

Exercise 3.59. Choose an ι as in Exercise 3.20. Let $\chi\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \overline{\mathbb{Q}}_\ell^\times$ be a continuous morphism, then we call χ *algebraic* if and only if the number $a_\chi \in \mathbb{Z}_\ell$ from Exercise 3.58.(c) is an integer $a_\chi \in \mathbb{Z}$. We call a continuous morphism $\rho\colon \mathbb{A}^\times/\mathbb{Q}^\times \to \mathbb{C}^\times$ *algebraic* if its restriction to $\mathbb{R}^\times \subset \mathbb{A}^\times$ is given by $x \mapsto x^{a_\rho}$ for some integer $a_\rho \in \mathbb{Z}$.

Show that the exist a unique bijection

$$\Psi\colon \mathrm{Hom}_{\text{cts, alg}}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \overline{\mathbb{Q}}_\ell^\times) \to \mathrm{Hom}_{\text{cts, alg}}(\mathbb{A}^\times/\mathbb{Q}^\times, \mathbb{C}^\times)$$

such that if χ maps to $\rho = \Psi(\chi)$, then

1. if χ is unramified at a prime number $p \neq \ell$, then ρ is unramified at p as well (*i.e.* $\rho(I_v) = 1$, where $I_v \subset \mathbb{A}^\times/\mathbb{Q}^\times$ is the subgroup $1 \times \mathcal{O}_{F_v}^\times \subset \mathbb{A}_F^{\times,v} \times F_v^\times = \mathbb{A}_F^\times$);
2. if χ is unramified at $p \neq \ell$, then $\chi(\mathrm{Frob}_p) = \rho(\widehat{p})$, where $\widehat{p}$ is the idèle $(1, p) \in \mathbb{A}^{\times,p} \times \mathbb{Q}_p^\times = \mathbb{A}^\times$;
3. and $a_\chi = a_\rho$.

Étale cohomology

Exercise 3.60. Let $\mathbb{F}_q$ be a finite field of q elements, and let $n \geq 0$. Prove the identity

$$\zeta_{\mathbb{P}^n_{\mathbb{F}_q}} = \frac{1}{(1-t)(1-qt)\dots(1-q^n t)}.$$

Exercise 3.61. Let E and F be elliptic curves over a finite field $\mathbb{F}_q$ of q elements, and let $a, b \in \mathbb{Z}$ be such that

$$\zeta_E = \frac{1 - at + qt^2}{(1-t)(1-qt)}, \quad \zeta_F = \frac{1 - bt + qt^2}{(1-t)(1-qt)}$$

Express the rational function $\zeta_{E\times F}$ in terms of a and b.

Exercise 3.62. Let X be a smooth projective variety of dimension d over a finite field $\mathbb{F}_q$ of q elements.

(i) Prove that in the functional equation

$$\zeta_X\left(\frac{1}{q^n t}\right) = \eta_X t^e \zeta_X(t),$$

we have

$$e = \sum_{i=0}^{2n} (-1)^i b_i \quad \text{with } b_i = \deg P_i$$

and

$$\eta_X = \pm q^{ne/2}.$$

(ii) Prove that the polynomials P_i satisfy

$$P_i\left(\frac{1}{q^n t}\right) = c_i t^{-b_i} P_{2n-i}(t)$$

for some $c_i \in \mathbb{Q}^\times$, and determine c_i in terms of P_i.

(You may use Theorem 3.28.)

Exercise 3.63. Let X, Y and Z be varieties over a field k, let $f\colon X \to Y$ and $g\colon Y \to Z$ be morphisms, and let $h = g \circ f$.

(a) Show that if f and g are étale, then h is étale.

(b) Show that if g and h are étale, then f is étale.

(c) Give an example where f and h are étale, but g is not.

Exercise 3.64. Let X be a variety over a field k, and let $f\colon U \to X$ and $g\colon V \to X$ be étale morphisms. Show that the canonical morphism $U \times_X V \longrightarrow X$ is étale.

Exercise 3.65. Let k be a field, let $Y = \operatorname{spec} k$ be the one-point variety over k, and let X be the closed subvariety of the affine line $\mathbb{A}^1_k$ defined by a polynomial $f \in k[x]$. Show that the canonical morphism $X \to Y$ is étale if and only if f is non-zero and separable.

Exercise 3.66. Let k be a field of characteristic different from 2, and let C be the nodal cubic curve in the affine plane $\mathbb{A}^2_k$ defined by the equation $y^2 = x^2(x+1)$. Show that there exists a finite étale covering $C' \to C$ of degree 2, where C' is connected.

Exercise 3.67. Let A be an Abelian group, and let X be a variety over a field k. For every étale morphism $U \to X$, let $A_X(U \to X)$ be the set of functions $U \to A$ that are continuous (*i.e.* locally constant) for the Zariski topology on U and the discrete topology on A. Prove that A_X is a sheaf on $X_{\text{ét}}$.
(*Hint:* you may use without proof that étale morphisms are open for the Zariski topology.)

Exercise 3.68. Let k be a field, let $\bar{k}$ be a separable closure of k, and let X be the one-point variety $\operatorname{spec} k$ over k. Prove that the category $\mathbf{Ab}(X_{\text{ét}})$ of sheaves for the étale topology on $X_{\text{ét}}$ is equivalent to the category of discrete Abelian groups with a continuous action of $\operatorname{Gal}(\bar{k}/k)$.

Exercise 3.69. Let X be a variety over a field k. For every object $U \to X$ in $X_{\text{ét}}$, a *sieve* on U is a collection $\mathcal{S}$ of morphisms $V \to U$ in the category $X_{\text{ét}}$ (we omit the morphisms to X from the notation) with the property that for every morphism $V' \to V$ in $X_{\text{ét}}$ and every morphism $V \to U$ in $\mathcal{S}$, the composed morphism $V' \to U$ is in $\mathcal{S}$. A *covering sieve* on U is a sieve $\mathcal{S}$ on U that is jointly surjective, i.e. for every point $x \in U$ there exists a morphism $V \to U$ in $\mathcal{S}$ whose image contains x. If $\mathcal{S}$ is a sieve on U and $f\colon U' \to U$ is any morphism in $X_{\text{ét}}$, we write $f^*\mathcal{S}$ for the collection of all morphisms $V \to U'$ for which the composed morphism $V \to U' \xrightarrow{f} U$ is in $\mathcal{S}$.

Prove the following statements, which together say that the collection of all covering sieves on objects of $X_{\text{ét}}$ is a *Grothendieck topology* on $X_{\text{ét}}$.

(i) For every object U in $X_{\text{ét}}$, the collection of all morphisms $V \to U$ in $X_{\text{ét}}$ is a covering sieve of U.

(ii) If $f\colon U' \to U$ is a morphism in $X_{\text{ét}}$ and $\mathcal{S}$ is a covering sieve of U, then $f^*\mathcal{S}$ is a covering sieve of U'.

(iii) Let $\mathcal{S}$ be a covering sieve of U, and let $\mathcal{T}$ be any sieve on U such that for every morphism $f\colon U' \to U$ in $\mathcal{S}$ the sieve $f^*\mathcal{T}$ is a covering sieve on U'. Then $\mathcal{T}$ is a covering sieve on U.

(*Hint:* use fibre products.)

Exercise 3.70. Formulate and prove an analogue of the previous exercise for classical topological spaces.

Weil–Deligne representations

Exercise 3.71. Prove the identity (3.11).

Exercise 3.72. Let (ρ, V, N) be a Weil–Deligne representation of F such that the smooth representation (ρ, V) is irreducible. Prove that N is the zero endomorphism.

Exercise 3.73. Let G be either the absolute Galois group or the Weil group of F, and let I be the inertia subgroup. Let ℓ be a prime number different from p, let V be a finite-dimensional $\mathbb{Q}_\ell$-vector space, and let $\rho\colon G \to \mathrm{Aut}_{\mathbb{Q}_\ell} V$ be a continuous representation.

(a) Suppose that the automorphism $\rho(g)$ is unipotent for every $g \in I$. Prove that if V is irreducible, then I acts trivially on V.

(b) Deduce that $\rho(g)$ is unipotent for every $g \in G$ if and only if I acts trivially on the semi-simplification of V.

(*Hint:* use the structure of the maximal pro-ℓ-primary part of the inertia group.)

Chapter 4

Complex representations of GL_n of a local field

Contents

The global Langlands correspondence for the group GL_n over $\mathbb{Q}$ is, roughly speaking, a correspondence between compatible families of n-dimensional ℓ-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the one hand, and *automorphic representations* of the adelic group $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$ on the other hand. The latter representations are (in general infinite-dimensional) complex representations of $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$, which are traditionally often denoted by π or σ.

Both sides of the Langlands correspondence are studied to a large extent using *local* methods. On the Galois side, a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ can be restricted to decomposition groups at the finite places of $\mathbb{Q}$, which can be identified with the local Galois groups $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. On the automorphic side, an automorphic representation π of $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$ decomposes as an (infinite) tensor product of certain representations π_p of the groups $\mathrm{GL}_n(\mathbb{Q}_p)$.

In this chapter, we will introduce the notions needed to understand these local components π_p. A useful reference for this chapter is [3, Chapter 1].

4.1 Haar measures and Hecke algebras

We begin with some general theory on locally profinite groups.

Haar measures

Let G be a locally compact topological group. We define

$$\mathcal{C}_{\mathrm{c}}(G) = \{f\colon G \to \mathbb{R} \text{ continuous with compact support}\}$$

and we let $\mathcal{C}_{\mathrm{c}}(G)^\vee$ denote the $\mathbb{R}$-linear dual of $\mathcal{C}_{\mathrm{c}}(G)$. The canonical left action of G on itself gives a right action

$$\begin{aligned} \mathcal{C}_{\mathrm{c}}(G) \times G &\longrightarrow \mathcal{C}_{\mathrm{c}}(G) \\ (f, g) &\longmapsto fg, \end{aligned}$$

where $fg \in \mathcal{C}_{\mathrm{c}}(G)$ is defined by $(fg)(h) = f(gh)$. This in turn gives a left action

$$\begin{aligned} G \times \mathcal{C}_{\mathrm{c}}(G)^\vee &\longrightarrow \mathcal{C}_{\mathrm{c}}(G)^\vee \\ (g, \phi) &\longmapsto g\phi \end{aligned}$$

where $(g\phi)(f) = \phi(fg)$. Similarly, the right action of G on itself gives a left action

$$\begin{aligned} G \times \mathcal{C}_{\mathrm{c}}(G) &\longrightarrow \mathcal{C}_{\mathrm{c}}(G) \\ (g, f) &\longmapsto gf, \end{aligned}$$

where $gf \in \mathcal{C}_{\mathrm{c}}(G)$ is defined by $(gf)(h) = f(hg)$. This in turn gives a right action

$$\begin{aligned} \mathcal{C}_{\mathrm{c}}(G)^\vee \times G &\longrightarrow \mathcal{C}_{\mathrm{c}}(G)^\vee \\ (\phi, g) &\longmapsto \phi g, \end{aligned}$$

where $(\phi g)(f) = \phi(gf)$.

Definition 4.1. A *measure* on G is an element $\mu \in \mathcal{C}_{\mathrm{c}}(G)^\vee$ such that if f is non-negative everywhere and not identically zero, then $\mu(f) > 0$. A *left Haar measure* on G is a measure μ satisfying

$$g\mu = \mu \quad \text{for all } g \in G.$$

A *right Haar measure* on G is a measure ν satisfying

$$\nu g = \nu \quad \text{for all } g \in G.$$

It is known (see Exercise 2.9) that there exists a unique left (resp. right) Haar measure on G, up to scaling by a positive constant. However, they are not necessarily equal.

If μ is a measure on G and S is a compact open subset of G, we write

$$\mu(S) = \mu(\mathbf{1}_S),$$

where $\mathbf{1}_S$ is the characteristic function of S, defined by

$$\begin{aligned} \mathbf{1}_S\colon G &\longrightarrow \mathbb{R} \\ g &\longmapsto \begin{cases} 1 & \text{if } g \in S, \\ 0 & \text{if } g \notin S. \end{cases} \end{aligned}$$

For μ either a left or a right Haar measure and $f \in \mathcal{C}_{\mathrm{c}}(G)$, we will use the following notations interchangeably:

$$\int_G f\, d\mu = \int_{x \in G} f(x) d\mu(x) = \mu(f).$$

One checks (Exercise 4.1) that the left invariance of μ and the right invariance of ν can be expressed as

$$\int_{x\in G} f(gx)d\mu(x) = \int_{x\in G} f(x)d\mu(x),$$
$$\int_{x\in G} f(xg)d\nu(x) = \int_{x\in G} f(x)d\nu(x).$$

Let G be a locally compact topological group. If μ is a left Haar measure on G, then for every $g \in G$, the element $\mu g \in \mathcal{C}_c(G)^\vee$ is again a left Haar measure on G. This means that there exists $\delta_G(g) > 0$ such that

$$\delta_G(g) \cdot \mu g = \mu \quad \text{for all } g \in G.$$

This gives a canonical group homomorphism

$$\delta_G \colon G \to \mathbb{R}_{>0}.$$

One can show (Exercise 4.2) that δ_G satisfies a corresponding identity for left Haar measures: if ν is a right Haar measure on G, then

$$g\nu = \delta_G(g) \cdot \nu \quad \text{for all } g \in G.$$

The function δ_G is called the *modular function* of G (no relation to modular forms). We say that G is *unimodular* if δ_G is identically 1.

Hecke algebras

We have seen that representations of a finite group G can be viewed as modules over the group algebra $\mathbb{C}[G]$. In this section we will introduce an appropriate analogue of this group algebra for locally profinite groups.

Let G be a locally profinite group. We write

$$\mathcal{H}(G) = \{f \colon G \to \mathbb{C} \mid f \text{ is locally constant and has compact support}\}.$$

(Note that "locally constant" is the same as continuous for the discrete topology on $\mathbb{C}$.)

We fix a right Haar measure ν on G. On $\mathcal{H}(G)$, we define a $\mathbb{C}$-bilinear multiplication map by

$$(f * g)(x) = \int_{y\in G} f(xy^{-1})g(y)d\nu(y).$$

Lemma 4.2. *Let G be a locally profinite group, and let ν be a right Haar measure on G.*

(i) The product defined above can also be written as

$$(f * g)(x) = \int_{y\in G} f(y^{-1})g(yx)d\nu(y).$$

(ii) The product is associative, i.e.

$$(f * g) * h = f * (g * h) \quad \text{for all } f, g, h \in \mathcal{H}(G).$$

(iii) There exists a unit element for the product $*$ on $\mathcal{H}(G)$ if and only if G is discrete.

Proof. See Exercise 4.4. □

For any compact open subgroup $K \subseteq G$, we write

$$\mathcal{H}(G, K) = \{f \in \mathcal{H}(G) \mid f \text{ is left and right } K\text{-invariant}\}.$$

Given two such subgroups $K' \subseteq K$, we have an injection $\mathcal{H}(G, K) \subseteq \mathcal{H}(G, K')$. Since every $f \in \mathcal{H}(G)$ is left and right K-invariant for suffiently small K, we can write $\mathcal{H}(G)$ as a direct limit

$$\mathcal{H}(G) = \varinjlim_{K} \mathcal{H}(G, K),$$

with K ranging over the set of compact open subgroups of G.

For any open compact subgroup $K \subseteq G$, we define an element $e_K \in \mathcal{H}(G)$ as $\nu(K)^{-1}$ times the characteristic function of K. Then we have

$$e_K * e_K = e_K$$

and

$$\mathcal{H}(G, K) = e_K * \mathcal{H}(G) * e_K.$$

Note that each $\mathcal{H}(G, K)$ has e_K as its unit element, but the maps between them do not respect these.

4.2 Smooth and admissible representations

A locally profinite group has a huge number of complex representations. For our purposes, the "well-behaved" representations are the ones satisfying certain conditions, namely *smoothness* and the stronger notion of *admissibility*.

Definition 4.3. Let G be a locally profinite group, let V be a $\mathbb{C}$-vector space (possibly infinite-dimensional), and let $\pi\colon G \to \mathrm{Aut}_{\mathbb{C}}(V)$ be a group homomorphism. We say that (π, V) is *smooth* if for every $v \in V$ there exists an open subgroup $K \subseteq G$ such that $Kv = \{v\}$. We say that (π, V) is *admissible* if it is smooth and for every open subgroup K the space

$$V^K = \{v \in V \mid \pi(k)v = v \text{ for all } k \in K\}$$

is finite-dimensional.

Let (π, V) and (π', V') be smooth representations of G. A *morphism* from (π, V) to (π', V') is a $\mathbb{C}$-linear map $t\colon V \to V$ satisfying $t(\pi(g)v) = \pi'(g)(t(v))$ for all $g \in G$ and $v \in V$.

The smooth representations of G form an Abelian category, and the admissible representations of G form a full subcategory. In particular, there is a notion of simple objects, called *irreducible (smooth) representations*. However, we note that these categories are in general *not* semi-simple. (They are if G is compact; see Exercise 4.10.)

We now introduce similar notions for Hecke algebras.

Definition 4.4. A *representation* of $\mathcal{H}(G)$ is a homomorphism

$$\pi\colon \mathcal{H}(G) \to \mathrm{End}_{\mathbb{C}}(V)$$

of (non-unital) $\mathbb{C}$-algebras, where V is a $\mathbb{C}$-vector space. We say that a representation (π, V) of $\mathcal{H}(G)$ is *smooth* if $\mathcal{H}(G)V$ is equal to V, *i.e.* if for every $v \in V$ there exists $f \in \mathcal{H}(G)$ such that $\pi(f)v = v$.

Like smooth representations of G, the smooth representations of $\mathcal{H}(G)$ form a category. We will see below that the two categories are equivalent.

Remark 4.5. A (smooth) representation of $\mathcal{H}(G)$ is also called a (smooth) $\mathcal{H}(G)$-module, but one needs to be somewhat careful with this terminology because $\mathcal{H}(G)$ is not a unital ring in general.

Theorem 4.6. *Let G be a locally profinite group. Then every smooth representation of G can be given the structure of a smooth representation of $\mathcal{H}(G)$ in a natural way. This gives an equivalence of categories*

$$\{\textit{smooth representations of } G\} \xrightarrow{\sim} \{\textit{smooth representations of } \mathcal{H}(G)\}.$$

Proof. We just sketch the construction; the details are left as an exercise.

Given a smooth representation (π, V) of G, a function $f \in \mathcal{H}(G)$ and a vector $v \in V$, we define

$$\pi(f)v = \int_G f(g)\pi(g)v \, d\nu(g) \in V.$$

This notation needs a definition. Because (π, V) is smooth and f is locally constant with compact support, we can choose a compact open subgroup $K \subseteq G$ such that for all $k \in K$ and $g \in G$ we have $\pi(k)v = v$ and $f(gk)$. Then we define the above integral as the finite sum

$$\pi(f)v = \nu(K) \sum_{g \in G/K} f(g)\pi(g)v \in V.$$

One checks that this gives V the structure of a smooth representation of $\mathcal{H}(G)$.

Conversely, given a smooth representation (π, V) of $\mathcal{H}(G)$, an element $g \in G$ and a vector $v \in V$, we define

$$\pi(g)v = \pi(f_{gK})v,$$

where K is an open compact subgroup of G such that $\pi(e_K)v = v$ and the function f_{gK} is $\nu(gK)^{-1}$ times the characteristic function of gK. Again, one checks that this gives V the structure of a smooth representation of G. □

Let (π, V) be a smooth representation of G, and let K be a compact open subgroup of G. Then the subspace V^K of K-invariants is in a natural way a module over the (unital) $\mathbb{C}$-algebra $\mathcal{H}(G, K)$; see Exercise 4.13.

Induction

As for finite groups, a very useful way to construct representations is by *induction* and *coinduced* (or *compact*) induction. In contrast to the case of finite groups, these constructions are in general not isomorphic.

Definition 4.7. Let G be a locally profinite group, let H be a closed subgroup of G, and let (π, V) be a smooth representation of H. The *induced representation* of G, notation $\mathrm{Ind}_H^G(\pi, V)$ is the pair (π', V') defined as follows. The $\mathbb{C}$-vector space V' is defined as the space of all functions

$$f\colon G \to V$$

satisfying the following conditions: we have

$$f(hg) = \pi(h)(f(g)) \quad \text{for all } g \in G, h \in H$$

and there exists a compact open subgroup $K \subseteq G$ such that

$$f(gk) = f(g) \quad \text{for all } g \in G, k \in K.$$

This V' is equipped with the left G-action coming from the right action of G on itself, *i.e.* the group homomorphism $\pi'\colon G \to \mathrm{Aut}_{\mathbb{C}}(V')$ is defined by

$$\pi'(g)(f) = (g' \mapsto f(g'g)) \quad \text{for all } g \in G, f \in V'.$$

The *coinduced representation* of G, notation $\mathrm{cInd}_H^G(\pi, V)$, is defined in the same way, but the space V' is replaced by the subspace of functions $f \in V'$ such that in addition the image of the support of f in $H\backslash G$ is compact.

Alternative names for the functors Ind_H^G and cInd_H^G are *smooth* and *compact* induction, respectively.

Proposition 4.8 (Frobenius reciprocity for smooth representations)**.** *Let G be a locally profinite group, let H be a closed subgroup, let V be a smooth representation of H, and let W be a smooth representation of G. Then there are canonical isomorphisms*

$$_G\mathrm{Hom}(\mathrm{cInd}_H^G V, W) \cong {}_H\mathrm{Hom}(V, \mathrm{Res}_H^G W)$$

and

$${}_H\mathrm{Hom}(\mathrm{Res}_H^G W, V) \cong {}_G\mathrm{Hom}(W, \mathrm{Ind}_H^G V)$$

Example 4.9. Let $G = \mathrm{GL}_2(\mathbb{Q}_p)$, let B be the closed subgroup of G consisting of upper triangular matrices, and let N be the closed normal subgroup of B consisting of matrices of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. There is an isomorphism

$$\begin{aligned} B/N &\xrightarrow{\sim} \mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \\ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) N &\longmapsto (a, d). \end{aligned}$$

Given two continuous characters

$$\chi_1, \chi_2\colon \mathbb{Q}_p^\times \to \mathbb{C}^\times,$$

we let χ be the character of B defined by

$$\chi\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) = \chi_1(a)\chi_2(d).$$

We then define a smooth representation (π, V) of G as the induced representation $\mathrm{Ind}_B^G \chi$. These representations are important building blocks in the construction and classification of irreducible smooth representations of G.

4.3 Unramified representations

The Langlands conjectures predict a relation between Galois representations on the one side and automorphic representations on the other side. In the local case, representations of the local Galois group should correspond to irreducible smooth admissible representations of the local group $\mathrm{GL}_n(\mathbb{Q}_p)$ (or over a finite extension of $\mathbb{Q}_p$). In particular, notions that exist on the one side, should have a counterpart on the other side. In this section we will look at the analogue of the ramification filtration $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)_i$ (where $i \geq -1$) on the side of smooth representations.

On the (local) Galois side, the simplest class of representations are the unramified representations, which have no ramification at all. We have seen that their isomorphism class is essentially given by a conjugacy class in $\mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$, or in $\mathrm{GL}_n(\mathbb{C})$ if the representation was complex. This conjugacy class is given by the image of the Frobenius element. After discussing ramification of smooth representations in a general context, we will specialize quickly to the case of unramified representations and make a detailed study of these since they are the simplest local representations.

Ramification of local representations

Let F be a finite extension of $\mathbb{Q}_p$, and write $G = \mathrm{GL}_n(F)$. Let π be a smooth admissible representation of G. Choose any vector $v \in \pi$ such that $v \neq 0$. By assumption the stabilizer K of v in G is open. Moreover, the subspace $\mathbb{C}[G \cdot v] \subset \pi$ spanned by the translates gv of v, is G-invariant and non-zero. By irreducibility of π, the above inclusion is equality. Thus π is generated by its K-invariant vectors.

Consider the functor F_K from the category of smooth admissible G-representations to the category of complex vector spaces, given by $F_K(\tau) = \tau^K$. Then F_K has an endomorphism ring R_K: If $E_i \colon F_K \to F_K$ are two endomorphisms, we can define $(E_i + E_i)(\tau) = E_i(\tau) + E_i(\tau)$ and $(E_i \cdot E_i)(\tau) = E_i(\tau) \circ E_i(\tau)$ for any smooth admissible representation τ. By general abstract non-sense, the ring R_K acts on the space $\tau^K = F_K(\tau)$ for any τ. Hence we have upgraded F_K to a functor to finite-dimensional complex vector spaces with a left R_K-module structure. Recall the Hecke algebra $H(G, K)$ of K-biinvariant functions $f \colon G \to \mathbb{C}$ such that $f(k_1 \cdot g \cdot k_2) = f(g)$, with $g \in G$ and $k_1, k_2 \in K$, where the product is defined by the convolution product $(f * h)(g) = \int_{x \in G} f(gx^{-1})h(x)\mathrm{d}g$, where the Haar measure on G is normalized so that the volume of K is 1. Since $\mathcal{H}(G, K)$ acts on τ^K for any smooth admissible G-representation, in a way that is functorial in τ, we get an morphism $\mathcal{H}(G, K) \to R_K$. This morphism turns out to be an isomorphism, so the Hecke algebra $\mathcal{H}(G, K) = R_K$ plays a similar role to the group algebra in the context of complex representations of a finite group.

To π we can try to attach the largest subgroup K such that π^K is non-zero. This group K is then a measure for "how ramified" π is. However, this group K is not well-defined (for instance if $v \in V$ is non-zero and has stabilizer K, then gv has stabilizer gKg^{-1}). What one can do is start with a compact open subgroup K and look at all representations π, all of whose irreducible subquotients have K-invariant vectors. These representations are called the *K-spherical representations*. The equivalence from Theorem 4.6 gives an equivalence from the category of smooth admissible K-spherical representations to the category of $\mathcal{H}(G, K)$-modules of finite dimension (in fact it's even an isomorphism of categories). The

algebra $\mathcal{H}(G, K)$ is of finite type, associative and unital (but not commutative in general).

As explained above, attaching a compact open subgroup $K \subset \mathrm{GL}_n(F)$ to a smooth admissible irreducible representation π of $\mathrm{GL}_n(F)$ is not really canonical but by looking at the structure of the local general linear group a little bit further, it is possible to make a well-defined definition of a conductor, as follows. Define for each integer $N \geq 1$ the following compact open subgroup $K(N)$ of matrices $g \in \mathrm{GL}_n(\mathcal{O}_F)$ such that g reduces to the identity matrix modulo N. The groups $K(N) \subset \mathrm{GL}_n(\mathcal{O}_F)$ form a basis of open neighborhoods of the identity element. In particular for any compact open subgroup $K \subset \mathrm{GL}_n(F)$, we can find a large N such that $K(N) \subset K$. The *conductor* of π is then the largest N such that $K(N)$ stabilizes a non-zero vector v in π.

Unramified representations

Let F be a p-adic local field, $G = \mathrm{GL}_n(F)$. The simplest class of irreducible representations of G are the $K = \mathrm{GL}_n(\mathcal{O}_F)$-spherical representations. We call these irreducible representations, the *unramified representations* of G. These representations have conductor equal to 1.

Remark 4.10. The interest of the group $\mathrm{GL}_n(\mathcal{O}_F) \subset \mathrm{GL}_n(F)$ is that it is a so-called *hyperspecial group*, which means that it arises from the group of $\mathcal{O}_F$-points on of a *connected reductive* model $\mathcal{G}/\mathcal{O}_F$ of the group GL_n. These hyperspecial groups are all conjugated, which means that these models $\mathcal{G}$ of GL_n all arise from the choice of a lattice Λ in F^n.

The Cartan decomposition

We wish to make a careful study of the unramified representations. Let $G = \mathrm{GL}_n(F)$ and $K = \mathrm{GL}_n(\mathcal{O}_F)$. As explained the unramified representations π of G correspond to simple modules over the Hecke algebra $\mathcal{H}(G, K)$. The Hecke algebra $\mathcal{H}(G, K)$ is a convolution algebra of functions on the double coset space

$$G/\!\!/K := K\backslash G/K = \mathrm{GL}_n(\mathcal{O}_F)\backslash \mathrm{GL}_n(F)/\mathrm{GL}_n(\mathcal{O}_F).$$

So to study the unramified representations, it is natural to first try to understand what the above double coset space looks like. Note that the quotient $\mathrm{GL}_n(F)/\mathrm{GL}_n(\mathcal{O}_F)$ is easily identified with the space X_F of lattices $\Lambda \subset F^n$. However, from this perspective the further quotient $\mathrm{GL}_n(\mathcal{O}_F)\backslash X_F$ seems rather messy at first. To compute it, the relevant theorem is called the *Smith normal form*, which can be thought of as an extension of the Gaussian elimination process (row/column reduction) to the context of principal ideal domains R.

Theorem 4.11. *Let R be a principal ideal domain, and A an $n \times n$ matrix with coefficients in R. Then there exist two invertible matrices $S, T \in \mathrm{GL}_n(R)$, such that SAT is a diagonal matrix* $\mathrm{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *with $\alpha_i \in R$ and $\alpha_i | \alpha_{i+1}$, for all $i = 1, 2, \ldots, n-1$. The elements $\alpha_i \in R$ are unique up to units.*

Sketch. By multiplying A on the left and on the right by suitable matrices in R, you see that it is possible to perform the following operations on A: (R1) Add a multiple of a row to another row, (R2) Add a multiple of a column to another column, and (R3) Multiply a

row or a column by a unit in R. By doing a form of Gaussian elimination you realize that the any matrix A can be brought down to the form stated in the theorem. Another way to think about this result is to consider the R module $R^n/A(R^n)$ where you view A as an endomorphism $R^n \to R^n$. The quotient of R^n by the image of A, $R^n/A(R^n)$, is then, since R is a PID, isomorphic to a direct sum of modules of the form R/I_i, with $I_i \subset R$ ideals. The generators of the ideals I_i, are then the elements α_i. Since $R/\alpha_i R \cong R/\alpha_j R$ if and only if α_i and α_j differ by a unit in $R^\times$, the uniqueness statement follows. □

The elements α_i are called the *elementary divisors* of the matrix A. If you are willing to suffer, you can compute them by computing many determinants (see theorem below), but in practice it is more convenient to do Gaussian elimination.

Theorem 4.12. *Let $i \in \mathbb{Z}$ be an index $1 \leq i \leq n$. The element $\alpha_1\alpha_2\cdots\alpha_i \in R$ is up to a unit in $R^\times$ equal to the greatest common divisor of the $i \times i$ minors of the matrix A.*

Remark 4.13. In the above statement, with greatest common divisor of two elements $\alpha, \beta \in R$, we meant a generator γ of the ideal $(\alpha, \beta) \subset R$ (in particular this element γ is only well-defined up to units).

If $R = \mathcal{O}_F$, we may take the α_i to be of the form $\varpi_F^{e_i}$, where $\varpi_F \in \mathcal{O}_F$ is a uniformizer, and we obtain the *Cartan decomposition*,

$$K\backslash G/K = \coprod_{e_1 \leq e_2 \leq \ldots \leq e_n} K \cdot \mathrm{diag}(\varpi_F^{e_1}, \varpi_F^{e_2}, \ldots, \varpi_F^{e_n}) \cdot K. \tag{4.1}$$

Remark 4.14. The Cartan decomposition is actually a statement for any reductive group over a local field; but in case of the group GL_n, the result boils down to the Smith normal form, which, as explained in the proof above, is basically a reflection of the classification of R-modules of finite type where R is a principal ideal domain.

Proposition 4.15. *The algebra $\mathcal{H}(G, K)$ is commutative.*

Sketch. The commutativity of $\mathcal{H}(G, K)$ can be seen using the Cartan decomposition explained above, and the observation that by this decomposition, the double cosets are invariant under taking transposes. Exercise 4.19. □

The unramified Hecke algebra

A very good reference on the unramified Hecke algebra and the Satake transform is the paper by Gross [7], which explains the theory for a general unramified reductive group. Another useful reference is Kottwitz's paper [8, Section 5], which explains the theory for GL_n.

It now becomes convenient to introduce some shorthand notation. Let's write $\mathbb{Z}^{n,+}$ for the set of $\lambda \in \mathbb{Z}^n$, such that $\lambda_i \leq \lambda_{i+1}$, $1 \leq i < n$. By Equation (4.1), we have as a vector space that $\mathcal{H}(G, K) = \bigoplus_{\lambda \in \mathbb{Z}^{n,+}} \mathbb{C}$. For $\lambda \in \mathbb{C}$ we write $c_\lambda \in \mathcal{H}(G, K)$ for the corresponding basis vector, so c_λ is the function $G \to \mathbb{C}$, such that for all $g \in G$, $c_\lambda(g) = 1$ if and only if the exponents in the Smith normal form of g are given by λ. On the algebra $\mathcal{H}(G, K)$ we have defined a multiplication operator $*$. It natural to express this multiplication with respect to the basis c_λ. We obtain structural constants $n_{\lambda,\mu}(\nu) \in \mathbb{Z}$ such that $c_\lambda * c_\mu = \sum_{\mu,\lambda \in \mathbb{Z}^{n,+}} n_{\lambda,\mu}(\nu) \cdot c_\nu$ holds for all $\lambda, \mu \in \mathbb{Z}^{n,+}$.

Let's attempt to expand the convolution product $(c_\lambda * c_\mu)(g) = \int_{x\in G} c_\lambda(x)c_\mu(x^{-1}g)\mathrm{d}x$. Write $\lambda(\varpi_F)$ for the matrix $\mathrm{diag}(\varpi_F^{\lambda_1}, \ldots, \varpi_F^{\lambda_n})$. We can decompose double cosets into right cosets $K\lambda(\varpi_F)K = \coprod x_i K$ and $K\mu(\varpi_F)K = \coprod y_i K$ (because this is what you have to do to compute the Haar measure of some subset). Then (see [7, p. 4–5]),

$$\begin{aligned}(c_\lambda * c_\mu)(g) = n_{\lambda,\mu}(\nu) &= \int_G c_\lambda(x)c_\mu(x^{-1}g)\mathrm{d}x = \sum_i \int_{x_iK} c_\mu(x^{-1}g)\mathrm{d}g \\ &= \sum_i \int_K c_\mu(kx_i^{-1}g)\mathrm{d}k = \sum_i c_\mu(x_i^{-1}g) = \#\{(i,j) : \nu(\varpi_F) \in x_i y_i K\}. \qquad (4.2)\end{aligned}$$

By taking $x_i = \lambda(\varpi_F)$ and $y_j = \mu(\varpi_F)$ we see that $n_{\lambda,\mu}(\lambda+\mu) > 0$. In fact, one can show that $n_{\lambda,\mu}(\lambda+\mu) = 1$ and that $n_{\lambda,\mu}(\nu)$ is non zero only if $\nu \leq \lambda + \mu$.

The Satake transform

Write $T \subset \mathrm{GL}_n$ for the diagonal torus. Thus $T(F)$ is the set of matrices of the form $\mathrm{diag}(x_1, x_2, \ldots, x_n) \in \mathrm{GL}_n(F)$ such that $x \in F^{\times,n}$. Similarly, $T(\mathcal{O}_F)$ is the group of diagonal matrices with coefficients in $\mathcal{O}_F^\times$. We write $B \subset \mathrm{GL}_n$ for the group of upper triangular matrices. Inside B we have the subgroup $N \subset B$ of upper triangular unipotent matrices; these are the upper triangular matrices with 1 on every diagonal term. This group $N \subset B$ is normal with quotient T.

In Peter's lectures we have seen parabolic induction of representations. In our current context this means that you start with a smooth character $\chi\colon T(F) \to \mathbb{C}^\times$ (so a morphism of groups with open kernel), and first extend χ to the group $B(F)$ via the surjection $B(F) \to B(F)/N(F) \xrightarrow{\sim} T(F)$. Then we can form the (normalized) induced representation

$$\pi_\chi = \mathrm{Ind}_{B(F)}^G(\chi \otimes \delta_{B(F)}^{1/2}).$$

A basic property of this induced representation is that for any Hecke operator $f \in \mathcal{H}(G,K)$ we have $\mathrm{Tr}\,\pi_\chi(f) = \mathrm{Tr}(f^{(B)}, \chi)$. Here $f^{(B)}$ is the constant term

$$\begin{aligned} f^{(B)}\colon T(F) &\longrightarrow \mathbb{C} \\ t &\longmapsto \delta_{B(F)}^{-1/2}(t) \cdot \int_{u\in N(F)} f(tu)\mathrm{d}u, \end{aligned} \qquad (4.3)$$

where we endow $N(F)$ with the (two-sided) Haar measure such that $N(\mathcal{O}_F)$ has measure 1. The constant term induces a morphism of rings

$$\begin{aligned} \mathcal{H}(G,K) &\longrightarrow \mathcal{H}(T(F), T(\mathcal{O}_F)) \\ f &\longmapsto f^{(B)}, \end{aligned}$$

where $\mathcal{H}(T(F), T(\mathcal{O}_F))$ is the convolution algebra of functions $T(F) \to \mathbb{C}$ with compact support that are both left and right $T(\mathcal{O}_F)$-invariant. Since $T(F)$ is commutative, a function $T(F) \to \mathbb{C}$ is left $T(\mathcal{O}_F)$-invariant if and only if it is right $T(\mathcal{O}_F)$-invariant, and there is no difference between left and right cosets. By applying the valuation to each coordinate in $T(F)$, we obtain an isomorphism

$$\begin{aligned} \mathrm{val}^n\colon T(F)/T(\mathcal{O}_F) &\xrightarrow{\sim} \mathbb{Z}^n, \\ \mathrm{diag}(x_1, \ldots, x_n) &\longmapsto (\mathrm{val}(x_1), \ldots \mathrm{val}(x_n)), \end{aligned}$$

and an isomorphism of $\mathbb{C}$-algebras

$$\begin{aligned} \mathbb{C}[\mathbb{Z}^n] &\xrightarrow{\sim} \mathcal{H}(T(F), T(\mathcal{O}_F)), \\ \sum_{\lambda \in \mathbb{Z}^n} a_\lambda \cdot \lambda &\longmapsto (t \mapsto a_{\mathrm{val}^n(t)}). \end{aligned} \tag{4.4}$$

We identify the group algebra $\mathbb{C}[\mathbb{Z}^n]$ with the polynomial algebra $\mathbb{C}[X_1^{\pm 1}, X_2^{\pm 1}, \ldots, X_n^{\pm 1}]$. The permutation group $\mathfrak{S}_n$ on n letters acts on this algebra by permuting the variables X_i. Satake's main theorem states that composition of the constant term with (4.4) is injective and has image equal to the subalgebra of $\mathfrak{S}_n$-invariants:

Theorem 4.16 (The Satake isomorphism)**.** *The constant term morphism $f \mapsto f^{(B)}$ induces an isomorphism*

$$\mathcal{S} \colon \mathcal{H}(G, K) \xrightarrow{\sim} \mathbb{C}[X_1^{\pm 1}, X_2^{\pm 1}, \ldots, X_n^{\pm 1}]^{\mathfrak{S}_n}.$$

Consequently any unramified irreducible representation π of $\mathrm{GL}_n(F)$ corresponds to a simple module V of the algebra $\mathbb{C}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]^{\mathfrak{S}_n}$. Since this algebra is commutative, such a module is 1-dimensional over $\mathbb{C}$ and corresponds to a maximal ideal

$$\mathfrak{m}_\pi \in \operatorname{spec\,max}(\mathbb{C}[X_1^{\pm 1}, X_2^{\pm 1}, \ldots, X_n^{\pm 1}]^{\mathfrak{S}_n}),$$

which we will henceforward call the *Satake parameter* of π. Viewing the above space of maximal ideals as a variety over $\mathbb{C}$, it is nothing but $\mathbb{C}^{\times,n}/\mathfrak{S}_n$. The upshot is that the unramified irreducible representations π of $\mathrm{GL}_n(F)$ correspond to unordered sequences of n non-zero complex numbers x_i. Attaching to the sequence x_i the unique semi-simple conjugacy class γ_π in $\mathrm{GL}_n(\mathbb{C})$ whose eigenvalues are the x_i, we obtain

Theorem 4.17 (Unramified local Langlands correspondence)**.** *The mapping $\pi \mapsto \gamma_\pi$ sets up a bijection between the isomorphism classes of unramified irreducible representations of $\mathrm{GL}_n(\mathbb{F})$ and semi-simple n-dimensional representations of the group $\mathrm{Frob}_F^{\mathbb{Z}}$.*

An informal introduction to the dual group

Although, strictly speaking, for the group $\mathrm{GL}_n(F)$ the above shows that one can get around it, I believe it is instructive to review the construction from the previous section from a somewhat higher and more abstract perspective. Moreover I think the dual group is one of the crucial ideas of Langlands when he stated his conjecture. Since we have not introduced reductive groups and their classification with root systems, and we do not want to assume this to be known, the discussion that follows will necessarily be sketchy and imprecise. The intention is that the reader will nevertheless get some "cultivation" out of it, and if he or she is interested will read the more serious references on this topic, such as the paper of Borel in PSPUM 33.

We begin with some preliminaries on algebraic tori. A *torus* T over a field F is a commutative group variety that over a finite separable extension E of F is isomorphic to a product of copies of $\mathbb{G}_{\mathrm{m}}$. In case $E = F$, so when $T \cong (\mathbb{G}_{\mathrm{m}})^n$ for some n, then we call the torus *split*. A typical example of a non-split torus is the group $U(1)$, obtained from a quadratic extension E/F as the kernel of the norm character $\mathrm{Res}_{E/F}\mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}$,

where $\mathrm{Res}_{E/F}$ is restriction of scalars. Since in our context we only work with GL_n, we can mostly ignore the non-split tori. To a torus T we may attach two important $\mathbb{Z}$-lattices which compare T with $\mathbb{G}_{\mathrm{m}}$, namely the *cocharacter lattice* $X_*(T) = \mathrm{Hom}_F(\mathbb{G}_{\mathrm{m}}, T)$ and the *character lattice* $X^*(T) = \mathrm{Hom}_F(T, \mathbb{G}_{\mathrm{m}})$.

Theorem 4.18. *The category of split tori over a field is equivalent to the category of finite free $\mathbb{Z}$-modules, via the functor $T \mapsto X_*(T)$. The category of split tori is also anti-equivalent to the category of finite free $\mathbb{Z}$-modules via the functor $T \mapsto X^*(T)$.*

In case of non-split tori, one can also make an equivalence to the category of finite free $\mathbb{Z}$-modules equipped with an action of $\mathrm{Gal}(\overline{F}/F)$. But, as explained above, we will not need that. If Λ is a finite free $\mathbb{Z}$-module, the functor $R \mapsto \Lambda \otimes_{\mathbb{Z}} R^\times$ is representatable by an algebraic torus T_Λ. Explicitly, Λ is isomorphic to $\mathbb{Z}^r$ for some r, and via this isomorphism, T_Λ is nothing but $\mathbb{G}_{\mathrm{m}}^r$. The significance of the (co)character lattice is mostly that it provides a very convenient way to describe the set of morphisms between two tori. Moreover, Theorem 4.18 makes it clear that there exists a duality on the category of tori. Namely, if T is torus, we know that there exists another torus T' such that the character lattice of T' coincides with the cocharacter lattice of T. On the category of finite free $\mathbb{Z}$-modules, this dual is simply the duality that takes a lattice Λ to the dual lattice $\mathrm{Hom}(\Lambda, \mathbb{Z})$. Even though on first sight it is a bit strange, we can furthermore vary the base field. For instance we may take a split torus T over the field F, pass to its cocharacter lattice Λ, take a field C that is unrelated to F, and consider the corresponding (dual if you want) torus over C. Since we look at representations with complex coefficients, we want to take the dual torus $\widehat{T}$ over $\mathbb{C}$, even though the (split) torus T is defined over the unrelated p-adic field $\mathbb{Q}_p$. Similarly, when looking at ℓ-adic representations, it may be natural to consider the dual torus $\widehat{T}$ over $\overline{\mathbb{Q}}_\ell$.

Let T/F be a split torus, then

$$\begin{aligned}&\mathrm{Hom}_{\text{smth, unr.}}(T(F), \mathbb{C}^\times) = \mathrm{Hom}_{\text{smth, unr.}}(T(F)/T(\mathcal{O}_F), \mathbb{C}^\times)\\ &= \mathrm{Hom}(X_*(T), \mathbb{C}^\times) = \mathrm{Hom}(X_*(T), \mathbb{Z}) \otimes \mathbb{C}^\times = X^*(\widehat{T}) \otimes \mathbb{C}^\times = \widehat{T}.\end{aligned}$$

Thus, stated in this way, points in the dual torus *are* the unramified representations of $T(F)$. Moreover, from the last equality in the above equation, for us it is natural to have $\widehat{T}$ over $\mathbb{C}$ (since we look at *complex* characters).

I believe it was Langlands who extended the above duality extends to the category of reductive groups over a field. To any reductive group G over F, let's say for simplicity that G is split, we can attach a complex dual group $\widehat{G}$. Here are some examples of reductive groups with their corresponding dual groups

Group	Dual group
GL_n	$\mathrm{GL}_n(\mathbb{C})$
SO_{2n+1}	$\mathrm{Sp}_{2n}(\mathbb{C})$
SO_{2n}	$\mathrm{SO}_{2n}(\mathbb{C})$
Sp_{2n}	$\mathrm{SO}_{2n+1}(\mathbb{C})$
GSp_{2n}	$\mathrm{GSpin}_{2n+1}(\mathbb{C})$

If T is a maximal torus in G, then $\widehat{T}$ can be viewed (up to conjugacy) as a maximal torus in the dual group $\widehat{G}$. In the computation from the previous section we worked with

the group GL_n over F. The dual group of GL_n is $\mathrm{GL}_n(\mathbb{C})$ (the group is "self-dual"). At the end of our computation we saw that the Satake parameter of an unramified representation naturally lives in the space $\widehat{T}/\mathfrak{S}_n$. The permutation group $\mathfrak{S}_n$ should here be viewed naturally as the *Weyl group* of $\widehat{T}$ in $\widehat{G}$, and the observation is that the space $\widehat{T}/\mathfrak{S}_n$ coincides with the space of semi-simple conjugacy classes in $\widehat{G}$. In the case of GL_n we saw that our Satake parameter was an unordered tuple of n non-zero complex numbers $x_1, x_2, \ldots, x_n$. The corresponding semi-simple conjugacy class in $\mathrm{GL}_n(\mathbb{C})$ is precisely the one whose eigenvalues are $x_1, x_2, \ldots, x_n$. Loosely speaking, the idea is that these conjugacy classes arise from some morphism ϕ from the local Galois group[1] to the dual group. Hence the idea is that, similar to the case of tori, the representations of reductive groups should correspond to Galois representations into the dual group.

4.4 Ramified representations

The goal of this section is to discuss a number of ramified representations. In a later section, after having discussed Weil–Deligne representations, the goal is to come back to these examples, and explain for these examples the corresponding representation on the Galois side.

The Steinberg representation

Arguably the first and simplest example of a ramified representation is the Steinberg representation. Every reductive group has such a representation.

Let's first discuss the Steinberg representation for the group $\mathrm{GL}_2(\mathbb{Q}_p)$. Let $B = \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2$ the Borel subgroup of upper triangular matrices. The quotient GL_2/B is naturally isomorphic to the space of lines passing through the origin in $\mathbb{A}^2$ (since B is the stabilizer of one such a line and GL_2 acts transitively). Hence $\mathrm{GL}_2/B = \mathbb{P}^1$, where GL_2 acts on $\mathbb{P}^1$ through its usual action. Consider the space $C^\infty(\mathbb{P}^1(\mathbb{Q}_p))$ of locally constant functions $f\colon \mathbb{P}^1(\mathbb{Q}_p) \to \mathbb{C}$ on which $\mathrm{GL}_2(\mathbb{Q}_p)$ acts by translations on the right: ${}^g f(x) := f(xg^{-1})$ for all $g \in \mathrm{GL}_2(\mathbb{Q}_p)$ and $f \in C^\infty(\mathbb{P}^1(\mathbb{Q}_p))$. Then $C^\infty(\mathbb{P}^1(\mathbb{Q}_p))$ is a smooth and admissible representation of $\mathrm{GL}_2(\mathbb{Q}_p)$, but notice that it is not irreducible. Namely inside $C^\infty(\mathbb{P}^1(\mathbb{Q}_p))$ we have the subspace $\mathbf{1} \subset C^\infty(\mathbb{P}^1(\mathbb{Q}_p))$ of constant functions, $\mathbb{P}^1(\mathbb{Q}_p) \ni x \mapsto c$, for a fixed constant $c \in \mathbb{C}$. Any translation of a constant function is again constant, so $\mathbf{1}$ is indeed a stable subspace of $C^\infty(\mathbb{P}^1(\mathbb{Q}_p))$. In particular the quotient $C^\infty(\mathbb{P}^1(\mathbb{Q}_p))/\mathbf{1}$ is a $\mathrm{GL}_2(\mathbb{Q}_p)$-representation as well. This representation is irreducible (Exercise 4.31), and it is the *Steinberg* representation of $\mathrm{GL}_2(\mathbb{Q}_p)$.

For $n > 2$ the definition of the Steinberg representation is similarly a space of locally constant function on a Grassman variety attached to GL_n, modulo all the subspaces that are obviously invariant, but a bit more involved. We first need to discuss some background information on parabolic subgroups of GL_n. A *parabolic subgroup* $P \subset \mathrm{GL}_n$ is by definition a connected subgroup such that the quotient variety GL_n/P is projective; the parabolic subgroup P is called a *Borel subgroup* if it is minimal for this property; or, which turns out to be equivalent, if P is a successive extension of $\mathbb{G}_\mathrm{m}$'s and $\mathbb{G}_\mathrm{a}$'s. In GL_n the standard

[1] To make this statement correct, we actually have to replace the Galois group by the *Weil group*, introduced in Section 3.6.

example of a Borel subgroup is the group B of upper triangular matrices B^+; another Borel subgroup is the group of lower triangular matrices B^-, and for any $g \in \mathrm{GL}_n(\mathbb{Q})$, the subgroup $gB^+g^{-1} \subset \mathrm{GL}_n$ is a Borel subgroup as well. In fact, all Borel subgroups are conjugate, so they are all of this form. A connected subgroup of GL_n is parabolic if and only if it contains a Borel subgroup. From now on let us fix one Borel and work henceforward with this fixed choice. We take $B = B^+ \subset \mathrm{GL}_n$ the group of upper triangular matrices. By convention, we call a parabolic subgroup P of GL_n *standard* if $B \subset P$. These groups all turn out to be of the upper block triangular form

$$P = \begin{pmatrix} A_1 & * & * & * \\ & A_2 & * & * \\ & & \ddots & * \\ & & & A_n \end{pmatrix}$$

where $r \in \mathbb{Z}_{\geq 0}$ is some integer, where $n_1, \ldots, n_r$ are all positive integers with $n = n_1 + \ldots + n_r$, where A_i is a matrix in GL_{n_i}, where the $*$'s indicate that those entries of the matrix can be anything and where the entries on the left below the bocks A_i are all 0. Thus, for every ordered partition $n = n_1 + n_2 + \ldots + n_r$ with positive numbers n_i the group GL_n has a standard parabolic subgroup as defined above, and these are all of them, so you can also take this as a definition. For any such $P \subset \mathrm{GL}_n(F)$ the quotient GL_n/P is projective and the space $\mathrm{GL}_n/P(F)$ is compact, and we can consider the space C_P of locally constant functions $f\colon \mathrm{GL}_n/P(F) \to \mathbb{C}$ on it. This space C_P again carries a representation of $\mathrm{GL}_n(F)$, acting by translations on the right as before in the GL_2 case. If P, P' are two parabolic subgroups of GL_n such that the partition corresponding to P is a refinement of the partition corresponding to P', we have an inclusion $P \subset P'$, a map $\mathrm{GL}_n/P(F) \to \mathrm{GL}_n/P'(F)$ and an induced map $C_{P'} \to C_P$. In particular, the spaces C_P are not irreducible if P has a refinement. To define the Steinberg representation St of $\mathrm{GL}_n(F)$, we consider the space C_B and let U be the subspace of C_B generated (as a representation) by all the subspaces C_P, where $P \subset \mathrm{GL}_n$ runs over all the standard parabolic groups with $P \neq B$. Then $U \subset C_B$ is a stable subspace, and the quotient C_B/U turns out to be irreducible. This is the *Steinberg representation.*

Remark 4.19. There is also a variant on the above construction, where instead of the Borel subgroup B you consider another parabolic subgroup, say P_0, which is not a Borel subgroup; and run the above construction with P_0 in place of B. Then you also get an irreducible representation, call it V_{P_0} of $\mathrm{GL}_n(F)$ which is smooth and admissible. Unless the representation that you get is one-dimensional, V_{P_0} is another example of a ramified representation. However, V_{P_0} is usually of less interest than the Steinberg representation, since it does not occur as a local component of discrete automorphic representations.

Cuspidal representations

We have seen that one way to construct admissible representations of $\mathrm{GL}_n(F)$ is by parabolic induction from characters of a Borel subgroup. In a similar way, one can construct admissible representations of $\mathrm{GL}_n(F)$ starting from irreducible representations of groups $\mathrm{GL}_m(F)$ with $m < n$. In the remainder of this section, we will study irreducible

admissible representations that do *not* arise as irreducible constituents of any representation arising from parabolic induction. These representations are called *cuspidal*. We will now give a precise definition of this notion.

Let $P \subset \mathrm{GL}_n$ be a standard parabolic subgroup corresponding to the partition $n = n_1 + n_2 + \ldots + n_r$ (see the previous section). Attached to P, there is the *Levi decomposition* $P = MN$, where M is the group $\mathrm{GL}_{n_1} \times \mathrm{GL}_{n_2} \times \cdots \mathrm{GL}_{n_r}$, embedded diagonally by blocks in GL_n, and N is the subgroup of P consisting of matrices that are the identity inside these blocks. The subgroup N is called the *unipotent radical* of P; it is normal in P, and there is a natural isomorphism $M \xrightarrow{\sim} P/N$.

Definition 4.20. Let F be a p-adic field. The *Jacquet module* (π_N, V_N) of an admissible representation (π, V) of $\mathrm{GL}_n(F)$ is the largest quotient of V on which N acts trivially. In other words, V_N is the quotient of V by the $\mathbb{C}$-linear subspace generated by all elements $v - nv$ with $v \in V$ and $n \in N(F)$.

If (π, V) is an admissible representation of $G = \mathrm{GL}_n(F)$, then the Jacquet module (π_N, V_N) is an admissible representation of $M = M(F)$. Sending (π, V) to (π_N, V_N) is a functor from the category of admissible representations of G to the category of admissible representations of M. This functor is left adjoint to parabolic induction (Exercise 4.35): for all admissible representations π of G and all admissible representations ρ of M, we have a natural isomorphism

$$\mathrm{Hom}_M(\pi_N, \rho) \cong \mathrm{Hom}_G(\pi, \mathrm{Ind}_P^G(\rho)).$$

Definition 4.21. Let (π, V) be an irreducible admissible representation of $\mathrm{GL}_n(F)$. We say that (π, V) is *cuspidal* if for all standard parabolic subgroups $P = MN \subset \mathrm{GL}_n$ with $P \neq \mathrm{GL}_n$, the representation (π_N, V_N) of M is trivial.

Slightly more explicitly, (π, V) is cuspidal if for every r-tuple $(n_1, \ldots, n_r)$ with $n_i \geq 1$ and $r \geq 2$ the representation (π_N, V_N) of M is trivial, where P is the standard parabolic subgroup corresponding to the partition $(n_1, \ldots, n_r)$, N is the unipotent radical of P and $M \simeq P/N$ is the diagonally embedded product $\mathrm{GL}_{n_1}(F) \times \cdots \times \mathrm{GL}_{n_r}(F)$.

Remark 4.22. In the literature, cuspidal representations are often called *supercuspidal*.

In Exercise 4.27, you will show that for $\mathrm{GL}_2(\mathbb{Q}_p)$, the Jacquet module of the Steinberg representation is one-dimensional. In fact this is true for all groups $\mathrm{GL}_n(F)$, and is not very difficult to prove. In particular, the Steinberg representation is not cuspidal. Similarly, by Exercise 4.29 the unramified representations are not cuspidal either.

Remark 4.23. In light of the local Langlands correspondence, the cuspidal representations correspond to the irreducible representations on the Galois side. Since any reducible representation can be decomposed into irreducible ones of lower dimension, one may try, when proving the local Langlands conjecture, to reduce the statement to the "cuspidal $\leftrightarrow$ irreducible" case. In fact, this is how all the known proofs of the local Langlands conjecture for $\mathrm{GL}_n(F)$ work.

The cuspidal representations of $\mathrm{GL}_n(F)$ are harder to construct than the non-cuspidal ones. In the remainder of this subsection, we will describe how to construct a family of examples for $\mathrm{GL}_2(F)$.

First, we consider a finite field k of q elements, and we consider complex representations of the finite group $G = \mathrm{GL}_2(k)$. We consider the subgroups

$$B = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, \quad N = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}, \quad Z = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \;\middle|\; a \in k^\times \right\}.$$

Just as in the case of local fields, one way to obtain representations of G is by induction from characters of B. In this way, one always gets representations that have non-trivial N-invariant subspaces. The representations that do not have this property are slightly more subtle to define.

Definition 4.24. A finite-dimensional representation ρ of G is *cuspidal* if the restriction of ρ to N does not contain the trivial representation of N.

(In other words, ρ is cuspidal if and only if the subspace of N-invariants vanishes.)

Let k' be a quadratic extension of k (unique up to isomorphism). By choosing a k-basis of k', we obtain embeddings $k' \hookrightarrow \mathrm{Mat}_2(k)$ and $k'^\times \hookrightarrow \mathrm{GL}_2(k)$. We write E for the image of $k'^\times$ in G; then E contains Z as a subgroup of index $q+1$.

We choose characters

$$\theta \colon E \to \mathbb{C}^\times$$

and

$$\psi \colon k \to \mathbb{C}^\times$$

such that ψ is non-trivial and θ satisfies $\theta^q \neq \theta$. We define a character

$$\begin{aligned} \theta * \psi \colon ZN &\longrightarrow \mathbb{C}^\times \\ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} &\longmapsto \theta(a)\psi(b). \end{aligned}$$

We consider the representations $\mathrm{Ind}_E^G \theta$ of dimension $(G : E) = q(q-1)$ and $\mathrm{Ind}_{ZN}^G (\theta * \psi)$ of dimension $(G : ZN) = (q+1)(q-1)$.

Theorem 4.25. *1. There is a decomposition*

$$\mathrm{Ind}_{ZN}^G (\theta * \psi) \cong \mathrm{Ind}_E^G \theta \oplus \pi_\theta$$

where π_θ is an irreducible cuspidal representation of G of dimension $q-1$.

2. *If θ' is another character of E with $\theta'^q \neq \theta'$, then π_θ and $\pi_{\theta'}$ are isomorphic if and only if $\theta' = \theta$ or $\theta' = \theta^q$.*

3. *Up to isomorphism, all irreducible cuspidal representations of G arise as π_θ for some character θ of E with $\theta^q \neq \theta$.*

We now shift our attention to the p-adic field F. Let F' be an unramified quadratic extension of F (unique up to isomorphism). Similarly to the above construction, we choose an F-basis of F', giving embeddings $F' \to \mathrm{Mat}_2(F)$ and $F'^\times \to \mathrm{GL}_2(F)$. We write E for the image of F' in $\mathrm{GL}_2(F)$.

We consider a character

$$\chi \colon F'^\times \to \mathbb{C}^\times$$

that is trivial on the group $\{x \in \mathcal{O}_{F'}^\times \mid x \equiv 1 \pmod{\mathfrak{p}}_{F'}\}$, where $\mathfrak{p}_{F'}$ is the maximal ideal of $\mathcal{O}_{F'}^\times$. (Such characters are said to be of "level 0".) Let σ be the non-trivial element of $\mathrm{Gal}(F'/F)$, and let $\chi^\sigma = \chi \circ \sigma$. Suppose that $\chi \neq \chi^\sigma$. Since χ has level 0, it induces a character

$$\tilde{\chi}\colon (\mathcal{O}_{F'}/\mathfrak{p}_{F'})^\times \to \mathbb{C}^\times.$$

One can show that $\tilde{\chi}$ satisfies $\tilde{\chi}^q \neq \tilde{\chi}$. Therefore the above construction gives an irreducible cuspidal representation

$$\tilde{\lambda}_{\tilde{\chi}}\colon \mathrm{GL}_2(\mathcal{O}_F/\mathfrak{p}_F) \to \mathrm{GL}_{q-1}(\mathbb{C}).$$

We inflate this to a representation

$$\lambda_{\tilde{\chi}}\colon \mathrm{GL}_2(\mathcal{O}_F) \to \mathrm{GL}_{q-1}(\mathbb{C}).$$

It follows from the construction that χ and $\lambda_{\tilde{\chi}}$ are compatible in the sense that they agree on the intersection of $\mathrm{GL}_2(\mathcal{O}_F)$ and E in $\mathrm{GL}_2(F)$. Hence there exists a unique representation

$$\begin{aligned}\Lambda_\chi\colon E\,\mathrm{GL}_2(\mathcal{O}_F) &\longrightarrow \mathrm{GL}_{q-1}(\mathbb{C})\\ xy &\longmapsto \chi(x)\lambda_{\tilde{\chi}}(y).\end{aligned}$$

Finally, we define

$$\pi_{F',\chi} = \mathrm{cInd}_{E\,\mathrm{GL}_2(\mathcal{O}_F)}^{\mathrm{GL}_2(F)} \Lambda_\chi.$$

It turns out that this is an irreducible cuspidal representation of $\mathrm{GL}_2(F)$.

4.5 $(\mathfrak{g}, K)$-modules

The Archimedean version of the concept of admissible representations turns out to be more complicated than for locally profinite groups. The main complication is that one either needs to consider representations on Hilbert spaces or Banach spaces, or alternatively (to avoid using functional analysis, which is what we will do) consider actions of Lie algebras and their universal enveloping algebras.

In this section, we write

$$G = \mathrm{GL}_n(\mathbb{R}).$$

We define

$$\mathfrak{g} = \mathrm{Lie}(G) = \mathrm{Mat}_n(\mathbb{R})$$

and

$$K = \mathrm{O}_n(\mathbb{R}).$$

Then K is a maximal compact subgroup of G. There is a natural representation

$$\begin{aligned}G \times \mathfrak{g} &\longrightarrow \mathfrak{g}\\ (g, x) &\longmapsto (\mathrm{Ad}\, g)x,\end{aligned}$$

where $\mathrm{Ad}\colon \mathfrak{g} \to \mathrm{Aut}_{\mathbb{R}}\mathfrak{g}$ is the adjoint representation; since $G = \mathrm{GL}_n(\mathbb{R})$, we can identify $(\mathrm{Ad}\, g)x$ with gxg^{-1} in $\mathrm{Mat}_n(\mathbb{R})$.

There is an *exponential map*

$$\exp\colon \mathfrak{g} \to G;$$

since $G = \mathrm{GL}_n(\mathbb{R})$, this is given by

$$\exp(x) = \sum_{m=0}^{\infty} \frac{1}{m!} x^m.$$

Note that this is not a group homomorphism unless $n \leq 1$. The *complexification* of $\mathfrak{g}$ is the complex Lie algebra

$$\mathfrak{g}_{\mathbb{C}} = \mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C}.$$

A *representation* of $\mathfrak{g}_{\mathbb{C}}$ is a $\mathbb{C}$-vector space V together with an $\mathbb{C}$-linear map

$$\pi \colon \mathfrak{g}_{\mathbb{C}} \to \mathrm{End}_{\mathbb{C}} V$$

satisfying

$$\pi([x, y]) = \pi(x) \circ \pi(y) - \pi(y) \circ \pi(x) \quad \text{for all } x, y \in \mathfrak{g}_{\mathbb{C}}.$$

A fundamental example of such a representation (which is also how the Lie algebra $\mathfrak{g}_{\mathbb{C}}$ will show up in the theory of automorphic forms) is the action of $\mathfrak{g}_{\mathbb{C}}$ on the space $\mathcal{C}^\infty(G)$ of smooth functions $G \to \mathbb{C}$ by (first-order) differential operators. This action is given on $\mathfrak{g}$ by

$$\begin{aligned}(\pi(x)\phi)(g) &= \frac{d}{dt}\phi(g \exp(tx)) \\ &= \lim_{t \to 0} t^{-1}(\phi(g \exp(tx) - \phi(g)) \quad \text{for all } x \in \mathfrak{g}, \phi \in \mathcal{C}^\infty(G), g \in G\end{aligned}$$

and extended to $\mathfrak{g}_{\mathbb{C}}$ by

$$\pi(x + iy)\phi = \pi(x)\phi + i(\pi(y)\phi) \quad \text{for all } x, y \in \mathfrak{g}, \phi \in \mathcal{C}^\infty(G).$$

The following definition is an Archimedean replacement for the notion of a smooth representation of a locally profinite group.

Definition 4.26. A $(\mathfrak{g}, K)$-*module* is a complex vector space V equipped with representations of the group K and of the Lie algebra $\mathfrak{g}$, both denoted by π, such that

- V, viewed as a representation of K, is a direct sum of irreducible continuous finite-dimensional representations of K;
- for all x in the Lie algebra $\mathrm{Lie}(K) \subseteq \mathfrak{g}$, the limit

  $$\frac{d}{dt}(\pi(\exp(tx))v)|_{t=0} = \lim_{t \to 0} \frac{1}{t}\big(\pi(\exp(tx))v - v\big)$$

  (where $\exp \colon \mathfrak{g} \to G$ is the exponential map) exists and is equal to $\pi(x)v$;
- for all $k \in K$ and $x \in \mathfrak{g}$, we have

  $$\pi(k) \circ \pi(x) \circ \pi(k^{-1}) = \pi((\mathrm{Ad}\, k)x).$$

The first condition above is a replacement for the representation of K being continuous; note we have not fixed a topology on V. The other two conditions state in that the actions should be compatible to the largest meaningful extent.

We note that the representation of $\mathfrak{g}$ on a $(\mathfrak{g}, K)$-module V can be extended in a canonical way to a representation of the complexified Lie algebra $\mathfrak{g}_{\mathbb{C}}$.

Definition 4.27. A $(\mathfrak{g}, K)$-module (π, V) is *admissible* if every irreducible continuous finite-dimensional representation of K occurs only finitely many times in V (up to isomorphism).

Theorem 4.28. *There exists an associative (but in general non-commutative and non-unital) $\mathbb{C}$-algebra $\mathcal{H}(G)$ such that every $(\mathfrak{g}, K)$-module is in a natural way a* smooth *representation of $\mathcal{H}(G)$, and this induces an equivalence of categories*

$$\{(\mathfrak{g}, K)\text{-modules}\} \xrightarrow{\sim} \{\text{smooth representations of } \mathcal{H}(G)\}.$$

In the next chapter, we will need the *universal enveloping algebra* of $\mathfrak{g}_{\mathbb{C}}$. This is an associative unital $\mathbb{C}$-algebra $U(\mathfrak{g}_{\mathbb{C}})$ together with a homomorphism

$$\iota \colon \mathfrak{g}_{\mathbb{C}} \to U(\mathfrak{g}_{\mathbb{C}})$$

of complex Lie algebras (*i.e.* a $\mathbb{C}$-linear map satisfying $\iota([x,y]) = \iota(x)\iota(y) - \iota(y)\iota(x)$) such that for every associative unital $\mathbb{C}$-algebra A and every Lie algebra homomorphism $f \colon \mathfrak{g}_{\mathbb{C}} \to A$ there is a unique extension of f to a homomorphism $U(\mathfrak{g}_{\mathbb{C}}) \to A$ of associative unital $\mathbb{C}$-algebras. In particular, every representation of $\mathfrak{g}$ on a $\mathbb{C}$-vector space V extends uniquely to a $U(\mathfrak{g}_{\mathbb{C}})$-module structure on V.

Example 4.29. For $n = 2$, and without complexification for simplicity, we have

$$\mathfrak{g} = \mathbb{R}z \oplus \mathbb{R}\hat{h} \oplus \mathbb{R}\hat{a}_+ \oplus \mathbb{R}\hat{a}_-$$

where

$$z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \hat{h} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \hat{a}_+ = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \hat{a}_- = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

The algebra $U(\mathfrak{g})$ is generated by these elements. They satisfy

$$[\hat{h}, \hat{a}_+] = 2\hat{a}_+, \quad [\hat{h}, \hat{a}_-] = -2\hat{a}_-, \quad [\hat{a}_+, \hat{a}_-] = \hat{h}.$$

We define an element $\Delta \in U(\mathfrak{g})$ by

$$\Delta = -\frac{1}{4}(\hat{h}^2 + 2\hat{a}_+\hat{a}_- + 2\hat{a}_-\hat{a}_+),$$

where we view $\hat{h}$, $\hat{a}_+$ and $\hat{a}_-$ as elements in $U(\mathfrak{g})$ via ι, and where the multiplication takes place in $U(\mathfrak{g})$; note that this is not the same as multiplying the matrices defining these elements!

Theorem 4.30. *For $G = \mathrm{GL}_2(\mathbb{R})$, the centre $Z(U(\mathfrak{g}_{\mathbb{C}}))$ of the $\mathbb{C}$-algebra $U(\mathfrak{g}_{\mathbb{C}})$ is a polynomial ring in two variables generated by z and Δ.*

The above theorem follows from the *Harish-Chandra isomorphism*. We omit the proof, but see Exercise 4.14.

Remark 4.31. One can develop a very similar theory for $\mathrm{GL}_n(\mathbb{C})$ (and also for other Lie groups); in the interest of brevity, we will not do this here.

4.6 The local Langlands correspondence for GL_n

Some useful references for this section are Cogdell's notes [1, Chapters 9 and 10] and Bushnell and Henniart's book [3, Chapters 2–7].

Throughout this section, let F be a p-adic field, and let q be the cardinality of the residue field of F. The local Langlands correspondence will link admissible representations of $\mathrm{GL}_n(F)$ with n-dimensional Weil–Deligne representations of F. Rather than stating directly how to construct an object on one side from an object on the other side, the correspondence identifies objects by means of their *L-functions* and *ϵ-factors*.

L-functions and ϵ-factors of admissible representations

For an admissible representation π of $\mathrm{GL}_n(F)$, one can define an L-function

$$L(\pi, s) \in \mathbb{C}(q^{-s})$$

and an ϵ-factor

$$\epsilon(\pi, s) \in \mathbb{C}[q^s, q^{-s}]^\times.$$

This was first done by Godement and Jacquet, and later in various other ways by Jacquet, Piatetski-Shapiro, Shalika and other authors. Explaining how these L-functions and ϵ-factors are defined is unfortunately beyond the scope of this course; we just give the most important examples to convey an idea of what these quantities look like.

If the admissible representation π is one-dimensional, then it is given by a character $\chi\colon F^\times \to \mathbb{C}^\times$. If χ is unramified and $\varpi \in F^\times$ is a uniformiser, we have (for a suitable choice of the fixed additive character $\psi\colon F \to \mathbb{C}^\times$)

$$\begin{aligned} L(\chi, s) &= (1 - \chi(\varpi)q^{-s})^{-1}, \\ \epsilon(\chi, s) &= q^{s-1/2}\chi(\varpi)^{-1}. \end{aligned}$$

If χ is ramified, then we have

$$L(\chi, s) = 1,$$

and the formula for $\epsilon(\chi, s)$ is more complicated (involving a certain Gauss sum). If π is obtained by parabolic induction from a character χ of the Borel subgroup $B \subset \mathrm{GL}_n(F)$, and if π is irreducible (so we exclude twists of the Steinberg representation), then we have

$$\begin{aligned} L(\pi, s) &= L(\chi_1, s) \dots L(\chi_n, s), \\ \epsilon(\pi, s) &= L(\chi_1, s) \dots L(\chi_n, s). \end{aligned}$$

Finally, if the representation π is cuspidal, then we have

$$L(\pi, s) = 1,$$

so only the ϵ-factor encodes non-trivial information about π.

More generally, one also needs to define, given a *pair* of two admissible representations π of $\mathrm{GL}_n(F)$ and π' of $\mathrm{GL}_{n'}(F)$, an L-function $L(\pi \times \pi', s)$ and an ϵ-factor $\epsilon(\pi \times \pi', s)$. In this notation, the product $\pi \times \pi'$ has *a priori* no meaning of its own; once the Langlands correspondence has been established, it becomes a consequence that there exists an

admissible representation of $\mathrm{GL}_{nn'}(F)$ that deserves the notation $\pi \times \pi'$. Here we content ourselves with explaining what these mean for $n' = 1$, in which case π' is a character χ of $F^\times$. We then define

$$L(\pi \times \chi, s) = L(\chi\pi, s),$$
$$\epsilon(\pi \times \chi, s) = \epsilon(\chi\pi, s),$$

where $\chi\pi$ $(= \pi \times \chi)$ is the admissible representation of $\mathrm{GL}_n(F)$ defined by

$$(\chi\pi)(g) = \chi(\det g)\pi(g).$$

L-functions and ϵ-factors of Weil–Deligne representations

Let (ρ, V, N) be a Weil–Deligne representation of F. Like for admissible representations, one can associate to (ρ, V, N) two fundamental quantities: a L-function

$$L((\rho, V, N), s) \in \mathbb{C}(q^{-s})$$

and an ϵ-factor

$$\epsilon((\rho, V, N), s) \in \mathbb{C}[q^s, q^{-s}]^{-1}.$$

The latter implicitly also depends on the choice of an additive character $\psi\colon F \to \mathbb{C}^\times$.

We first regard (ρ, V) simply as a smooth representation of W_F. We choose a geometric Frobenius element $\phi \in W_F$, and we define the L-function by the usual formula

$$L(\rho, s) = \det(1 - \rho(\phi)q^{-s})^{-1} \in \mathbb{C}(q^{-s}).$$

The ϵ-factor is more complicated and cannot be expressed in a simple formula in general. The fact that there is a "consistent" definition of ϵ-factors at all is already quite deep; this is the content of the following theorem.

Theorem 4.32 (Dwork, Langlands, Deligne)**.** *Let F be a p-adic field, and let $\psi\colon F \to \mathbb{C}^\times$ be a smooth additive character. There exists a unique family of functions*

$$\epsilon(\rho, s) \in \mathbb{C}[q^s, q^{-s}]^\times$$

where E is a finite extension of F inside $\bar{F}$ and ρ is a semi-simple finite-dimensional smooth representation of W_F, such that the following properties are satisfied:

1. *If ρ is one-dimensional and $\chi\colon E^\times \to \mathbb{C}^\times$ is the character corresponding to ρ via the reciprocity isomorphism, then one has*

   $$\epsilon(\rho, s) = \epsilon(\chi, s)$$

   where the right-hand side is the ϵ-factor occurring in the functional equation for χ.

2. *For all ρ_1 and ρ_2 in $\mathcal{G}(E)$, we have*

   $$\epsilon(\rho_1 \oplus \rho_2, s) = \epsilon(\rho_1, s)\epsilon(\rho_2, s).$$

3. *For all finite extensions $K/E/F$ inside $\bar{F}$ and $\rho \in \mathcal{G}(E)$, we have*

   $$\frac{\epsilon(\mathrm{Ind}_{W_K}^{W_E} \rho, s)}{\epsilon(\rho, s)} = \left(\frac{\epsilon(\mathrm{Ind}_{W_K}^{W_E} \mathbf{1}_K, s)}{\epsilon(\mathbf{1}_K, s)}\right)^{\dim \rho}.$$

Remark 4.33. The ϵ-factors depend on the choice of the additive character $\psi\colon F \to \mathbb{C}^\times$. For a finite extension E/F, we fix a non-trivial additive character ψ_E as the composition of ψ with the trace map $E \to F$.

We now take the operator N into account, and make the following definitions (with V^N the kernel of N):

$$\begin{aligned} L((\rho, V, N), s) &= L(\rho|_{V^N}, s), \\ \epsilon((\rho, V, N), s) &= \epsilon(\rho, s)\frac{L(\rho^\vee, 1-s)}{L(\rho, s)}\frac{L(\rho|_{V^N}, 1-s)}{L(\rho^\vee|(V^\vee)^{N^\vee}, s)} \end{aligned}$$

Here $(\rho^\vee, V^\vee, N^\vee)$ is defined as follows: $V^\vee$ is the dual vector space of V, $\rho^\vee$ is the dual representation (inverse transpose on matrices), and $N^\vee$ is the *negative* of the transpose of N.

The local Langlands correspondence

The local Langlands correspondence states that there is a canonical bijection between two sets: on the "automorphic" side we have the set $\mathcal{A}_n(F)$ of isomorphism classes of irreducible admissible representations of $\mathrm{GL}_n(F)$, and on the "Galois" side we have the set $\mathrm{WD}_n(F)$ of isomorphism classes of n-dimensional Weil–Deligne representations of F.

Theorem 4.34 (Local Langlands correspondence)**.** *There exist unique bijections*

$$\begin{aligned} \mathcal{A}_n(F) &\to \mathrm{WD}_n(F) \\ \pi &\mapsto \rho_\pi \end{aligned}$$

with the following properties:

1. *For all $\pi \in \mathcal{A}_n(F)$, $\pi' \in \mathcal{A}_{n'}(F)$ we have*

$$\begin{aligned} L(\pi \times \pi', s) &= L(\rho_\pi \otimes \rho_{\pi'}, s), \\ \epsilon(\pi \times \pi', s) &= \epsilon(\rho_\pi \otimes \rho_{\pi'}, s). \end{aligned}$$

2. *The determinant of ρ_π corresponds to the central character of π via the reciprocity isomorphism rec_F from local class field theory. In particular, for $\chi \in \mathcal{A}_1(F)$, the smooth character $\rho_\chi\colon W_F \to \mathbb{C}^\times$ corresponds to the smooth character $\chi\colon F^\times \to \mathbb{C}^\times$ via this isomorphism.*

3. *The correspondence is compatible with taking duals: $\rho_{\pi^\vee} = \rho_\pi^\vee$.*

4. *For every character $\chi\colon F^\times \to \mathbb{C}^\times$, we have $\rho_{\chi\pi} = \rho_\chi \otimes \rho_\pi$, where $\rho_{\chi\pi}(g) = \chi(\det g)\pi(g)$.*

The following theorem says that the local Langlands correspondence holds when restricting to suitable *cuspidal* representations on the automorphic side and to *irreducible* Weil–Deligne representations (which are just irreducible representations of the Weil group) on the Galois side.

Let $\mathcal{A}_n^0(F)$ be the subset of $\mathcal{A}_n(F)$ consisting of isomorphism classes of *cuspidal* irreducible admissible representations. We denote by $\mathcal{G}(F)$ the set of isomorphism classes of semi-simple finite-dimensional smooth representations of W_F, by $\mathcal{G}_n(F)$ the set of such representations of dimension n, and by $\mathcal{G}_n^0(F)$ the subset of irreducible ones.

Theorem 4.35 (Harris, Taylor; Henniart)**.** *There exist unique bijections*

$$\mathcal{A}_n^0(F)_f \to \mathcal{G}_n^0(F)$$
$$\pi \mapsto \rho_\pi$$

(where the subscript f denotes irreducible admissible representations of $\mathrm{GL}_n(F)$ with central character of finite order) satisfying the properties of the local Langlands correspondence.

In fact, the full local Langlands correspondence can be deduced from this.

4.7 Exercises

Haar measures and Hecke algebras

Exercise 4.1. Let G be locally compact topological group, let μ be a left Haar measure on G, and let ν be a right Haar measure on G. Using the notation introduced in the text, show that the left invariance of μ and the right invariance of ν can be expressed as

$$\int_{x\in G} f(gx)d\mu(x) = \int_{x\in G} f(x)d\mu(x),$$
$$\int_{x\in G} f(xg)d\nu(x) = \int_{x\in G} f(x)d\nu(x)$$

for all continuous functions $f\colon G \to \mathbb{R}$ with compact support.

Exercise 4.2. Let G be a locally compact topological group, and let μ and ν be left and right Haar measure on G, respectively. Let $\delta_G\colon G \to \mathbb{R}_{>0}$ be the modular function as defined via μ by the equation

$$\delta_G(g)\cdot \mu g = \mu \quad \text{for all } g \in G.$$

(a) Show that δ_G also satisfies

$$g\nu = \delta_G(g)\cdot \nu \quad \text{for all } g \in G.$$

(b) Show that the elements $\delta_G^{-1}\mu$ and $\delta_G\nu$ in $\mathcal{C}_c(G)^\vee$ defined by

$$(\delta_G^{-1}\mu)(f) = \int_{x\in X} f(x)\delta_G(x)^{-1}d\mu(x) \quad \text{and} \quad (\delta_G\nu)(f) = \int_{x\in X} f(x)\delta_G(x)d\nu(x)$$

for $f \in \mathcal{C}_c(G)$ are right and left Haar measures, respectively.

Exercise 4.3. Let G be a compact topological group.

(a) Show that the group G is unimodular.

(b) Show that G has finite total volume for its Haar measure.

Exercise 4.4. Prove Lemma 4.2.

Exercise 4.5. Let G be a finite group (equipped with the discrete topology).

(a) Prove that the map μ sending a function $f\colon G \to \mathbb{R}$ to $\frac{1}{\#G}\sum_{x\in G} f(x)$ is a Haar measure on G.

(b) Prove that the Hecke algebra $\mathcal{H}(G)$ (with respect to the above Haar measure) is canonically isomorphic to the group algebra $\mathbb{C}[G]$.

Exercise 4.6. Consider the group $G = \mathrm{GL}_n(\mathbb{R})$ with coordinates $x_{i,j}$ for $1 \leq i, j \leq n$. Show that $\left|\det(x_{i,j})_{i,j=1}^n\right|^{-n} \prod_{i,j=1}^n dx_{i,j}$ is a (two-sided) Haar measure on G.

Exercise 4.7. Let B be the group of upper triangular matrices $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbb{Q}_p)$, and let $B_0 = B \cap \mathrm{GL}_2(\mathbb{Z}_p) = \left(\begin{smallmatrix} \mathbb{Z}_p^\times & \mathbb{Z}_p \\ 0 & \mathbb{Z}_p^\times \end{smallmatrix}\right)$.

(a) Let μ be the unique left Haar measure on B such that $\mu(B_0) = 1$. For all $r, s, t \in \mathbb{Z}$, compute $\mu(B_{r,s,t})$, where $B_{r,s,t}$ is the compact open subset of B defined by

$$B_{r,s,t} = \begin{pmatrix} p^r\mathbb{Z}_p^\times & p^s\mathbb{Z}_p \\ 0 & p^t\mathbb{Z}_p^\times \end{pmatrix}.$$

(b) Prove that the modular function δ_B of B is given by

$$\delta_B\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \frac{|d|_p}{|a|_p}.$$

Smooth and admissible representations

Exercise 4.8. Let G be a locally profinite group, and let $\pi\colon G \to \mathrm{Aut}_{\mathbb{C}}(V)$ be a complex representation of G. Show that (π, V) is smooth if and only if the map

$$\begin{aligned} G \times V &\to V \\ (g, v) &\mapsto \pi(g)v \end{aligned}$$

is continuous for the discrete topology on V.

Exercise 4.9. Let p be a prime number, and let $G = \mathrm{GL}_n(\mathbb{Q}_p)$.

(a) Let K be a compact open subgroup of G. Show that the set G/K is countable.

(b) Let (π, V) be an irreducible smooth representation of G. Show that the dimension of V is countable.

Exercise 4.10. Let G be a profinite group. Let (π, V) be a smooth representation of G. Prove the following statements:

(i) If π is irreducible, then the homomorphism $G \to \mathrm{Aut}_{\mathbb{C}}(V)$ factors through a finite quotient of G.

(ii) If π is irreducible, then V has finite dimension.

(iii) The representation V is unitary, *i.e.* there exists a positive definite Hermitean product $\langle\cdot,\cdot\rangle$ on V such that $\langle gv, gw\rangle = \langle v, w\rangle$ for all $v, w \in V$ and all $g \in G$.

(iv) π is semi-simple.

Exercise 4.11. Let G be a locally profinite group. Let $\mathcal{C}(G)$ be the $\mathbb{C}$-vector space of all locally constant functions $G \to \mathbb{C}$, viewed as a representation of G via the right action of G on itself. Is the representation $\mathcal{C}(G)$ smooth? If so, is it admissible?

Exercise 4.12. Let G be a locally profinite group, and let π be an admissible representation of G. Let $f \in \mathcal{H}(G)$ be a locally constant compactly supported function. Show that the $\mathbb{C}$-linear map

$$V \to V$$
$$v \mapsto \pi(f)v$$

defined in Theorem 4.6 has finite rank.

Exercise 4.13. Let G be a locally profinite group, and let (π, V) be a smooth representation of G.

(a) Show that for every compact open subgroup $K \subseteq G$, the space of invariants V^K is a module for the (unital) $\mathbb{C}$-algebra $\mathcal{H}(G, K)$.

(b) Show that the following conditions are equivalent:

(i) (π, V) is irreducible;

(ii) V is non-zero, and for every compact open subgroup $K \subseteq G$, the $\mathcal{H}(G, K)$-module V^K is either zero or simple.

$(\mathfrak{g}, K)$-modules

Exercise 4.14. Verify that the elements z and Δ of $U(\mathfrak{g}_{\mathbb{C}})$ defined in Example 4.29 lie in the centre of $U(\mathfrak{g}_{\mathbb{C}})$.

Exercise 4.15. Let $\mathfrak{g} = \mathrm{Lie}(\mathrm{GL}_1(\mathbb{R})) = \mathbb{R}$ and $K = \mathrm{O}_1(\mathbb{R}) = \{\pm 1\}$. Give an elementary classification of $(\mathfrak{g}, K)$-modules and of admissible $(\mathfrak{g}, K)$-modules.

In the exercises below, we take $G = \mathrm{GL}_2(\mathbb{R})$, so $K = \mathrm{O}_2(\mathbb{R}) = \mathrm{SO}_2(\mathbb{R}) \sqcup \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\mathrm{SO}_2(\mathbb{R})$ and $\mathfrak{g} = \mathrm{Lie}(G) = \mathrm{Mat}_2(\mathbb{R})$. For $\theta \in \mathbb{R}$, we write $r_\theta = \left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right) \in \mathrm{SO}_2(\mathbb{R})$. We write $P = \left(\begin{smallmatrix} 1 & 1 \\ i & -i \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{C})$, so that $r_\theta = P\left(\begin{smallmatrix} \exp(-i\theta) & 0 \\ 0 & \exp(i\theta) \end{smallmatrix}\right)P^{-1}$, and we define elements $z, a_+, a_-, h \in \mathfrak{g}_{\mathbb{C}}$ as the images of the elements considered in Example 4.29 under the map $x \mapsto PxP^{-1}$, so that

$$z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad a_\pm = \frac{1}{2}\begin{pmatrix} 1 & \pm i \\ \pm i & -1 \end{pmatrix}, \quad h = [a_+, a_-] = i\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Exercise 4.16. Let k be a non-negative integer, and let V_k be the k-th symmetric power of the standard two-dimensional representation of G, *i.e.* V_k is the $\mathbb{C}$-vector space of homogeneous polynomials of degree k in $\mathbb{C}[x, y]$ and the action of G is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} x^m y^n = (ax + cy)^m (bx + dy)^n \quad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G.$$

Show that there is a natural way to view V_k as a $(\mathfrak{g}, K)$-module (π_k, V_k) and that there exists a $\mathbb{C}$-basis $(v_{-k}, v_{-k+2}, \ldots, v_{k-2}, v_k)$ of V_k such that the action of K is given by

$$\pi_k(r_\theta)v_l = \exp(-il\theta)v_l \quad \text{and} \quad \pi_k\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}v_l = v_{-l}$$

and the action of $\mathfrak{g}$ is given by

$$\pi_k(a_\pm)v_l = \frac{k \mp l}{2} v_{l\pm 2} \quad \text{and} \quad \pi_k(h)v_l = lv_l.$$

Exercise 4.17. Let k be an integer with $k \geq 2$, and let V_k be a $\mathbb{C}$-vector space with basis $\{v_l\}_{l \in S_k}$ indexed by the countable set $S_k = \{l \in \mathbb{Z} : |l| \geq k, l \equiv k \pmod 2\}$.

(a) Show that there is a representation π_k of K on V_k given by

$$\pi_k(r_\theta)v_l = \exp(-il\theta)v_l \quad \text{and} \quad \pi_k\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} v_l = v_{-l}.$$

(b) Show that this representation can be extended to a $(\mathfrak{g}, K)$-module structure on V_k satisfying

$$\pi_k(a_\pm)v_l = \frac{k \pm l}{2} v_{l\pm 2} \quad \text{and} \quad \pi_k(h)v_l = lv_l.$$

(The $(\mathfrak{g}, K)$-module (π_k, V_k) corresponds to the *discrete series representation* of weight k of $\mathrm{GL}_2(\mathbb{R})$.)

Exercise 4.18. Let $\chi_1, \chi_2 \colon \mathbb{R}^\times \to \mathbb{C}^\times$ be two continuous group homomorphisms, and let $\epsilon = \chi_1(-1)\chi_2(-1)$.

(a) Show that for every $l \in \mathbb{Z}$ with $(-1)^l = \epsilon$, there exists a unique continuous function

$$\phi_l \colon G \to \mathbb{C}^\times$$

satisfying

$$\phi_l\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} r_\theta\right) = \exp(-il\theta)\chi_1(a)\chi_2(d) \quad \text{for all } a, d \in \mathbb{R}^\times, b, \theta \in \mathbb{R}.$$

(b) Show that the $\mathbb{C}$-vector space V_{χ_1,χ_2} spanned by the functions ϕ_l for all $l \in \mathbb{Z}$ with $(-1)^l = \epsilon$ is in a natural way a representation of K.

(c) Show that V_{χ_1,χ_2} also has a natural $(\mathfrak{g}, K)$-module structure, and determine the action of the operators $a_\pm$ and h on V_{χ_1,χ_2} with respect to the basis $\{\phi_l\}$.

(The $(\mathfrak{g}, K)$-module V_{χ_1,χ_2} corresponds to the *principal series representation* attached to the pair (χ_1, χ_2); this representation is induced from the character $\chi \colon \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \to \mathbb{C}^\times$ sending $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ to $\chi_1(a)\chi_2(b)$.)

Unramified representations

In the exercises below F is a p-adic local field.

Exercise 4.19. Show that the algebra $\mathcal{H}(\mathrm{GL}_n(F), \mathrm{GL}_n(\mathcal{O}_F))$ is commutative.

Exercise 4.20. Show that the constant term mapping $f \mapsto f^{(B(F))}$ is indeed a morphism of rings.

Exercise 4.21. Show that if you remove the normalizing factor $\delta_{B(F)}^{-1/2}(t)$ from Equation (4.3), then you also get a ring homomorphism

$$\mathcal{H}(G,K) \to \mathbb{C}[X_1^{\pm 1}, X_2^{\pm 1}, \ldots, X_n^{\pm 1}],$$

but this map (the 'unnormalized Satake transform') does not have image in the subalgebra of $\mathfrak{S}_n$-invariants.

Exercise 4.22. Compute the Satake transform of the characteristic function of the double coset $\mathrm{GL}_2(\mathbb{Z}_p) \cdot \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot \mathrm{GL}_2(\mathbb{Z}_p) \subset \mathrm{GL}_2(\mathbb{Q}_p)$.

Exercise 4.23. Compute the function $f \in \mathcal{H}(\mathrm{GL}_n(\mathbb{Q}_p), \mathrm{GL}_n(\mathbb{Z}_p))$ whose Satake transform is equal to $X_1 X_2 \cdots X_n \in \mathbb{C}[X_1^{\pm 1}, X_2^{\pm 1}, \ldots, X_n^{\pm 1}]^{\mathfrak{S}_n}$.

Exercise 4.24. Compute the $\mathrm{GL}_2(\mathbb{Z}_p)$-biinvariant function f on $\mathrm{GL}_2(\mathbb{Q}_p)$ whose Satake transform is equal to $X + Y \in \mathbb{C}[X^{\pm 1}, Y^{\pm 1}]^{\mathfrak{S}_2}$.

Exercise 4.25. Let $\chi\colon (\mathbb{Q}_p^\times)^2 \to \mathbb{C}^\times$ be a smooth character. Compute the Jacquet module $\mathrm{Ind}_{B(\mathbb{Q}_p)}^{\mathrm{GL}_2(\mathbb{Q}_p)}(\chi)_N$ where $B = \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2$ and $N = \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \subset \mathrm{GL}_2$.

Exercise 4.26. In this exercise we make the Satake isomorphism $\mathcal{H}(\mathrm{GL}_2(F), \mathrm{GL}_2(\mathcal{O}_F)) \xrightarrow{\sim} \mathbb{C}[X_1^{\pm 1}, X_2^{\pm 1}]^{\mathfrak{S}_2}$ explicit for GL_2.

(a) Show the two families of polynomials $f_j = X_1^j + X_2^j$ and $g_j = X_1^j X_2^j$ in $\mathbb{C}[X_1^{\pm 1}, X_2^{\pm 1}]^{\mathfrak{S}_2}$ for $j \in \mathbb{Z}$ generate the algebra $\mathbb{C}[X_1^{\pm 1}, X_2^{\pm 1}]^{\mathfrak{S}_2}$ as a complex vector space, and that $f_0 - 2g_0 = 0$ is the only non-trivial linear relation between these functions.

(b) Consider on $\mathcal{H}(\mathrm{GL}_2(F), \mathrm{GL}_2(\mathcal{O}_F))$ the basis consisting of the indicator functors of double cosets. Express the functions f_j and g_j with respect to this basis.

Ramified representations

In the exercises below F is a p-adic local field.

Exercise 4.27. Compute the Jacquet module St_N of the Steinberg representation where $N \subset \mathrm{GL}_2(\mathbb{Q}_p)$ is the group of upper triangular matrices in $\mathrm{GL}_2(\mathbb{Q}_p)$, *i.e.* the matrices of the form $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q}_p)$ with $x \in \mathbb{Q}_p$.

Exercise 4.28. Let V be a smooth representation of $G = \mathrm{GL}_n(F)$ which is finitely generated (*i.e.* there exists some finite-dimensional subspace $W \subset V$ such that $G \cdot W$ generates V as a complex vector space). Show that there exists a quotient $V \twoheadrightarrow W$ where W is irreducible and smooth.

Exercise 4.29. Let (π, V) be a smooth admissible representation of $G = \mathrm{GL}_n$. Let $K = \mathrm{GL}_n(\mathcal{O}_F)$ and $P \subset \mathrm{GL}_n$ a standard parabolic subgroup with Levi decomposition $P = MN$. Show that the mapping $V \to V_{N(F)}$ maps V^K surjectively onto $(V_{N(F)})^{M(\mathcal{O}_F)}$.

Exercise 4.30. Let (V, π) be a finite-dimensional smooth irreducible representation of $G = \mathrm{GL}_n(F)$. Show that V is 1-dimensional.

Exercise 4.31. Show that the Steinberg representation of $\mathrm{GL}_2(F)$ defined by $C^\infty(\mathbb{P}^1(F))/\mathbf{1}$ is an irreducible smooth and admissible representation of $\mathrm{GL}_2(F)$.

Exercise 4.32. Let V be a smooth irreducible representation of $G = \mathrm{GL}_n(F)$, and $A\colon V \to V$ be a non-trivial morphism. In this exercise we show that $A = \mu \cdot \mathrm{id}$, where μ is some scalar in $\mathbb{C}$.

(a) Show that V is of countable dimension.

(b) Assume that $A \neq \mu \cdot \mathrm{id}$ for all $\mu \in \mathbb{C}$. Show that the operator $A - \mu \cdot \mathrm{id}$ is invertible.

(c) Let $v \in V$ be non-zero. Show that the collection of vectors $(A - \mu \cdot \mathrm{id})^{-1}(v) \in V$ where μ ranges over $\mathbb{C}$ is linearly independent and derive a contradiction.

Exercise 4.33. Let V be a smooth irreducible representation of $G = \mathrm{GL}_2(F)$, which is not cuspidal. Show that V is admissible. [2]

Exercise 4.34. Let π be an irreducible smooth admissible representation of $G = \mathrm{GL}_n(F)$. Show that there exists a partition $n = n_1 + n_2 + \ldots + n_r$ cuspidal representations $\sigma_1, \sigma_2, \ldots, \sigma_r$ of $\mathrm{GL}_{n_1}(F)$, $\mathrm{GL}_{n_2}(F)$, ..., $\mathrm{GL}_{n_r}(F)$, such that π appears as a subrepresentation of the parabolic induction $\mathrm{Ind}_{P(F)}^{G(F)}(\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_r)$, where $P \subset \mathrm{GL}_n$ is the standard parabolic subgroup corresponding to the partition (n_i) of n.

Exercise 4.35. Let $G = \mathrm{GL}_n$ and $P \subset G$ a standard parabolic subgroup with Levi decomposition $P = MN$. Show that the Jacquet module is left adjoint to the parabolic induction: $\mathrm{Hom}_{M(F)}(\pi_{N(F)}, \rho) \cong \mathrm{Hom}_{G(F)}(\pi, \mathrm{Ind}_{P(F)}^{G(F)}(\rho))$ for all smooth admissible representations π of $G(F)$ and all smooth admissible representations ρ of $M(F)$.

Exercise 4.36. Let $G = \mathrm{GL}_n$ and $P \subset \mathrm{GL}_n$ a standard parabolic subgroup with Levi decomposition $P = MN$. Show that the Jacquet functor $V \mapsto V_{N(F)}$ maps smooth admissible representations of $G(F)$ to smooth admissible representations of $M(F)$.

Exercise 4.37. Let $f \in \mathcal{H}_0(\mathrm{GL}_2(\mathbb{Q}_p))$ be the characteristic function of the double coset $\mathrm{GL}_2(\mathbb{Z}_p) \cdot \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot \mathrm{GL}_2(\mathbb{Z}_p) \subset \mathrm{GL}_2(\mathbb{Q}_p)$. Normalize the Haar measure on $\mathrm{GL}_2(\mathbb{Q}_p)$ so that the volume of $\mathrm{GL}_2(\mathbb{Z}_p)$ is 1. Compute the trace $\mathrm{Tr}\,\pi(f)$ when

(a) $\pi = \mathbf{1}$ is the trivial representation.

(b) $\pi = \mathrm{St}$ is the Steinberg representation.

Exercise 4.38. Consider the Iwahori subgroup $I \subset \mathrm{GL}_2(\mathbb{Z}_p)$ of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $c \equiv 0 \mod p$. Answer questions (a) and (b) of Exercise 4.37, but now with f equal to the characteristic function of $I\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)I$. Assume that the Haar measure on $\mathrm{GL}_2(\mathbb{Q}_p)$ is normalized so that $\mathrm{vol}(I) = 1$.

Exercise 4.39. Let $\mathbb{F}_9$ be a field of 9 elements, and let θ be a complex character of $\mathbb{F}_9^\times$ with $\theta^3 \neq \theta$. Give an explicit description of the 2-dimensional representation π_θ of $\mathrm{GL}_2(\mathbb{F}_3)$ defined in Theorem 4.25.

[2] In fact, this result is also true without the assumption "not cuspidal", but then the proof is more difficult. Moreover, the result also holds for $\mathrm{GL}_n(F)$ in place of $\mathrm{GL}_2(F)$.

The local Langlands correspondence

Exercise 4.40. Let $j \geq 1$ be an integer. Inside its algebraic closure $\overline{\mathbb{Q}}_p$ the field $\mathbb{Q}_p$ has a unique extension of degree j that is unramified, we write $\mathbb{Q}_{p^j}$ for it. We can restrict any Weil–Deligne representation $r = (\phi, N)$ of $W(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ to the representation $r|_{W(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^j})} = (\phi|_{W(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^j})}, N)$ of $W(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^j})$. We write $\mathrm{Unr}(\mathrm{GL}_n(\mathbb{Q}_p))$ for the set of isomorphism classes of unramified smooth irreducible representations of $\mathrm{GL}_n(\mathbb{Q}_p)$, and $\mathrm{WD}(\mathbb{Q}_p)$ (resp. $\mathrm{WD}(\mathbb{Q}_{p^j})$) for the set of isomorphism classes of unramified representations of $W(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ (resp. $W(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^j})$).

(a) Use the local Langlands correspondence to show that there exists a unique mapping $\mathrm{Unr}(\mathrm{GL}_n(\mathbb{Q}_p)) \to \mathrm{Unr}(\mathrm{GL}_n(\mathbb{Q}_{p^j}))$ making the diagram below commute:

$$\begin{array}{ccccc} \mathrm{WD}(\mathbb{Q}_p) & \ni & r \longmapsto r|_{W(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^j})} & \in & \mathrm{WD}(\mathbb{Q}_{p^j}) \\ {\scriptstyle \mathrm{rec}_{\mathbb{Q}_p}}\downarrow\cong & & \downarrow \quad\quad \downarrow & & \cong\downarrow{\scriptstyle \mathrm{rec}_{\mathbb{Q}_{p^j}}} \\ \mathrm{Unr}(\mathrm{GL}_n(\mathbb{Q}_p)) & \ni & \pi \vdash \cdots \succ B(\pi) & \in & \mathrm{Unr}(\mathrm{GL}_n(\mathbb{Q}_{p^j})) \end{array}$$

(b) Show that if r is unramified, then $r|_{W(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^j})}$ is unramified as well. Use the Satake transform to show that $r \mapsto r|_{W(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^j})}$ induces a morphism

$$\operatorname{spec}\max(\mathbb{C}[X_1^{\pm 1}, X_2^{\pm 1}, \ldots, X_n^{\pm 1}]^{\mathfrak{S}_n}) \to \operatorname{spec}\max(\mathbb{C}[X_1^{\pm 1}, X_2^{\pm 1}, \ldots, X_n^{\pm 1}]^{\mathfrak{S}_n})$$

and hence an endomorphism of the ring $\mathbb{C}[X_1^{\pm 1}, X_2^{\pm 1}, \ldots, X_n^{\pm 1}]^{\mathfrak{S}_n}$. Describe this endomorphism with an explicit formula.

Chapter 5

Automorphic representations

Contents

Some useful references for this chapter are the exposition by Kudla [1, Chapter 7] and the books of Gelbart [5, Sections 3 and 5] and Bump [2, Chapter 3].

5.1 Modular forms as functions on $\mathrm{GL}_2(\mathbb{R})$

We begin by recalling the classical definition of modular forms. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on the complex upper half-plane $\mathcal{H}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}.$$

For $n \geq 1$, we define

$$\Gamma_1(n) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{n} \right\}.$$

Definition 5.1. Let n and k be positive integers. A *modular form* of weight k for $\Gamma_1(n)$ is a holomorphic function

$$f \colon \mathcal{H} \to \mathbb{C}$$

such that

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} z \right) = (cz+d)^k f(z) \quad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(n)$$

and such that f is "holomorphic at infinity".

The space of modular forms of weight k for $\Gamma_1(n)$ is a finite-dimensional $\mathbb{C}$-vector space denoted by $\mathrm{M}_k(\Gamma_1(n))$.

There is a smooth map

$$\begin{aligned} p\colon \mathrm{GL}_2(\mathbb{R})^+ &\longrightarrow \mathcal{H} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\longmapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} i = \frac{ai+b}{ci+d}. \end{aligned}$$

Given $f \in \mathrm{M}_k(\Gamma_1(n))$, we would like to construct a smooth function

$$\tilde{f}\colon \mathrm{GL}_2(\mathbb{R})^+ \to \mathbb{C}$$

that is *invariant* under the action of $\Gamma_1(n)$. We therefore define

$$\tilde{f}(g) = j(g) f(gi)$$

where $j\colon \mathrm{GL}_2(\mathbb{R})^+ \to \mathbb{C}$ is a function satisfying

$$j(\gamma g) f(\gamma g i) = j(g) f(gi) \quad \text{for all } \gamma \in \Gamma_1(n), g \in \mathrm{GL}_2(\mathbb{R})^+,$$

which by the transformation property of f translates to

$$j(\gamma g)(cgi+d)^k = j(g) \quad \text{for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(n), g \in \mathrm{GL}_2(\mathbb{R})^+.$$

The simplest choice is

$$j\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ci+d)^{-k},$$

so we take as our definition

$$\tilde{f}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ci+d)^{-k} f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} i\right) \quad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})^+.$$

One then checks that $\tilde{f}$ satisfies the following transformation properties for all $g \in G$:

- $\tilde{f}(\gamma g) = \tilde{f}(g)$ for all $\gamma \in \Gamma_1(n)$;
- $\tilde{f}(zg) = \tilde{f}(gz) = t^{-k} f(g)$ for all $z = \left(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix}\right)$ with $t \in \mathbb{R}^\times$;
- $\tilde{f}(g r_\theta) = \exp(-ik\theta)\tilde{f}(g)$ for all $\theta \in \mathbb{R}$, where $r_\theta = \left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right) \in \mathrm{SO}_2(\mathbb{R})$.

Remark 5.2. Other choices for j are possible, for example

$$j\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{(ad-bc)^{k/2}}{(ci+d)^k}.$$

5.2 Adelic modular forms

Let n and k be positive integers, and let $\mathrm{M}_k(\Gamma_1(n))$ be the $\mathbb{C}$-vector space of modular forms of weight k for $\Gamma_1(n)$.

Now let $K_1(n)$ be the compact open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \subset \mathrm{GL}_2(\mathbb{A}_f)$ defined by

$$K_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) \;\middle|\; c \equiv 0, d \equiv 1 \pmod{n} \right\}.$$

Let us write

$$G = \mathrm{GL}_2, \quad K = K_1(n).$$

Then we clearly have

$$K_1(n) \cap \mathrm{SL}_2(\mathbb{Z}) = \Gamma_1(n) \quad \text{in } \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

Furthermore, the determinant map

$$\det\colon K \to \widehat{\mathbb{Z}}^\times$$

is surjective. Thanks to strong approximation for SL_2, this implies (see Exercise 5.1) that the continuous map

$$G(\mathbb{R})^+ \times K \longrightarrow G(\mathbb{Q})\backslash G(\mathbb{A})$$

is surjective. Taking the quotient by the right action of K (viewed as a subgroup of $G(\mathbb{A}^\infty) \subset G(\mathbb{A})$), we obtain a surjective continuous map

$$G(\mathbb{R})^+ \longrightarrow G(\mathbb{Q})\backslash\big(G(\mathbb{R}) \times G(\mathbb{A}^\infty)/K\big),$$

where $G(\mathbb{A}^\infty)/K$ is viewed as a discrete left $G(\mathbb{Q})$-set.

Lemma 5.3. *The above map induces a homeomorphism*

$$\Gamma_1(n)\backslash G(\mathbb{R})^+ \xrightarrow{\sim} G(\mathbb{Q})\backslash\big(G(\mathbb{R}) \times G(\mathbb{A}^\infty)/K\big).$$

Proof. For $g \in G(\mathbb{R})^+$, let $[g]$ denote the image of g on the right-hand side. We claim that two elements $g, h \in G(\mathbb{R})^+$ satisfy $[g] = [h]$ if and only if there exists $\gamma \in \Gamma_1(n)$ such that $\gamma g = h$. By definition, the identity $[g] = [h]$ is equivalent to the existence of $g_0 \in G(\mathbb{Q})$ and $k \in K$ such that

$$(g, 1) = g_0(h, k) = (g_0 h, g_0 k) \quad \text{in } G(\mathbb{R}) \times G(\mathbb{A}^\infty).$$

If such g_0 and k exist, we have

$$g_0 = gh^{-1} \in G(\mathbb{Q}) \cap G(\mathbb{R})^+ = G(\mathbb{Q})^+$$

and

$$g_0 = k^{-1} \in G(\mathbb{Q}) \cap K = G(\mathbb{Z}) \cap K$$

and hence

$$g_0 \in \mathrm{SL}_2(\mathbb{Z}) \cap K = \Gamma_1(n).$$

Thus we can take $\gamma = g_0$. Conversely, if $\gamma \in \Gamma_1(n)$ satisfies $\gamma g = h$, then taking $g_0 = k^{-1} = \gamma$ above shows that $[g] = [h]$.

By the definition of the quotient topology, there exists a bijective continuous map as in the lemma. The proof that the inverse of this map is also continuous is left to the reader (Exercise 5.2). □

Given a continuous function

$$\tilde{f}\colon G(\mathbb{R})^+ \to \mathbb{C}$$

satisfying

$$\tilde{f}(\gamma g) = \tilde{f}(g) \quad \text{for all } g \in G(\mathbb{R})^+, \gamma \in \Gamma_1(n)$$

we can transfer $\tilde{f}$ to a continuous function

$$\phi\colon G(\mathbb{Q})\backslash G(\mathbb{A}) \to \mathbb{C}$$

satisfying

$$\phi(g(1,k)) = \phi(g) \quad \text{for all } g \in G(\mathbb{A}), k \in K.$$

The space $G(\mathbb{Q})\backslash G(\mathbb{A})$ has a continuous right $G(\mathbb{A})$-action, and hence the space of continous functions $G(\mathbb{Q})\backslash G(\mathbb{A}) \to \mathbb{C}$ has a left $G(\mathbb{A})$-action.

Morally speaking, an *automorphic representation* of G is a subrepresentation of $G(\mathbb{A})$ on a suitable space of smooth functions on $G(\mathbb{Q})\backslash G(\mathbb{A})$. Unfortunately, due to the action of $G(\mathbb{R})$, these spaces are "too big" to be handled in a convenient algebraic way. Therefore, instead of a representation of the full group $G(\mathbb{A})$, we will consider representations of $G(\mathbb{A}^\infty)$ that are additionally equipped not with the structure of a representation of $G(\mathbb{R})$, but with the structure of a $(\mathfrak{g}, K)$-module.

Remark 5.4. The spaces $G(\mathbb{Q})\backslash\big(G(\mathbb{R}) \times G(\mathbb{A}^\infty)/K\big)$ are examples of *Shimura varieties*.

5.3 Global representations

Let F be a number field. For simplicity, it is probably best to restrict oneself (at first) to the case

$$F = \mathbb{Q}.$$

There are no essential difficulties in generalising everything to the case where F is an arbitrary number field.

We will write

$$G = \mathrm{GL}_{n,F}$$

viewed as an algebraic group over F. In particular, we will be interested in the topological groups $G(F)$ (with the discrete topology), $G(F_v)$ for completions of V (with the natural topology) and $\mathbb{G}(\mathbb{A}_F)$ (with the restricted product topology).

For every Archimedean place v, we define

$$\mathfrak{g}_v = \mathrm{Lie}(G(F_v)) = \mathrm{Mat}_n(F_v)$$

and we let K_v be the standard maximal compact subgroup of $G(F_v)$, given by

$$K_v = \begin{cases} \mathrm{O}_n(F_v) & \text{if } v \text{ is real,} \\ \mathrm{U}_n(F_v) & \text{if } v \text{ is complex.} \end{cases}$$

We put

$$\mathfrak{g}_{\mathbb{C}} = \prod_{v \text{ infinite}} \mathfrak{g}_v \otimes_{\mathbb{R}} \mathbb{C}$$

and

$$K_\infty = \prod_{v \text{ infinite}} K_v.$$

Definition 5.5. A function $\phi\colon G(\mathbb{A}_F) \to \mathbb{C}$ is *smooth* if it satisfies the following properties:

(i) There exists a compact open subgroup $K \subset G(\mathbb{A}_F^\infty)$ such that $\phi(gk) = \phi(g)$ for all $g \in G(\mathbb{A}_F)$ and $k \in K$.

(ii) For every $g^\infty \in G(\mathbb{A}_F^\infty)$, the function

$$\begin{aligned} G(F \otimes_{\mathbb{Q}} \mathbb{R}) &\to \mathbb{C} \\ g_\infty &\mapsto \phi(g_\infty, g^\infty) \end{aligned}$$

is smooth (*i.e.* infinitely continuously differentiable).

Definition 5.6. An *automorphic form* for G is a smooth function

$$\phi\colon G(F)\backslash G(\mathbb{A}_F) \to \mathbb{C}$$

(or equivalently a smooth function $\phi\colon G(\mathbb{A}_F) \to \mathbb{C}$ satisfying $\phi(g_0 g) = \phi(g)$ for all $g_0 \in G(F)$ and $g \in G(\mathbb{A}_F)$) with the following properties:

(i) ϕ is K_∞-*finite*, *i.e.* the $\mathbb{C}$-vector space spanned by the smooth functions $G(\mathbb{A}_F) \to \mathbb{C}$, $g \mapsto \phi(gk)$ for $k \in K_\infty$ is finite-dimensional.

(ii) ϕ is $Z(U(\mathfrak{g}_\mathbb{C}))$-*finite*, *i.e.* the $\mathbb{C}$-vector space $Z(U(\mathfrak{g}_\mathbb{C}))\phi$ is finite-dimensional, where the action of $\mathfrak{g}_\mathbb{C}$, and hence of $U(\mathfrak{g}_\mathbb{C})$ and $Z(U(\mathfrak{g}_C))$, on the space of smooth functions $G(\mathbb{A}_F) \to \mathbb{C}$ is defined through the right action of $G(F \otimes_{\mathbb{Q}} \mathbb{R})$ on $G(\mathbb{A}_F)$.

(iii) ϕ is of *moderate growth*.

The $\mathbb{C}$-vector space of automorphic forms for G is denoted by $\mathcal{A}(G)$.

The condition of moderate growth requires some explanation. We consider the embedding

$$\begin{aligned} \mathrm{GL}_n(\mathbb{A}_F) &\longrightarrow \mathbb{A}_F^{n^2+1} \\ A = (a_{i,j})_{i,j=1}^n &\longmapsto (a_{1,1}, a_{1,2}, \ldots, a_{n,n}, (\det A)^{-1}). \end{aligned}$$

The norm $\|g\|$ of an element $g \in \mathrm{GL}_n(\mathbb{A}_F)$ is defined as $\prod_v \max_i |x_i|_v$, where $(x_1, \ldots, x_{n^2+1})$ is the image of g under the above embedding and v runs over all places of F. Then ϕ is said to be of *moderate growth* if there exist real numbers $B, C > 0$ such that $|\phi(g)| \leq C\|g\|^B$ for all $g \in G(\mathbb{A}_F)$.

Remark 5.7. Although there is a left action of the group $G(\mathbb{A}_F)$ on the space of all continuous functions $G(\mathbb{A}_F) \to \mathbb{C}$, this action does *not* induce an action of $G(\mathbb{A}_F)$ on $\mathcal{A}(G)$. The reason is that the condition of K_∞-finiteness is not preserved.

Definition 5.8. An *admissible representation* of $G(\mathbb{A}_F)$ is a pair (π, V) where V is a $\mathbb{C}$-vector space equipped with the structure of both a smooth representation of $G(\mathbb{A}_F^\infty)$ and a $(\mathfrak{g}, K_\infty)$-module, both of which are denoted by π, such that the two actions commute and such that every irreducible continuous finite-dimensional representation of the compact group $K = K_\infty \times G(\mathcal{O}_F)$ occurs only finitely many times in V (up to isomorphism). We say that (π, V) is *irreducible* if (π, V) has exactly two subrepresentations (namely the zero subspace and V itself).

Definition 5.9. An *automorphic representation* of $G(\mathbb{A}_F)$ is an irreducible admissible representation of $G(\mathbb{A}_F)$ (in the above sense) that is isomorphic to a subquotient of $\mathcal{A}(G)$.

5.3.1 The space of cuspforms

Definition 5.10. We call an automorphic form $f \in \mathcal{A}(G)$ a *cuspform*, if for every strict standard parabolic subgroup $P = MN \subset G$, and all $g \in G(\mathbb{A}_F)$, we have

$$\int_{n \in N(\mathbb{A}_F)} f(gn) = 0.$$

We write $\mathcal{A}_0(G) \subset \mathcal{A}(G)$ for the subspace of cuspforms.

The (algebraic) cuspforms should correspond to those Galois representations that are irreducible. Since any semi-simple representation is a sum of irreducible representations, the cuspforms should form the building blocks of all automorphic representations.

Definition 5.11. We call an automorphic representation π of $G(\mathbb{A}_F)$ *cuspidal* if it appears in the space of cusp forms on G.

5.4 Decomposing automorphic representations into local components

The goal of this section is to explain Flath's tensor product decomposition. We begin with a proposition that can be found in Bourbaki chapter 2 on algebra:

Proposition 5.12. *Let A, B be unitary, associative algebras over $\mathbb{C}$ that are of finite type. If M is an A-module and N is a B-module, we equip $M \otimes_{\mathbb{C}} N$ with the following structure of $A \otimes_{\mathbb{C}} B$-module:*

$$(a \otimes b) \cdot (x \otimes y) := (ax) \otimes (by)$$

for all $a \in A$, $b \in B$, $x \in M$ and $y \in N$.

(i) If M, N are simple modules, then $M \otimes_{\mathbb{C}} N$ is a simple $A \otimes_{\mathbb{C}} B$-module.

(ii) Any simple $A \otimes_{\mathbb{C}} B$-module X is isomorphic to a module of the form $M \otimes_{\mathbb{C}} N$, where M, N are determined uniquely up to isomorphism of A (resp. B)-modules.

For simplicity, we will focus mostly on the finite part of the automorphic representations. Hence representations of the group $G(\mathbb{A}_F^\infty)$. Let $K \subset G(\mathbb{A}_F^\infty)$ be a compact open subgroup, of the form

$$K = \prod_{\text{finite } F\text{-places } v} K_v \subset G(\mathbb{A}_F^\infty), \qquad K_v \subset G(F_v) \text{ compact open subgroup.}$$

Furthermore, we assume that $K_v = \mathrm{GL}_n(\mathcal{O}_{F_v})$ for all $v \notin S$, where S is some finite subset of finite F-places that we fix from now on. For what we are about to do, making these assumptions on K impose no restrictions on generality (they can always be achieved by conjugating are shrinking an arbitrary compact open $K \subset G(\mathbb{A}_F^\infty)$). The group $G(\mathbb{A}_F^\infty)$ is locally profinite. We consider the Haar measure on this group giving K measure 1. Then we can consider the Hecke algebra $\mathcal{H}(G(\mathbb{A}_F^\infty)//K)$ of compactly supported and locally constant functions, where the product is defined by the usual convolution integral with respect to our fixed Haar measure. It is not hard to see that in fact

$$\mathcal{H}(G(\mathbb{A}_F^\infty)//K) \cong \bigotimes_{\text{finite } F\text{-places } v} \mathcal{H}(G(F_v)//K_v),$$

and moreover, as before, to give a smooth admissible irreducible representation π of $G(\mathbb{A}_F^\infty)$ is to give a simple module M over the Hecke algebra $\mathcal{H}(G(\mathbb{A}_F^\infty)//K)$.

Let us focus our attention on the simple modules M of $\mathcal{H}(G(\mathbb{A}_F^\infty)//K)$. We have our set of finite F-places S outside which we have $K_v = \mathrm{GL}_n(\mathcal{O}_{F_v})$. Write $K_S = \prod_{v\in S} K_v$ and $K^S = \prod_{v\notin S} K_v = \mathrm{GL}_n(\widehat{\mathcal{O}}_F^S)$. Then we have $G(\mathbb{A}_F^\infty) = G(\mathbb{A}_{F,S}^\infty) \times G(\mathbb{A}_F^{\infty,S})$ and the algebra $\mathcal{H}(G(\mathbb{A}_F^\infty)//K)$ decomposes into $\mathcal{H}(G(\mathbb{A}_{F,S}^\infty)//K_S) \otimes_{\mathbb{C}} \mathcal{H}(G(\mathbb{A}_F^{S,\times})//K^S)$. Consequently, by Proposition 5.12 there is a corresponding decomposition of the module M into a tensor product $M_S \otimes M^S$, where M_S and M^S are modules over $\mathcal{H}(G(\mathbb{A}_{F,S}^\infty)//K_S)$ and $\mathcal{H}(G(\mathbb{A}_F^{\infty,S})//K^S)$. Note that the algebra

$$\mathcal{H}(G(\mathbb{A}_F^{\infty,S})//K^S) = \bigotimes_{v\notin S} \mathcal{H}(G(F_v)//K_v),$$

is a tensor product of commutative algebras, and hence commutative. Therefore the simple module M^S is one dimensional over $\mathbb{C}$. By considering the restrictions

$$\mathcal{H}(G(F_v)//K_v) \subset \mathcal{H}(G(\mathbb{A}_F^{\infty,S})//K^S) \circlearrowright M^S \cong \mathbb{C}$$

we obtain for every finite F-places $v \notin S$ a one dimensional module M_v over $\mathcal{H}(G(F_v)//K_v)$. We then have $M \cong \bigotimes_v M_v$, as $\mathcal{H}(G(\mathbb{A}_F^{\infty,S})//K^S)$-modules. To study the places v in S, notice first that the tensor product

$$\mathcal{H}(G(\mathbb{A}_{F,S}^\infty)//K_S) \cong \bigotimes_{v\in S} \mathcal{H}(G(F_v)//K_v),$$

ranges over a finite set. Hence by applying Proposition 5.12 multiple times to break up the module M_S, we also obtain modules M_v for the places $v \in S$. In conclusion, we have decomposed $M \cong \bigotimes_v M_v$ as $\mathcal{H}(G(\mathbb{A}_{F,S}^\infty)//K_S) \cong \bigotimes_v \mathcal{H}(G(F_v)//K_v)$-module. Finally, the module M corresponds to the representation π. The local modules M_v correspond to certain local representations π_v of $\mathrm{GL}_n(F_v)$, which are smooth admissible and irreducible, and uniquely determined up to isomorphism. We will write formally,

$$\pi \cong \bigotimes_v{}' \pi_v. \tag{5.1}$$

Beware: The dash in the exponent indicates that the above is a *restricted tensor product* and not a tensor product in the usual sense. It is also possible to obtain π from the π_v directly (so without going through the Hecke algebra's). To do this, choose for almost all F-places v a non-zero element $\xi_v \in \pi_v^{K_v}$. Then the restricted tensor product can be viewed as the subspace of the full infinite tensor product $\bigotimes_v \pi_v$ generated by all elementary tensors $\otimes_v t_v$ with $t_v = \xi_v$ for almost all places v.

By including further arguments to separate out the modules at infinity (note that there are only finitely many infinite places), one can prove *Flath's tensor product decomposition*:

Theorem 5.13 (Flath, 1979)**.** *Let (π, V) be an irreducible admissible representation of $G(\mathbb{A}_F)$. Then there exist*

- *an irreducible admissible $(\mathfrak{g}, K_\infty)$-module (π_∞, V_∞),*
- *an irreducible admissible representation (π_v, V_v) for every finite place v of F,*

- *a non-zero element $\xi_v \in K_v$, for all but finitely many v*

such that π is isomorphic to the restricted tensor product of the V_v with respect to the ξ_v. Furthermore, each (π_v, V_v) is unique up to isomorphism.

We are now ready to define the partial L-function of a irreducible smooth admissible $G(\mathbb{A}_F^\infty)$ representation π. There exists, as stated above, a finite set of finite F-places S, outside which π is unramified, *i.e.* the local representations π_v from (5.1) are unramified for $v \notin S$. From the Satake isomorphism, we get for each $v \notin S$ a corresponding Satake parameter $\phi_v \in \mathrm{GL}_n(\mathbb{C})/\sim$. Then, we define as usual

$$L_v(\pi, s) = \frac{1}{\det(1 - \phi_v X)}\bigg|_{X=q_v^{-s}} \in \mathbb{C}(p^{-s}),$$

where q_v is the cardinality of the residue field of F at v. The partial L-function is then defined as a formal product

$$L^S(\pi, s) = \prod_{v \notin S} L_v(\pi, s).$$

It is possible to define local factors $L_v(\pi, s)$ for the finite $v \in S$, and also the infinite places v. Then, the completed L-function is the product over all the F-places. A first major question one would like to show is, if π is automorphic, that $L(\pi, s)$ converges to meromorphic function on the complex plane $\mathbb{C}$, and understand its poles. To do this, the first step is to get the partial L-function $L^S(\pi, s)$ under control.

Strong multiplicity one theorem

Let $\pi \cong \bigotimes_v' \pi_v$ be a cuspidal automorphic representation of $G(\mathbb{A}_F)$. Let S be a finite set of finite F-places such that for the finite F-places away from S the representation π_v is unramified. In particular, we can attach to π the collection of Satake parameter $\{\phi_v\}_{v \notin S}$, where $\phi_v \in \mathrm{GL}_n(\mathbb{C})/\sim$ is a semi-simple conjugacy class.

Theorem 5.14 (Strong multiplicity one)**.** *Let S' be any finite set of finite F-places v containing S. The (isomorphism class of) the automorphic representation π is uniquely determined by the collection of Satake parameters $\{\phi_v\}_{v \notin S'}$*

Remark 5.15. For groups different from GL_n the above theorem fails (in fact, for several reasons).

Conversely, when given a collection of conjugacy classes $\{\phi_v\}_{v \notin S}$, one may wonder if there exists an automorphic representation giving rise to these ϕ_v. A priori, there are uncountably many choices for these ϕ_v, but there exist only countably many automorphic representations. So, most of these collections $\{\phi_v\}$ do not correspond to automorphic representations. Moreover, if you make random choices for these ϕ_v, there is no reason for the partial L-function $L^S(\pi, s)$ to converge.

Algebraic automorphic representations

Unfortunately, we do not have time to discuss this topic in depth; we only give a sketch. We refer to [19, Section 3] for more details.

When studying $(\mathfrak{g}, K_\infty)$-modules, we came across the algebra $Z = Z(U(\mathfrak{g}_\mathbb{C}))$, where $\mathfrak{g}_\mathbb{C}$ is the Lie algebra of $\mathrm{GL}_n(\mathbb{C})$. By the Harish-Chandra isomorphism, the algebra Z is isomorphic to the algebra of $\mathfrak{S}_n$-invariants of the polynomial algebra $\mathbb{C}[X_1, \ldots, X_n]$. Any irreducible $(\mathfrak{g}, K_\infty)$-module M_∞ has a central character, and this central character corresponds through Harish-Chandra's isomorphism to sequence of n complex numbers. The module M_∞ is called *algebraic* if these complex numbers are integers.

Definition 5.16. Let F be a number field. An automorphic representation π of $\mathrm{GL}_n(\mathbb{A}_F)$ is *algebraic* if its component at infinity is an algebraic $(\mathfrak{g}, K_\infty)$-module.

The global Langlands conjecture

We can now state the global Langlands conjecture.

Conjecture 5.17. *Let F be a number field, and consider the group $G = \mathrm{GL}_{n,F}$ over F. Let ℓ be a prime number and choose an isomorphism $\iota\colon \mathbb{C} \xrightarrow{\sim} \overline{\mathbb{Q}}_\ell$. Then, for any algebraic cuspidal automorphic representation π of $\mathrm{GL}_n(\mathbb{A}_F)$ there exists a semi-simple Galois representation $\rho_\pi = \rho_{\pi,\iota}\colon \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ such that for all finite F-places v where π is unramified and $v \nmid \ell$, the Galois representation ρ_π is unramified as well, and $\rho_\pi(\mathrm{Frob}_v)_{\mathrm{ss}}$ is conjugate to $\iota\phi_{\pi_v} \in \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$, where ϕ_{π_v} is the Satake parameter of π_v.*

At the ramified places the correspondence should be compatible with the local Langlands correspondence, but note that the above already pins down both the automorphic representation (by strong multiplicity one) and the Galois representation (by the Chebotarev density theorem).

The above conjecture can be combined with further conjectures. Fontaine-Mazur's conjecture states that any irreducible Galois representation ρ_π appearing in the cohomology of a smooth projective variety X over F, should arize from an automorphic form. Hence this conjecture describes the image of $\pi \mapsto \rho_\pi$ in Langland's conjecture.

5.5 Exercises

Exercise 5.1. Let K be a compact open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Prove that the map

$$\mathrm{GL}_2(\mathbb{R})^+ \times K \longrightarrow \mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A})$$

is surjective if and only if the determinant map $\det\colon K \to \widehat{\mathbb{Z}}^\times$ is surjective.
(*Hint:* you may use without proof that SL_2 satisfies strong approximation outside $\{\infty\}$.)

Exercise 5.2. Prove that the map from Lemma 5.3 is a homeomorphism.

Exercise 5.3. Consider the elements a_+, a_- of the complexified Lie algebra $\mathfrak{g}_\mathbb{C} \cong \mathrm{Mat}_2(\mathbb{C})$ of $\mathrm{GL}_2(\mathbb{R})$ defined before Exercise 4.16. Let $f\colon \mathcal{H} \to \mathbb{C}$ be a smooth function, let k be an integer, and define

$$\tilde{f}\colon \mathrm{GL}_2(\mathbb{R})^+ \to \mathbb{C}$$

by

$$\tilde{f}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ci+d)^{-k} f\left(\frac{ai+b}{ci+d}\right).$$

(a) Prove formulae expressing the effect of $a_\pm$ on $\tilde{f}$ in terms of the partial derivatives of f with respect to the coordinates x and y on $\mathcal{H}$ (with $z = x + iy$).

(b) Show that $a_- \tilde{f} = 0$ if and only if f is holomorphic.

(c) Is it true that $a_+ \tilde{f} = 0$ if and only if f is antiholomorphic?

Exercise 5.4. (a) Let F be a number field, and let V be a direct sum of finitely many continuous one-dimensional representations of $\mathbb{A}_F^\times$ (corresponding to continuous group homomorphisms $\mathbb{A}_F^\times \to \mathbb{C}^\times$). Show that V is an admissible representation of $\mathbb{G}_{\mathrm{m},F} = \mathrm{GL}_{1,F}$.

(b) *(Bonus question.)* Is every finite-dimensional admissible representation of $\mathbb{G}_{\mathrm{m},F}$ of the above form?

Exercise 5.5. Show that an automorphic representation of $\mathbb{G}_\mathrm{m} = \mathrm{GL}_1$ over a number field F is the same as a Hecke character of F.

Let F be a number field, let $\omega\colon \mathbb{A}_F^\times \to \mathbb{C}^\times$ be a Hecke character of F, and let $G = \mathrm{GL}_{n,F}$ with $n \geq 1$. An *automorphic form with central character* ω is an automorphic form $\phi \in \mathcal{A}(G)$ satisfying the additional property

$$\phi(g \operatorname{diag}(x)) = \omega(x)\phi(g) \quad \text{for all } g \in G(\mathbb{A}_F),$$

where $\operatorname{diag}(x)$ is x viewed as a scalar matrix. The $\mathbb{C}$-vector space of automorphic forms with central character ω is denoted by $\mathcal{A}(G, \omega)$.

Exercise 5.6. Show that as an admissible representation of $G(\mathbb{A}_F)$, the space $\mathcal{A}(G)$ of automorphic forms for G is the direct sum of its subspaces $\mathcal{A}(G, \omega)$.

Exercise 5.7. Let $f \in \mathrm{M}_k(\Gamma_1(n))$ be a modular form, and suppose that f is an *eigenform for the diamond operators* $\langle d \rangle$ for $d \in (\mathbb{Z}/n\mathbb{Z})^\times$. This means that there exists a Dirichlet character

$$\chi\colon (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$$

such that for all $z \in \mathcal{H}$ and all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $n \mid c$, we have

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z).$$

Let $\phi_f \in \mathcal{A}(\mathrm{GL}_{2,\mathbb{Q}})$ be the automorphic form attached to f. For $s \in \mathbb{C}$, let $\omega_{\chi,s}\colon \mathbb{A}_\mathbb{Q}^\times \to \mathbb{C}^\times$ be the Hecke character defined in Section 2.6. Show that ϕ_f lies in $\mathcal{A}(\mathrm{GL}_{2,\mathbb{Q}}, \omega_{\chi,s}^{-1})$ for some $s \in \mathbb{C}$, and determine s.

Bibliography

[1] J. Bernstein and S. Gelbart (editors), *An Introduction to the Langlands Program*. With contributions by D. Bump, J. W. Cogdell, D. Gaitsgory, E. de Shalit, E. Kowalski and S. S. Kudla. Birkhäuser, Boston, 2004.

[2] D. Bump, *Automorphic forms and representations*. Cambridge University Press, Cambridge, 1997.

[3] C. Bushnell and G. Henniart, *The local Langlands conjecture for* GL(2). Grundlehren der Mathematischen Wissenschaften **335**. Springer-Verlag, Berlin, 2006.

[4] J. W. Cogdell, *On Artin L-functions*, `https://people.math.osu.edu/cogdell.1/artin-www.pdf`.

[5] S. Gelbart, *Automorphic Forms on Adèle Groups*. Annals of Mathematics Studies 83. Princeton University Press, Princeton, New Jersey, 1975.

[6] S. Gelbart, An elementary introduction to the Langlands program. *Bull. A.M.S.* **10** (1984), no. 2, 177–219.

[7] B. H. Gross, On the Satake isomorphism. In: *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, 223–237, London Math. Soc. Lecture Note Ser., 254, Cambridge Univ. Press, Cambridge, 1998.

[8] R. E. Kottwitz, Orbital integrals on GL_3. *Amer. J. Math.* **102** (1980), no. 2, 327–384.

[9] H. Matsumura, *Commutative Ring Theory*. Translated by Miles Reid. Cambridge University Press, 1986.

[10] J. Neukirch, *Algebraische Zahlentheorie*. Springer-Verlag, Berlin/Heidelberg, 1992.

[11] F. Oort, The Weil conjectures. *Nieuw Archief voor Wiskunde* (5) **15** (2014), no. 3, 211–219.

[12] J-P. Serre, *Classes des corps cyclotomiques*. Séminaire Bourbaki, décembre 1958, `http://archive.numdam.org/ARCHIVE/SB/SB_1958-1960__5_/SB_1958-1960__5__83_0/SB_1958-1960__5__83_0.pdf`.

[13] J-P. Serre, *Cohomologie galoisienne* (cinquième édition). Springer-Verlag, Berlin/Heidelberg/New York, 1997.

[14] J-P. Serre, *Representations linéaires des groupes finis*. Hermann, Paris, 1967.

[15] J. H. Silverman, *The Arithmetic of Elliptic Curves* (second edition). Springer-Verlag, Berlin/Heidelberg/New York, 2009.

[16] The Stacks Project Authors, *Stacks Project*, 2016, `http://stacks.math.columbia.edu/`.

[17] P. Stevenhagen, *Number Rings*. Course notes, 2012, `http://websites.math.leidenuniv.nl/algebra/ant.pdf`

[18] J. Tate, Number theoretic background. In: A. Borel and W. Casselman (editors), *Automorphic forms, representations and L-functions* (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, 3–26, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979.

[19] R. Taylor, *Galois Representations*, `www.math.ias.edu/~rtaylor/longicm02.pdf`.