Part IV — Topics in Number Theory
Definitions

Based on lectures by A. J. Scholl
Notes taken by Dexter Chua

Lent 2018

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

The "Langlands programme" is a far-ranging series of conjectures describing the connections between automorphic forms on the one hand, and algebraic number theory and arithmetic algebraic geometry on the other. In these lectures we will give an introduction to some aspects of this programme.

Pre-requisites

The course will follow on naturally from the Michaelmas term courses *Algebraic Number Theory* and *Modular Forms and L-Functions*, and knowledge of them will be assumed. Some knowledge of algebraic geometry will be required in places.

Contents

0 Introduction

1 Class field theory

1.1 Preliminaries

Notation. Let K be a field. We will write $\bar{K}$ for a separable closure of K, and $\Gamma_K = \mathrm{Gal}(\bar{K}/K)$. We have

$$\Gamma_K = \lim_{L/K \text{ finite separable}} \mathrm{Gal}(L/K),$$

which is a *profinite group*. The associated topology is the *Krull topology*.

Notation. We write K^{ab} for the maximal abelian subextension of $\bar{K}$, and then

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) = \Gamma_K^{\mathrm{ab}} = \frac{\Gamma_K}{[\Gamma_K, \Gamma_K]}.$$

Definition (Non-Archimedean local field)**.** A *non-Archimedean local field* is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$.

Definition (Archimedean local field)**.** An Archimedean local field is a field that is $\mathbb{R}$ or $\mathbb{C}$.

Definition (Valuation ring)**.** The *valuation ring* of a non-Archimedean local field F is

$$\mathcal{O} = \mathcal{O}_F = \{x \in F : v(x) \geq 0\}.$$

Any element $\pi = \pi_f \in \mathcal{O}_F$ with $v(\pi) = 1$ is called a *uniformizer*. This generates the maximal ideal

$$\mathfrak{m} = \mathfrak{m}_F = \{x \in \mathcal{O}_F : v(x) \geq 1\}.$$

Definition (Residue field)**.** The *residue field* of a non-Archimedean local field F is

$$k = k_F = \mathcal{O}_F/\mathfrak{m}_F.$$

This is a finite field of order $q = p^r$.

Definition (Inertia group)**.** The *inertia group* I_F is defined to be

$$I_F = \mathrm{Gal}(\bar{F}/F^{\mathrm{ur}}) \subseteq \Gamma_F.$$

Definition (Wild inertia group)**.** The *wild inertia group* P_F is the maximal pro-p-subgroup of I_F.

Definition (Arithmetic Frobenius)**.** The *arithmetic Frobenius* $\varphi_q \in \mathrm{Gal}(\bar{k}/k)$ (where $|k| = q$) is defined to be

$$\varphi_q(x) = x^q.$$

Definition (Geometric Frobenius)**.** The *geometric Frobenius* is

$$\mathrm{Frob}_q = \varphi_q^{-1} \in \mathrm{Gal}(\bar{k}/k).$$

Definition (Tame mod n character)**.** The *tame mod n character* is the map $t(n) : I_F = \mathrm{Gal}(\bar{F}/F^{ur}) \to \mu_n(\bar{k})$ given by

$$\gamma \mapsto \gamma(\pi_n)/\pi_n \pmod{\pi}.$$

1.2 Local class field theory

Definition (Weil group)**.** Let F be a non-Archimedean local field. Then the *Weil group* of F is the topological group W_F defined as follows:

- As a group, it is

  $$W_F = \{\gamma \in \Gamma_F \mid \gamma|_{F^{ur}} = \mathrm{Frob}_q^n \text{ for some } n \in \mathbb{Z}\}.$$

  Recall that $\mathrm{Gal}(F^{ur}/F) = \hat{\mathbb{Z}}$, and we are requiring $\gamma|_{F^{ur}}$ to be in $\mathbb{Z}$. In particular, $I_F \subseteq W_F$.

- The topology is defined by the property that I_F is an *open* subgroup with the profinite topology. Equivalently, W_F is a fiber product of topological groups

  $$\begin{array}{ccc} W_F & \hookrightarrow & \Gamma_F \\ \downarrow & & \downarrow \\ \mathbb{Z} & \hookrightarrow & \hat{\mathbb{Z}} \end{array}$$

  where $\mathbb{Z}$ has the discrete topology.

Definition (Relative Weil group)**.** Let F be a non-Archimedean local field, and E/F Galois but not necessarily finite. We define

$$W_{E/F} = \{\gamma \in \mathrm{Gal}(E^{\mathrm{ab}}/F) : \gamma|_{F^{ur}} = \mathrm{Frob}_q^n, n \in \mathbb{Z}\} = \frac{W_F}{\overline{[W_E, W_E]}}.$$

with the quotient topology.

1.3 Global class field theory

Definition (Global field)**.** A *global field* is a number field or $k(C)$ for a smooth projective absolutely irreducible curve $C/\mathbb{F}_q$, i.e. a finite extension of $\mathbb{F}_q(t)$.

Definition (Place)**.** Let K be a global field. Then a *place* is a valuation on K. If K is a number field, we say a valuation v is a *finite place* if it is the valuation at a prime $\mathfrak{p} \lhd \mathcal{O}_K$. A valuation v is an *infinite place* if comes from a complex or real embedding of K. We write Σ_K for the set of places of K, and Σ_K^∞ and $\Sigma_{K,\infty}$ for the sets of finite and infinite places respectively. We also write $v \nmid \infty$ if v is a finite place, and $v \mid \infty$ otherwise.

If K is a function field, then all places are are finite, and these correspond to closed points of the curve.

Notation. If v is a finite place, we write $\mathcal{O}_v \subseteq K_v$ for the valuation ring of the completion.

Definition (Adele)**.** The *adeles* is defined to be the restricted product

$$\mathbb{A}_K = \prod_v{}' K_V = \left\{(x_v)_{v \in K_v} : x_v \in \mathcal{O}_v \text{ for all but finitely many } v \in \Sigma_K^\infty\right\}.$$

We can write this as $K_\infty \times \hat{K}$ or $\mathbb{A}_{K,\infty} \times \mathbb{A}_K^\infty$, where

$$K_\infty = \mathbb{A}_{K,\infty} = K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

consists of the product over the infinite places, and

$$\hat{K} = \mathbb{A}_K^\infty = \prod_{v\nmid\infty}{}' K_V = \bigcup_{S \subseteq \Sigma_K^\infty \text{ finite}} \prod_{v \in S} K_v \times \prod_{v \in \Sigma_K^\infty \setminus S} \mathcal{O}_v.$$

This contains $\hat{\mathcal{O}}_K = \prod_{v\nmid\infty} \mathcal{O}_K$. In the case of a number field, $\hat{\mathcal{O}}_K$ is the profinite completion of $\mathcal{O}_K$. More precisely, if K is a number field then

$$\hat{\mathcal{O}}_K = \lim_{\mathfrak{a}} \mathcal{O}_K/\mathfrak{a} = \lim \mathcal{O}_K/N\mathcal{O}_K = \mathcal{O}_K \otimes_{\mathbb{Z}} \hat{\mathbb{Z}},$$

where the last equality follows from the fact that $\mathcal{O}_K$ is a finite $\mathbb{Z}$-module.

Definition (Idele)**.** The *ideles* is the restricted product

$$J_K = \mathbb{A}_K^\times = \prod_v{}' K_v^\times = \left\{(x_v)_v \in \prod K_v^\times : x_v \in \mathcal{O}_v^\times \text{ for almost all } v\right\}.$$

Definition (Idele class group)**.** The *idele class group* is then

$$C_K = J_K/K^\times.$$

Definition (Ramification)**.** If $v \mid \infty$ is a real place of K, and L/K is a finite abelian extension, then we say v is ramified if for some (hence all) places w of L above v, w is complex.

Definition (Content homomorphism)**.** The *content homomorphism* is the map

$$\begin{aligned} c : J_K &\to \text{ fractional ideals of } K \\ (x_v)_v &\mapsto \prod_{v\nmid\infty} \mathfrak{p}_v^{v(x_v)}, \end{aligned}$$

where $\mathfrak{p}_v$ is the prime ideal corresponding to v. We ignore the infinite places completely.

Definition (Modulus)**.** A *modulus* is a finite formal sum

$$\mathfrak{m} = \sum_{v \in \Sigma_k} m_v \cdot (v)$$

of places of K, where $m_v \geq 0$ are integers.

Definition ($\mathfrak{a}(\infty)$)**.** If $\mathfrak{a} \lhd \mathcal{O}_K$ is an ideal, we write $\mathfrak{a}(\infty)$ for the modulus with $m_v = v(\mathfrak{a})$ for all $v \nmid \infty$, and $m_v = 1$ for all $v \mid \infty$.

Definition (Ray class field)**.** If L/K is abelian with $\mathrm{Gal}(L/K) \cong J_K/K^\times U_\mathfrak{m}$ under the Artin map, we call L the *ray class field* of K modulo $\mathfrak{m}$.

Definition (Conductor)**.** If L corresponds to $U \subseteq J_K$, then $U \supseteq K^\times U_\mathfrak{m}$ for some $\mathfrak{m}$. The minimal such $\mathfrak{m}$ is the *conductor* of L/K.

1.4 Ideal-theoretic description of global class field theory

Definition (Ray class group)**.** Let $\mathfrak{m}$ be a modulus. The *generalized ideal class group*, or *ray class group* modulo $\mathfrak{m}$ is

$$\mathrm{Cl}_\mathfrak{m}(K) = I_S/P_\mathfrak{m}.$$

2 L-functions

2.1 Hecke characters

Definition (Hecke character)**.** A *Hecke character* is a continuous (not necessarily unitary) homomorphism

$$\chi : J_K/K^\times \to \mathbb{C}^\times.$$

Definition (Unramified character)**.** If F is a local field, a character $\chi : F \to \mathbb{C}^\times$ is *unramified* if

$$\chi|_{\mathcal{O}_F^\times} = 1.$$

If $F \cong \mathbb{R}$, we say $\chi : F^\times \to \mathbb{C}^\times$ is unramified if $\chi(-1) = 1$.

Definition (Algebraic homomorphism)**.** A homomorphism $K^\times \to \mathbb{C}^\times$ is *algebraic* if there exists integers $n(\sigma)$ (for all $\sigma : K \hookrightarrow \mathbb{C}$) such that

$$\varphi(x) = \prod \sigma(x)^{n(\sigma)}.$$

Definition (Algebraic Hecke character)**.** A Hecke character $\chi = \chi_\infty \chi^\infty : J_K/K^\times \to \mathbb{C}^\times$ is *algebraic* if there exists an algebraic homomorphism $\varphi : K^\times \to \mathbb{C}^\times$ such that $\varphi(x) = \chi_\infty(x)$ for all $x \in K_\infty^{\times,0}$, i.e. $\chi_\infty = \varphi \prod_{v \text{ real}} \operatorname{sgn}_v^{e_v}$ for $e_v \in \{0, 1\}$.

We say φ (or the tuple $(n(\sigma))_\sigma$) is the *infinite type* of χ.

Definition (Serre type)**.** A homomorphism $\varphi : K^\times \to \mathbb{C}^\times$ is of *Serre type* if it is algebraic and $\varphi(\mathcal{O}_K^\times)$ is finite.

Definition (CM field)**.** K is a CM field if K is a totally complex quadratic extension of a totally real number field K^+.

2.2 Abelian L-functions

Definition (Hecke L-function)**.** Let $\chi : C_K \to \mathbb{C}^\times$ be a Hecke character. For $v \in \Sigma_K$, we define local L-factors $L(\chi_v)$ as follows:

- If v is non-Archimedean and χ_v unramified, i.e. $\chi_v|_{\mathcal{O}_{K_v}^\times} = 1$, we set

$$L(\chi_v) = \frac{1}{1 - \chi_v(\pi_v)}.$$

- If v is non-Archimedean and χ_v is ramified, then we set

$$L(\chi_v) = 1.$$

- If v is a real place, then χ_v is of the form

$$\chi_v(x) = x^{-N} |x|_v^s,$$

  where $N = 0, 1$. We write

$$L(\chi_v) = \Gamma_\mathbb{R}(s) = \pi^{-s/2}\Gamma(s/2).$$

– If v is a complex place, then χ_v is of the form

$$\chi_v(x) = \sigma(x)^{-N}|x|_v^s,$$

where σ is an embedding of K_v into $\mathbb{C}$ and $N \geq 0$. Then

$$L(\chi_v) = \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$$

We then define

$$L(\chi_v, s) = L(\chi_v \cdot |\ \cdot\ |_v^s).$$

So for finite unramified v, we have

$$L(\chi_v, s) = \frac{1}{1 - \chi_v(\pi_v)q_v^{-s}},$$

where $q_v = |\mathcal{O}_{K_v}/(\pi_v)|$.

Finally, we define

$$L(\chi, s) = \prod_{v \nmid \infty} L(\chi_v, s)$$
$$\Lambda(\chi, s) = \prod_{v} L(\chi_v, s).$$

2.3 Non-abelian L-functions

Definition. Let F be local and non-Archimedean. Let $\rho : W_F \to \mathrm{GL}_{\mathbb{C}}(V)$ be a representation. Then we define

$$L(\rho, s) = \det(1 - q^{-s}\rho(\mathrm{Frob}_F)|_{V^{I_F}})^{-1},$$

where V^{I_F} is the invariants under I_F.

3 ℓ-adic representations

Definition (ℓ-adic representation)**.** Let G be a topological group. An *ℓ-adic representation* consists of the following data:

- A finite extension $E/\mathbb{Q}_\ell$;
- An E-vector space V; and
- A continuous homomorphism $\rho : G \to \mathrm{GL}_E(V) \cong \mathrm{GL}_n(E)$.

Definition (Weil–Deligne representation)**.** A *Weil–Deligne representation* of W_F over a field E of characteristic 0 is a pair (ρ, N), where

- $\rho : W_F \to \mathrm{GL}_E(V)$ is a finite-dimensional representation of W_F over E with open kernel; and
- $N \in \mathrm{End}_E(V)$ is nilpotent such that for all $\gamma \in W_F$, we have

$$\rho(\gamma)N\rho(\gamma)^{-1} = \omega(\gamma)N,$$

Definition (Weil–Langlands group)**.** We define the *(Weil–)Langlands group* to be

$$\mathcal{L}_F = W_F \times \mathrm{SU}(2).$$

4 The Langlands correspondence

4.1 Representations of groups

Definition (Smooth representation)**.** A *smooth representation* of G is a continuous representation of G over $\mathbb{C}$, where $\mathbb{C}$ is given the discrete topology. That is, it is a pair (π, V) where V is a complex vector space and $\pi : G \to \mathrm{GL}_{\mathbb{C}}(V)$ a homomorphism such that for every $v \in V$, the stabilizer of v in G is open.

Definition (Admissible representation)**.** We say (π, V) is *admissible* if for every open compact subgroup $K \subseteq G$ the fixed set $V^K = \{v \in V : \pi(g)v = v \; \forall g \in K\}$ is finite-dimensional.

4.2 Hecke algebras

Notation. We write $C_c^\infty(G)$ for the vector space of locally constant functions $f : G \to \mathbb{C}$ of compact support.

Definition (Hecke algebra)**.** The *Hecke algebra* is defined to be

$$\mathcal{H}(G, K) = \{\varphi \in C_c^\infty(G) : \varphi(kgk') = \varphi(g) \text{ for all } k, k' \in K\}.$$

This is spanned by the characteristic functions of double cosets KgK.

Definition (Convolution product)**.** The *convolution product* on $\mathcal{H}(G, K)$ is

$$(\varphi * \varphi')(g) = \int_G \varphi(x)\varphi'(x^{-1}g) \, \mathrm{d}\mu(x).$$

Observe that this integral is actually a finite sum.

4.3 The Langlands classification

Definition (Contragredient)**.** Let (π, V) be a smooth representation. We define $V^* = \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$, and the representation (π^*, V^*) of G is defined by

$$\pi_*(g)\ell = (v \mapsto \ell(\pi(g^{-1})v)).$$

We then define the *contragredient* $(\tilde{\pi}, \tilde{v})$ to be the subrepresentation

$$\tilde{V} = \{\ell \in V^* \text{ with open stabilizer}\}.$$

Definition (Matrix coefficient)**.** Let (π, V) be a smooth representation, and $v \in V$, $\ell \in \tilde{V}$. The *matrix coefficient* $\pi_{v,\ell}$ is defined by

$$\pi_{v,\ell}(g) = \ell(\pi(g)v).$$

This is a locally constant function $G \to \mathbb{C}$.

Definition (Square integrable representation)**.** Let (π, V) be an irreducible smooth representation of G. We say it is *square integrable* if ω_π is unitary and

$$|\pi_{v,\ell}| \in L^2(G/Z)$$

for all (v, ℓ).

Definition (Tempered representation)**.** Let (π, V) be irreducible, ω_π unitary. We say it is *tempered* if for all (v, ℓ) and $\varepsilon > 0$, we have

$$|\pi_{v,\ell}| \in L^{2+\varepsilon}(G/Z).$$

Definition (Essentially square integrable)**.** Let (π, V) be irreducible. Then (π, V) is *essentially square integrable* (or *essentially tempered*) if

$$\pi \otimes (\chi \circ \det)$$

is square integrable (or tempered) for some character $\chi : F^\times \to \mathbb{C}$.

Definition (Supercuspidal representation)**.** We say π is *supercuspidal* if for all (v, ℓ), the support of $\pi_{v,\ell}$ is compact mod Z.

Definition (Induced representation)**.** Let $\chi : B \to \mathbb{C}$ be a character. We define the induced representation $\mathrm{Ind}_B^G(\chi)$ to be the space of locally constant functions $f : g \to \mathbb{C}$ such that

$$f(bg) = \chi(b)\delta_B(b)^{1/2} f(g)$$

for all $b \in B$ and $g \in G$, where G acts by

$$\pi(g)f : x \mapsto f(xg).$$

The function $\delta_B(b)^{1/2}$ is defined by

$$\delta_B(b) = |\det \mathrm{ad}_B(b)|.$$

More explicitly, if the diagonal entries of $b \in B$ are $x_1, \ldots, x_n$, then

$$\delta_B(b) = \prod_{i=1}^n |x_i|^{n+1-2i} = |x_1|^{n-1}|x_2|^{n-3} \cdots |x_n|^{-n+1}$$

This is a smooth representation since $B \backslash G$ is compact. In fact, it is admissible and of finite length.

When this is irreducible, it is said to be a *principle series representation* of G.

4.4 Local Langlands correspondence

5 Modular forms and representation theory