Galois Representations

Sommersemester 2008

Universität Duisburg-Essen

Gabor Wiese

gabor.wiese@uni-due.de

Version of 13th February 2012

Preface

This lecture gives an introduction to the theory of Galois representations. It consists of the following three main parts.

- In a long introduction we introduce the necessary terminology, give and sketch principal examples (e.g. cyclotomic character, Galois representations attached to elliptic curves, abelian varieties and modular forms) and introduce L-functions.
- The next chapter is on general representation theory. Among other things, the Brauer-Nesbitt theorem is proved and fields of definition of Galois representations are discussed.
- The third chapter is devoted to the local theory of Galois representations. For an ℓ-adic and a mod ℓ Galois representation there are huge differences between the local representation at $p \neq \ell$ and the one at ℓ. We define and discuss conductors for Artin representations and ℓ-adic and mod ℓ representations away from ℓ. We also introduce Weil-Deligne representations that serve to classify these. Moreover, also the local representation at ℓ is discussed in so far that fundamental characters are introduced. The goal of this chapter is the precise formulation of Serre's modularity conjecture.
- A planned fourth chapter on complex Galois representations could not be realized due to time constraints. It was planned to focus on the 1-dimensional case. This can be used to sketch a proof of Chebotarev's density theorem. Finally, it would have been nice to discuss how the Mellin transformation and its inverse allows to move between modular forms and their L-functions. Consequences for Artin's conjecture could also have been be mentioned.

(These notes should be reworked. G.W.)

Contents

1 Introduction **4**

1.1 Representations of a profinite group 4

1.2 Galois representations 6

1.3 Principal examples of Galois representations 12

1.4 L-functions 17

2 General representation theory **20**

2.1 Simple and semi-simple rings and modules 21

2.2 Scalar extensions 27

2.3 Splitting fields 30

2.4 Character theory 34

2.5 Definability of Galois representations 37

3 Local theory **42**

3.1 Conductor 42

3.2 Weil-Deligne representations 60

3.3 Serre's conjecture 65

Chapter 1

Introduction

In this chapter we will

- define Galois representations,
- introduce basic properties, such as the representation being unramified,
- give some of the motivating geometric examples and
- define L-functions.

1.1 Representations of a profinite group

Definition 1.1.1 *Let G be a profinite group and let k be a topological field. By an n-*dimensional representation of *G we mean a continuous homomorphism of groups*

$$\rho : G \to \mathrm{GL}_n(k).$$

Example 1.1.2 *(1) If G is a finite group with the discrete topology and k are the complex numbers, then we are in the context of the standard theory of representations of finite groups.*

(2) More concretely: $\mathbb{Z}/N\mathbb{Z} \to \mathrm{GL}_1(\mathbb{C})$, $1 \mapsto \zeta_N = e^{2\pi i/N}$.

(3) For a finite group G the regular representation *is defined by the natural left G-action on the group algebra $\mathbb{C}[G]$.*

(4) We have the augmentation exact sequence

$$0 \to I_G \to \mathbb{C}[G] \xrightarrow{g \mapsto 1} \mathbb{C} \to 0$$

with the aumentation ideal $I_G = (g-1) \lhd \mathbb{C}[G]$.

The left action of G on I_G gives rise to the augmentation representation.

(5) Let M be any $\mathbb{C}[G]$-module. Then G also acts on $\mathrm{End}_{\mathbb{C}}(M)$ by $(g.\sigma)(m) = g.(\sigma(g^{-1}.m))$ for $g \in G$, $m \in M$ and $\sigma \in \mathrm{End}_{\mathbb{C}}(M)$. This representation is called the adjoint representation of M. *Thinking about this representation in terms of matrices, g acts by conjugation. Hence, the augmentation representation can be restricted to the matrices of trace 0.*

We always consider $\overline{\mathbb{F}}_l$ with the discrete topology.

Definition 1.1.3 *Let ρ be an n-dimensional representation of G over k.*

(a) The representation ρ is called

- *an* Artin representation *if $k \subseteq \mathbb{C}$ (topological subfield),*
- *an* l-adic representation *if $k \subseteq \overline{\mathbb{Q}}_l$,*
- *a* mod l representation *if $k \subseteq \overline{\mathbb{F}}_l$.*

(b) The representation ρ is called

- abelian *if $\rho(G)$ is an abelian group,*
- dihedral *if $\rho(G)$ is a dihedral group, etc.*

Definition 1.1.4 *Two n-dimensional representations ρ_1 and ρ_2 of G over k are called* equivalent *if there exists some $M \in \mathrm{GL}_n(k)$ such that for all $g \in G$*

$$\rho_1(g) = M\rho_2(g)M^{-1}.$$

Proposition 1.1.5 *Let G be a profinite group, k a topological field and $\rho : G \to \mathrm{GL}_n(k)$ a representation. The image of ρ is finite in any of the three cases:*

(a) ρ is an Artin representation,

(b) ρ is a mod l representation,

(c) G is a pro-p-group and ρ is an l-adic representation with $l \neq p$.

Proof. Exercise 1. □

Proposition 1.1.6 *Let k be a local field with complete discrete valuation ring $\mathcal{O}$, maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F} = \mathcal{O}/\mathfrak{m}$ of characteristic l. Let G be a profinite group and $\rho : G \to \mathrm{GL}_n(k)$ a representation. Then there exists a representation*

$$\rho_1 : G \to \mathrm{GL}_n(\mathcal{O})$$

such that

$$G \xrightarrow{\rho_1} \mathrm{GL}_n(\mathcal{O}) \xrightarrow{\text{inclusion}} \mathrm{GL}_n(k)$$

is equivalent to ρ.

Proof. Exercise 2. □

Definition 1.1.7 *Assume the set-up of Proposition 1.1.6. The composition*

$$\overline{\rho} : G \xrightarrow{\rho_1} \mathrm{GL}_n(\mathcal{O}) \xrightarrow{\text{natural projection}} \mathrm{GL}_n(\mathbb{F})$$

is called a mod l reduction of ρ*.*

Remark 1.1.8 *The reduction depends on the choice of ρ_1. Later we will see (Brauer-Nesbitt theorem) that the semi-simplification of $\overline{\rho}$ is independent of this choice.*

1.2 Galois representations

We assume infinite Galois theory. A good reference is [Neukirch], Section IV.1.

Definition 1.2.1 *Let K be a field. We denote by G_K the absolute Galois group of K, i.e. the Galois group of a separable closure of G.*

Let k be a topological field. A representation of G_K over k is called a Galois representation*.*

If K is a global field (e.g. a number field), then a representation of G_K is called a global Galois representation*. If K is a local field, then we speak of a* local Galois representation*.*

Remark 1.2.2 *One often hears about* ℓ-adic Galois representations *(or even* elladic *ones) as compared to* p-adic Galois representations*. In that case, what people usually mean the following: Let*

$$G_K \to \mathrm{GL}_n(k)$$

be an n-dimensional Galois representation with K a finite extension of $\mathbb{Q}_p$ and k a finite extension of $\mathbb{Q}_l$. The situation $l \neq p$ is referred to as ℓ-adic, and the situation $l = p$ as p-adic.

The behaviour is fundamentally different! Wild inertia (to be explained in a second), which is a pro-p group, has a finite image in the first case (by Proposition 1.1.5), but it can have a very large image in the second case. We will go into that in the chapter on local Galois representations in a bit more detail.

Before we can go on, we need to recall some algebraic number theory. We start by the finite situation. Let K be a number field and $\mathfrak{p}$ a prime. Then we can complete K at $\mathfrak{p}$ (with respect to the non-archimedean absolute value attached to $\mathfrak{p}$ or by completing the ring of integers of K at $\mathfrak{p}$ in the sense of commutative algebra) to obtain $K_\mathfrak{p}$, a finite extension of $\mathbb{Q}_p$, where $(p) = \mathbb{Z} \cap \mathfrak{p}$ is the rational prime number lying under $\mathfrak{p}$. Then $K_\mathfrak{p}$ is a local field with a non-archimedean absolute value $| \cdot |$, discrete valuation ring

$$\mathcal{O}_{K_\mathfrak{p}} = \mathcal{O}_\mathfrak{p} = \{x \in K_\mathfrak{p} \mid \ | x |\leq 1\}$$

and valuation ideal

$$\widehat{\mathfrak{p}} = \{x \in K_\mathfrak{p} \mid \ | x |< 1\}.$$

We shall also write $\mathfrak{p}$ for $\widehat{\mathfrak{p}}$. In the sequel we need and assume that the absolute value $|\cdot|$ is *correctly normalized*. For the residue fields, we shall use the notation

$$\mathbb{F}(\mathfrak{p}) = \mathbb{F}(K_{\mathfrak{p}}) := \mathcal{O}_{\mathfrak{p}}/\widehat{\mathfrak{p}}.$$

The residue field can also be seen as the quotient of the ring of integers of K by $\mathfrak{p}$.

Now we move on to discuss finite Galois extensions. Let L/K be a finite Galois extension of number fields and $\mathfrak{P}/\mathfrak{p}/p$ prime ideals in these fields. The *decomposition group of* $\mathfrak{P}$ is defined as

$$D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) | \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

It is naturally isomorphic to the local Galois group

$$D(\mathfrak{P}/\mathfrak{p}) \cong \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}).$$

Indeed, recall that L is dense in $L_{\mathfrak{P}}$ and K in $K_{\mathfrak{p}}$. An automorphism $\sigma \in D(\mathfrak{P}/\mathfrak{p})$ can be uniquely extended by continuity to an automorphism in the local Galois group. To go in the converse direction, one just restricts the automorphism to L.

Whenever we have a Galois extension of local fields $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, we can consider the reduction mod $\mathfrak{P}$ of all field automorphisms in $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, since each of them fixes the valuation rings. The reduction map

$$\pi(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = \pi(\mathfrak{P}/\mathfrak{p}) : \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(\mathbb{F}(\mathfrak{P})/\mathbb{F}(\mathfrak{p}))$$

is surjective. To see the surjectivity, we consider $L_{\mathfrak{P}}$ as $K_{\mathfrak{p}}[X]/(f(X))$ with f an irreducible polynomial (monic and with coefficients in $\mathcal{O}_{\mathfrak{p}}$) of degree equal to $[L_{\mathfrak{P}} : K_{\mathfrak{p}}]$. Let us fix a root α of f. An element in the Galois group is uniquely given by the image of α, i.e. the Galois group consists of the elements σ_β with $\sigma_\beta(\alpha) = \beta$. The factorization of f mod $\mathfrak{p}$ is of the form $g(X)^e$ and the reduction $\overline{\alpha}$ of α is a root of g. An element $\overline{\sigma} \in \mathrm{Gal}(\mathbb{F}(\mathfrak{P})/\mathbb{F}(\mathfrak{p}))$ is uniquely given by the image $\overline{\sigma}(\overline{\alpha})$, which is of the form $\overline{\beta}$ with β a root of f. Hence, σ_β reduces to $\overline{\sigma}$, showing the surjectivity.

A canonical generator of $\mathrm{Gal}(\mathbb{F}(\mathfrak{P})/\mathbb{F}(\mathfrak{p}))$ is given by the (arithmetic) *Frobenius endomorphism* (or *Frobenius element*) $\mathrm{Frob}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = \mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$ which is defined as $x \mapsto x^q$ with $q = \#\mathbb{F}(\mathfrak{p}) = N(\mathfrak{p})$. The integer $N(\mathfrak{p})$ is called the *norm of* $\mathfrak{p}$. The kernel of the reduction map is called the *inertia group* $I(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = I(\mathfrak{P}/\mathfrak{p})$, so that we have the exact sequence

$$0 \to I(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \xrightarrow{\pi(L_{\mathfrak{P}}/K_{\mathfrak{p}})} \mathrm{Gal}(\mathbb{F}(\mathfrak{P})/\mathbb{F}(\mathfrak{p})) \to 0.$$

The field extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ (or the prime $\mathfrak{P}$ above $\mathfrak{p}$) is *unramified* if and only if $I(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is trivial, i.e. if and only if the reduction map $\pi(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is an isomorphism. The inertia group $I(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ has a unique p-Sylow group $P(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = P(\mathfrak{P}/\mathfrak{p})$, which is called the *wild inertia group*. The field extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ (or the prime $\mathfrak{P}$ above $\mathfrak{p}$) is *tamely ramified* if $P(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is trivial; otherwise, it is called *wildly ramified*.

Now we investigate what happens if we change the prime $\mathfrak{P}$ lying above a fixed $\mathfrak{p}$ in the Galois extension L/K. One knows that any other prime is of the form $\sigma(\mathfrak{P})$ with $\sigma \in \mathrm{Gal}(L/K)$. Then we clearly have

$$D(\sigma(\mathfrak{P})/\mathfrak{p}) = \sigma \circ D(\mathfrak{P}/\mathfrak{p}) \circ \sigma^{-1}$$

and, consequently, similar statements for $I(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ and $P(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. Hence, if the extension L/K is unramified (or tamely ramified) at one $\mathfrak{P}$, then so it is at all $\sigma(\mathfrak{P})$, whence we say that L/K is unramified (or tamely ramified) at the 'small' ideal $\mathfrak{p}$.

Suppose L/K is unramified at $\mathfrak{p}$, so that the reduction map $\pi(\mathfrak{P}/\mathfrak{p})$ is an isomorphism. We can thus consider $\mathrm{Frob}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ as an element of $D(\mathfrak{P}/\mathfrak{p})$. We have

$$\mathrm{Frob}(\sigma(\mathfrak{P})/\mathfrak{p}) = \sigma \circ \mathrm{Frob}(\mathfrak{P}/\mathfrak{p}) \circ \sigma^{-1},$$

so that the Frobenius elements of the primes lying over $\mathfrak{p}$ form a conjugacy class in $\mathrm{Gal}(L/K)$. We will often write $\mathrm{Frob}_{\mathfrak{p}}$ for either this conjugacy class or any element in it.

Our next goal is to pass to infinite Galois extensions. For that it is often useful to take an *embedding point of view* on primes. We fix once and for all algebraic closures $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}}_p$ for all p. The field $\overline{\mathbb{Q}}_p$ also has an absolute value $|\cdot|$ which is chosen such that the restriction of $|\cdot|$ to any finite extension of $\mathbb{Q}_p$ contained in $\overline{\mathbb{Q}}_p$ gives the standard absolute value on that field.

Let $K \subset \overline{\mathbb{Q}}$ be a number field (even if we do not write the inclusion into our fixed $\overline{\mathbb{Q}}$, we often mean it). A prime $\mathfrak{p}$ lying above p is the same as an embedding of K into $\overline{\mathbb{Q}}_p$. Indeed, we can see the completion $K_{\mathfrak{p}}$ as a subfield of $\overline{\mathbb{Q}}_p$; and given an embedding $\iota : K \hookrightarrow \overline{\mathbb{Q}}_p$ we obtain an ideal $\mathfrak{p}$ as the inverse image under ι of the valuation ideal of $\overline{\mathbb{Q}}_p$. This allows us to generalize the above discussion and it also enables us to view $\overline{\mathbb{Q}}_p$ and $\mathbb{C}$ on an equal footing. The role of the 'choice of a prime above $\mathfrak{p}$' is now played by embeddings.

Let again K be a number field (inside $\overline{\mathbb{Q}}$) and fix an embedding $\iota_{\mathfrak{p}} : K \hookrightarrow \overline{\mathbb{Q}}_p$. Consider an embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ extending $\iota_{\mathfrak{p}}$. It corresponds to choices of prime ideals above $\mathfrak{p}$ for *every* extension $K \subseteq L \subset \overline{\mathbb{Q}}$ which are compatible with intersection. We also obtain an embedding of absolute Galois groups

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_{\mathfrak{p}}) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/K), \quad \sigma \mapsto \iota^{-1} \circ \sigma \circ \iota.$$

Note that this definition makes sense, since $\overline{\mathbb{Q}}/K$ is a normal extension. If we have two such embeddings ι_1 and ι_2, then the two embeddings of Galois groups are conjugate by $\iota_1 \circ \iota_2^{-1}$, just as in the case of finite primes.

Let $K_{\mathfrak{p}} \subset L_{\mathfrak{P}} \subset M_{\tilde{\mathfrak{P}}}$ be finite degree subfields of $\overline{\mathbb{Q}}_p$. We obtain a projective system of short exact sequences:

$$\begin{tikzcd}
0 \arrow[r] & I(M_{\tilde{\mathfrak{P}}}/K_{\mathfrak{p}}) \arrow[r] \arrow[d, two heads] & \mathrm{Gal}(M_{\tilde{\mathfrak{P}}}/K_{\mathfrak{p}}) \arrow[r, "\pi(M_{\tilde{\mathfrak{P}}}/K_{\mathfrak{p}})"] \arrow[d, two heads] & \mathrm{Gal}(\mathbb{F}(\tilde{\mathfrak{P}})/\mathbb{F}(\mathfrak{p})) \arrow[r] \arrow[d, two heads] & 0 \\
0 \arrow[r] & I(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \arrow[r] & \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \arrow[r, "\pi(L_{\mathfrak{P}}/K_{\mathfrak{p}})"] & \mathrm{Gal}(\mathbb{F}(\mathfrak{P})/\mathbb{F}(\mathfrak{p})) \arrow[r] & 0.
\end{tikzcd}$$

The projective limit over compact sets is exact, hence, we obtain the exact sequence

$$0 \to I_{K_{\mathfrak{p}}} \to G_{K_{\mathfrak{p}}} \xrightarrow{\pi_{\mathfrak{p}}} G_{\mathbb{F}(\mathfrak{p})} \to 0,$$

where $I_{K_{\mathfrak{p}}} = I_{\mathfrak{p}}$ is the projective limit over the inertia groups. With the same reasoning we obtain that the projective limit $P_{K_{\mathfrak{p}}} = P_{\mathfrak{p}}$ over the wild inertia groups is equal to the (necessarily unique) pro-p Sylow group of $I_{K_{\mathfrak{p}}}$. We again call $I_{K_{\mathfrak{p}}}$ and $P_{K_{\mathfrak{p}}}$ the *inertia (group)* respectively the *wild inertia (group) of $K_{\mathfrak{p}}$ (or of $\mathfrak{p}$)*. By $\mathrm{Frob}_{\mathfrak{p}}$ we denote the Frobenius element in $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}(\mathfrak{p}))$.

We can see complex conjugation as a variant of this. Suppose there is an embedding τ_∞ of K into $\mathbb{R}$. Then for any embedding $\tau : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ extending τ_∞, the map

$$\tau^{-1} \circ \text{(complex conjugation in } \mathbb{C}/\mathbb{R}) \circ \tau$$

defines an element of G_K. It is called *a complex conjugation*. Again, all complex conjugations are conjugate.

Now we come to the very important definition of unramified and tamely ramified Galois representations. We start with the local case.

Definition 1.2.3 *Let $K_{\mathfrak{p}}$ be a finite extension of $\mathbb{Q}_p$ and let k be any topological field. Consider a local Galois representation $\rho : G_{K_{\mathfrak{p}}} \to \mathrm{GL}_n(k)$. It is called*

- unramified *if $\rho(I_{K_{\mathfrak{p}}}) = 0$,*
- tamely ramified *if $\rho(P_{K_{\mathfrak{p}}}) = 0$.*

Let ρ be a representation as in the definition and let V be the k-vector space underlying it, i.e. such that $\rho : G_{K_{\mathfrak{p}}} \to \mathrm{GL}_n(k) = \mathrm{GL}(V)$. Denote by $V^{I_{K_{\mathfrak{p}}}}$ the sub-vector space $V^{\rho(I_{K_{\mathfrak{p}}})}$ of V consisting of the elements fixed by $I_{K_{\mathfrak{p}}}$. We obtain the unramified representation

$$\rho^{I_{K_{\mathfrak{p}}}} : G_{K_{\mathfrak{p}}} \to \mathrm{GL}(V^{I_{K_{\mathfrak{p}}}}) = \mathrm{GL}_m(k)$$

for some $m \leq n$. Clearly, ρ is unramified if and only if $\rho = \rho^{I_{K_{\mathfrak{p}}}}$.

Evaluating an unramified representation at the Frobenius element makes sense, since any preimage under $\pi_{K_{\mathfrak{p}}}$ of $\mathrm{Frob}_{K_{\mathfrak{p}}}$ is uniquely determined up to a trivially acting element from $I_{K_{\mathfrak{p}}}$.

Definition 1.2.4 *The* characteristic polynomial of Frobenius of ρ *is defined as*

$$\Phi(\rho)(X) := \mathrm{charpoly}(\rho^{I_{K_\mathfrak{p}}}(\mathrm{Frob}_{K_\mathfrak{p}})) = \det(X - \mathrm{Frob}_{K_\mathfrak{p}} \mid V^{I_{K_\mathfrak{p}}}) \in k[X].$$

Very often one sees a slightly different version, namely

$$\tilde{\Phi}(\rho)(X) := \det(1 - X\,\mathrm{Frob}_{K_\mathfrak{p}} \mid V^{I_{K_\mathfrak{p}}}) \in k[X].$$

We have the relation

$$\tilde{\Phi}(\rho)(X) = X^n \cdot \Phi(\rho)(X^{-1}).$$

Now we treat the global situation.

Definition 1.2.5 *Let K be a number field (inside $\overline{\mathbb{Q}}$), and k any topological field. Consider a global Galois representation $\rho : G_K \to \mathrm{GL}_n(k)$. Let $\mathfrak{p}$ be a prime of K corresponding to an embedding $\iota_\mathfrak{p} : K \hookrightarrow \overline{\mathbb{Q}}_p$. Choose any embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ extending $\iota_\mathfrak{p}$, giving rise to an embedding of $G_{K_\mathfrak{p}}$ into G_K. The Galois representation ρ is called* unramified (respectively, tamely ramified) at $\mathfrak{p}$ *if the restriction of ρ to $G_{K_\mathfrak{p}}$ is unramified (respectively, tamely ramified).*

We also define the characteristic polynomial of Frobenius at $\mathfrak{p}$ *as*

$$\Phi_\mathfrak{p}(\rho) := \Phi(\rho|_{G_{K_\mathfrak{p}}}) \in k[X]$$

and

$$\tilde{\Phi}_\mathfrak{p}(\rho) := \tilde{\Phi}(\rho|_{G_{K_\mathfrak{p}}}) \in k[X].$$

Note that these properties do not depend on the choice of ι (for the statement on the characteristic polynomial we use that conjugate matrices have the same characteristic polynomial).

Definition 1.2.6 *Let ρ be as in the previous definition with $n = 1, 2$. Then ρ is called* odd *if the image of all complex conjugations has determinant -1.*

I have seen different definitions of odd representations for $n > 2$, and I am not sure which one is the ’correct’ one.

The Frobenius elements play a very special role in the theory. Their images determine the Galois representation uniquely. This is a consequence of Chebotarev’s density theorem.

Recall that the norm of an ideal is denoted as $N(\mathfrak{p}) = \#\mathbb{F}(\mathfrak{p})$.

Definition 1.2.7 *Let K be a number field and S a set of primes of K.*

(a) The Dirichlet density of S *is defined as*

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

if the limit exists.

(b) The natural density of S *is defined as*

$$\delta(S) := \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in S \mid N(\mathfrak{p}) < x\}}{\#\{\mathfrak{p} \mid N(\mathfrak{p}) < x\}},$$

if the limit exists.

The existence of the natural density implies the existence of the Dirichlet density, but the converse does not hold in general.

Theorem 1.2.8 (Chebotarev's density theorem) *Let L/K be a finite Galois extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$. Let $\sigma \in G$ be any element. We use the notation $[\sigma]$ to denote the conjugacy class of σ in G. Define the set of primes*

$$P_{L/K}(\sigma) = \{\mathfrak{p} \mid [\mathrm{Frob}_{\mathfrak{p}}] = [\sigma]\}.$$

The Dirichlet density of this set is

$$d(P_{L/K}(\sigma)) = \frac{\#[\sigma]}{\#G}.$$

In other words, the Frobenius elements are uniformly distributed over the conjugacy classes of the Galois group.

We will at least give a precise sketch of the proof later this lecture and we will also present important applications. Here we provide a first one concerning Galois representations.

Corollary 1.2.9 *Let K be a number field, k a topological field and $\rho : G_K \to \mathrm{GL}_n(k)$ a global Galois representation that ramifies at most at finitely many primes of K. Then the set*

$$\{\rho(\mathrm{Frob}_{\mathfrak{p}}) | \mathfrak{p} \text{ unramified }\}$$

is a dense subset of the image $\rho(G_K)$.

In other words, the Frobenius elements topologically generate the image of the Galois representation. Hence, the Galois representation is uniquely determined by the images of the Frobenius elements.

Proof. Recall that in a profinite group G a subset $X \subset G$ is dense in G if and only if the image of X under all natural projections $G \twoheadrightarrow G_i$ is equal to G_i.

We apply this with $G = \rho(G_K)$ and X the set of Frobenius images. All the finite quotients of G correspond to finite Galois extensions and, consequently, Chebotarev's density theorem (Theorem 1.2.8) implies that the image of X in any finite quotient is all of it. □

1.3 Principal examples of Galois representations

Cyclotomic character

Let K be a field of characteristic 0 and $\overline{K}$ a separable closure. Let

$$\mu_m(\overline{K}) = \overline{K}^\times[m] = \ker\left(\overline{K}^\times \xrightarrow{x \mapsto x^m} \overline{K}^\times\right)$$

be the m-torsion points of $\overline{K}^\times$, i.e. the m-th roots of unity. By choosing a *compatible system of roots of unity* ζ_{l^n} we obtain the isomorphism of projective systems

$$\begin{tikzcd}
\mathbb{Z}/l^n\mathbb{Z} \arrow[r, "1\mapsto\zeta_{l^n}", "\sim"'] \arrow[d, two heads, "1\mapsto 1"] & \mu_{l^n}(\overline{K}) \arrow[d, two heads, "x\mapsto x^l"] \\
\mathbb{Z}/l^{n-1}\mathbb{Z} \arrow[r, "1\mapsto\zeta_{l^{n-1}}", "\sim"'] & \mu_{l^{n-1}}(\overline{K}),
\end{tikzcd}$$

giving rise to an isomorphism

$$\mathbb{Z}_l \cong \varprojlim_n \mu_{l^n}(\overline{K}^\times) =: T_l(\overline{K}^\times).$$

The object on the right is called the *l-adic Tate module of $\overline{K}^\times$*. Note that G_K acts compatibly on all objects on the right.

We can hence define a Galois representation:

$$\chi_l : G_K \xrightarrow{\sigma\mapsto\left(x\mapsto\sigma(x)\right)} \mathrm{Aut}(T_l(\overline{K}^\times)) \cong \mathbb{Z}_l^\times = \mathrm{GL}_1(\mathbb{Z}_l) \hookrightarrow \mathrm{GL}_1(\mathbb{Q}_l).$$

It is called the *l-adic cyclotomic character (over $\overline{K}$).* Alternatively, one can let

$$V_l(\overline{K}^\times) := \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l(\overline{K}^\times),$$

yielding an isomorphism $\mathbb{Q}_l \cong V_l(\overline{K}^\times)$.

The standard example is with $K = \mathbb{Q}$.

Proposition 1.3.1 *Let χ_l be the cyclotomic character over $\overline{\mathbb{Q}}$. It is a 1-dimensional global Galois representation, which is unramified at all primes $p \neq l$ and is characterized there by*

$$\chi_l(\mathrm{Frob}_p) = p.$$

More generally, we have

$$\sigma(\zeta) = \zeta^{\chi_l(\sigma)}$$

for all $\zeta \in \mu_{l^n}(\overline{K}^\times)$, all n and all $\sigma \in G_{\mathbb{Q}}$. In particular, the image of any complex conjugation is equal to -1.

Proof. Exercise 3. □

Abelian varieties

Let K be a field and A an abelian variety of dimension g over K. Let

$$A(\overline{K})[m] = \ker\left(A(\overline{K}) \xrightarrow{P \mapsto m \cdot P} A(\overline{K})\right)$$

be the m-torsion points of $A(\overline{K})$. One defines the *l-adic Tate module of A* by

$$T_l(A) := \varprojlim_n A(\overline{K})[l^n]$$

with respect to the projective system

$$A(\overline{K})[l^n] \twoheadrightarrow A(\overline{K})[l^{n-1}], \;\; P \mapsto l \cdot P.$$

If l is not the characteristic of K, then, as is well known, one can compatibly identify $A(\overline{K})[l^n]$ with $(\mathbb{Z}/l^n\mathbb{Z})^{2g}$, yielding an isomorphism

$$T_l(A) \cong (\mathbb{Z}_l)^{2g}.$$

One often puts

$$V_l(A) := T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \cong (\mathbb{Q}_l)^{2g}.$$

The absolute Galois group G_K acts on $T_l(A)$ and on $V_l(A)$, since it compatibly acts on all the $A(\overline{K})[l^n]$. This yields the *Galois representation attached to A*:

$$\rho_A : G_K \to \mathrm{Aut}_{\mathbb{Q}_l}(V_l(\overline{K})) \cong \mathrm{GL}_{2g}(\mathbb{Q}_l).$$

Theorem 1.3.2 *Let K be a number field. Then ρ_A is unramified at all primes $\mathfrak{p}$ of K at which A has good reduction.*

We will not prove this theorem in this course. Here is a more precise theorem for the special case of elliptic curves.

Theorem 1.3.3 *Let K be a number field and E an elliptic curve over K. Let $\mathfrak{p}$ be a prime of K at which E has good reduction. Then ρ_E is unramified at $\mathfrak{p}$ and we have*

$$\Phi_{\mathfrak{p}}(\rho_E) = X^2 - a_{\mathfrak{p}}X + N(\mathfrak{p})$$

and

$$\tilde{\Phi}_{\mathfrak{p}}(\rho_E) = 1 - a_{\mathfrak{p}}X + N(\mathfrak{p})X^2$$

where $a_{\mathfrak{p}} \in \mathbb{Z}$ such that

$$\#E(\mathbb{F}(\mathfrak{p})) = N(\mathfrak{p}) + 1 - a_{\mathfrak{p}} = \Phi_{\mathfrak{p}}(\rho_E)(1).$$

Furthermore, the determinant of ρ_E is equal to the cyclotomic character of K.

Modular forms

The great importance of modular forms for modern number theory is due to the fact that one may attach a 2-dimensional representation of the Galois group of the rationals to each normalised cuspidal eigenform. The following theorem is due to Shimura for $k = 2$ and due to Deligne for $k \geq 2$.

Theorem 1.3.4 *Let $k \geq 2$, $N \geq 1$, l a prime not dividing N, and $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ a character.*

Then to any normalised eigenform $f \in \mathrm{S}_k(N, \epsilon\,; \mathbb{C})$ with $f = \sum_{n\geq 1} a_n(f)q^n$ one can attach a Galois representation of the rationals

$$\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$$

such that

(i) ρ_f is irreducible (to be explained later),

(ii) ρ_f is odd,

(iii) for all primes $p \nmid Nl$ the representation ρ_f is unramified at p and

$$\Phi_p(\rho_f)(X) = X^2 - a_p(f)X + \epsilon(p)p^{k-1}.$$

By reduction and semi-simplification one obtains the following consequence.

Theorem 1.3.5 *Let $k \geq 2$, $N \geq 1$, l a prime not dividing N, and $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_l^\times$ a character.*

Then to any normalised eigenform $f \in \mathrm{S}_k(N, \epsilon\,; \mathbb{C})$ with $f = \sum_{n\geq 1} a_n(f)q^n$ and to any prime ideal $\mathfrak{P}$ of the ring of integers of $\mathbb{Q}_f = \mathbb{Q}(a_(f) : n \in \mathbb{N})$ with residue characteristic l, one can attach a mod l Galois representation

$$\overline{\rho}_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

such that

(i) $\overline{\rho}_f$ is semi-simple,

(ii) $\overline{\rho}_f$ is odd,

(iii) for all primes $p \nmid Nl$ the representation $\overline{\rho}_f$ is unramified at p and

$$\Phi_p(\rho_f)(X) \equiv X^2 - a_p(f)X + \epsilon(p)p^{k-1} \mod \mathfrak{P}.$$

There is also a weight one version of these theorems due to Deligne and Serre.

Theorem 1.3.6 *Let $N \geq 1$ and $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ a character.*

Then to any normalised eigenform $f \in \mathrm{S}_1(N, \epsilon\,; \mathbb{C})$ with $f = \sum_{n\geq 1} a_n(f)q^n$ one can attach a Galois representation of the rationals

$$\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{C})$$

such that

(i) ρ_f *is odd,*

(ii) for all primes $p \nmid N$ *the representation* ρ_f *is unramified at* p *and*

$$\Phi_p(\rho_f)(X) = X^2 - a_p(f)X + \epsilon(p).$$

Now we will sketch the construction of these Galois representations. Later in the course we may go into more details.

Let $f = \sum_{n \geq 1} a_n q^n \in S_k(\Gamma_1(N))$ be a Hecke eigenform. Let $\mathbb{T}$ be the sub-$\mathbb{Q}$-algebra inside $\mathrm{End}_{\mathbb{C}}(S_k(\Gamma_1(N)))$ generated by all Hecke operators T_n with $(n, N) = 1$. It is an Artin $\mathbb{Q}$-algebra and hence decomposes as the direct product over the localizations at its maximal ideals:

$$\mathbb{T} \cong \prod_{\mathfrak{m}} \mathbb{T}_{\mathfrak{m}}.$$

Recall that

$$\mathfrak{m} = \ker(\mathbb{T} \xrightarrow{T_n \mapsto a_n} \mathbb{C})$$

is such a maximal ideal. The residue field $\mathbb{T}/\mathfrak{m}$ is equal to the coefficient field $\mathbb{Q}_f := \mathbb{Q}(a_n | (n, N) = 1)$, as one easily sees. If one assumes that f is a newform, then $\mathbb{T}_{\mathfrak{m}} \cong \mathbb{Q}_f$. We shall do that from now on.

From the Eichler-Shimura theorem it follows that the localization $\mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Q}[X,Y]_{k-2})_{\mathfrak{m}}$ is a $\mathbb{T}_{\mathfrak{m}} = \mathbb{Q}_f$-vector space of dimension 2. This we will explain now. We compute its dimension after tensoring it over $\mathbb{Q}$ with $\mathbb{C}$:

$$\mathbb{C} \otimes_{\mathbb{Q}} \mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Q}[X,Y]_{k-2})_{\mathfrak{m}} \cong \prod_{\sigma : \mathbb{Q}_f \hookrightarrow \mathbb{C}} \mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2})_{\sigma(\tilde{\mathfrak{m}})},$$

with $\tilde{\mathfrak{m}} = \ker(\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{T} \xrightarrow{T_n \mapsto a_n} \mathbb{C})$ (this is not so difficult to check). Hence, it suffices to show that the $\mathbb{C}$-dimension of $\mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2})_{\sigma(\tilde{\mathfrak{m}})}$ is equal to 2. This is an easy consequence of the Eichler-Shimura isomorphism

$$\mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2})_{\sigma(\tilde{\mathfrak{m}})} \cong S_k(\Gamma_1(N))_{\mathfrak{m}} \oplus \overline{S_k(\Gamma_1(N))}_{\mathfrak{m}}.$$

From the q-expansion pairing it follows that the dimension of $S_k(\Gamma_1(N))_{\mathfrak{m}}$ is equal to the dimension of $(\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{T})_{\sigma(\tilde{\mathfrak{m}})}$, which is 1 for a newform.

The Galois representation comes from a $G_{\mathbb{Q}}$-action on $\mathbb{Q}_l \otimes_{\mathbb{Q}} \mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Q}[X,Y]_{k-2})_{\mathfrak{m}}$. Since

$$\mathbb{Q}_l \otimes_{\mathbb{Q}} \mathbb{Q}_f \cong \prod_{\lambda | l} \mathbb{Q}_{f,\lambda},$$

we obtain for every $\lambda \mid l$ a map

$$G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_{f,\lambda}) \hookrightarrow \mathrm{GL}_2(\overline{\mathbb{Q}}_l).$$

We shall not explain the properties of this representation here, as it involves too much material for this introduction. Nevertheless, we shall try to motivate why there is a Galois action.

One needs to get geometry into the business. Using that $\mathbb{H}$, the upper half plane, is simply connected and, since $\Gamma_1(N)$ acts with finite stabilizers on it (for $N \geq 4$ even with trivial stabilizers), one can identify

$$\mathrm{H}^1(\Gamma_1(N), \mathbb{Q}[X,Y]_{k-2}) \cong \mathrm{H}^1(Y_1(N), \underline{\mathbb{Q}[X,Y]_{k-2}}),$$

where $\underline{\mathbb{Q}[X,Y]_{k-2}}$ is the locally constant sheaf on $Y_1(N)$ (seen as a Riemann surface) which in small enough neighbourhoods looks like $\mathbb{Q}[X,Y]_{k-2}$. Formally, this sheaf can be obtained as the direct image sheaf $(\pi_* \underline{\mathbb{Q}[X,Y]_{k-2}})^{\Gamma_1(N)}$, where $\pi : \mathbb{H} \twoheadrightarrow Y_1(N)$ is the natural projection and now $\underline{\mathbb{Q}[X,Y]_{k-2}}$ stands for the constant sheaf on $\mathbb{H}$ with a suitable $\Gamma_1(N)$-action (we do not go into details here). By a suitable extension to the cusps one finds an isomorphism

$$\mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Q}[X,Y]_{k-2}) \cong \mathrm{H}^1(X_1(N), \underline{\mathbb{Q}[X,Y]_{k-2}}).$$

It is very important to note that the Hecke operators respect this isomorphism.

In general, one now has the comparison theorem

$$\mathbb{Q}_l \otimes_{\mathbb{Q}} \mathrm{H}^1(X_1(N)(\mathbb{C}), \underline{\mathbb{Q}[X,Y]_{k-2}})_{\mathfrak{m}} \cong \prod_{\lambda | l} \mathrm{H}^1_{\mathrm{et}}(X_1(N)_{\mathbb{Q}} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}, \underline{\mathbb{Q}_l[X,Y]_{k-2}})_{\mathfrak{m}_\lambda}$$

with a suitable étale sheaf and the decomposition $\mathbb{Q}_l \otimes_{\mathbb{Q}} \prod_{\lambda|l} \mathbb{T}_{\mathfrak{m}} \cong \mathbb{T}_{\mathfrak{m}_\lambda} \cong \prod_{\lambda|l} \mathbb{Q}_{f,\lambda}$. On the right hand side, one finds the desired $G_{\mathbb{Q}}$-action.

If $k = 2$, there is a slightly more down to earth description, which avoids the use of étale cohomology. We explain this version now. Let $X = X_1(N)(\mathbb{C})$ the modular curve as a Riemann surface. Consider the exact sequence of sheaves:

$$0 \to \underline{\mu_{n,X}} \to \mathcal{O}_X^\times \xrightarrow{x \mapsto x^n} \mathcal{O}_X^\times \to 0.$$

We explain. Exactness of a sequence of sheaves is tested on the stalks. Taking an n-th root of a non-zero holomorphic function in some small enough neighbourhood is always possible, giving the surjectivity. We define $\underline{\mu_{n,X}}$ as the kernel. We claim that it is a locally constant sheaf, which in small enough neighbourhoods looks like μ_n, the n-th roots of unity. This is very easy to see: the n-th power of a function $\phi : U \to \mathbb{C}$ with $U \subset X$ open and connected is identically 1 if and only if $\phi(x) = \zeta$ for some $\zeta \in \mathbb{C}$ with $\zeta^n = 1$ and all $x \in X$. We now pass to the long exact sequence in cohomology

$$0 \to \mu_n(\mathbb{C}) \to \mathbb{C}^\times \xrightarrow{x \mapsto x^n} \mathbb{C}^\times \to \mathrm{H}^1(X, \underline{\mu_{n,X}}) \to \mathrm{H}^1(X, \mathcal{O}_X^\times) \xrightarrow{x \mapsto x^n} \mathrm{H}^1(X, \mathcal{O}_X^\times),$$

using $\mathcal{O}_X(X) = \mathbb{C}$, since X is connected. We obtain

$$\mathrm{H}^1(X, \underline{\mu_{n,X}}) \cong \ker\big(\mathrm{H}^1(X, \mathcal{O}_X^\times) \xrightarrow{x \mapsto x^n} \mathrm{H}^1(X, \mathcal{O}_X^\times)\big).$$

Since $\underline{\mu_{n,X}}$ is locally constant, one finds

$$\mathrm{H}^1(X, \underline{\mu_{n,X}}) \cong \mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mu_n) \cong \mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), \mathbb{Z}/n\mathbb{Z}),$$

subject to some identification between the n-th roots of unity and $\mathbb{Z}/n\mathbb{Z}$.

Next, we identify $\ker\left(\mathrm{H}^1(X,\mathcal{O}_X^\times)\xrightarrow{x\mapsto x^n}\mathrm{H}^1(X,\mathcal{O}_X^\times)\right)$ with $\mathrm{Jac}(X)(\mathbb{C})[n]$. One has an isomorphism

$$\mathrm{Pic}(X)\cong\mathrm{H}^1(X,\mathcal{O}_X^\times)$$

(see e.g. Liu's book on 'Arithmetic Geometry'), under which $x\mapsto x^n$ on the right becomes multiplication by n on the left. All together, we now have

$$\mathrm{H}^1_{\text{par}}(\Gamma_1(N),\mathbb{Z}/n\mathbb{Z})\cong\ker\left(\mathrm{Pic}(X)\xrightarrow{P\mapsto nP}\mathrm{Pic}(X)\right).$$

Elements in the n-torsion of $\mathrm{Pic}(X)$ are necessarily of degree 0, whence

$$\mathrm{H}^1_{\text{par}}(\Gamma_1(N),\mathbb{Z}/n\mathbb{Z})\cong\mathrm{Pic}(X)[n]=\mathrm{Pic}^0(X)[n]=\mathrm{Jac}(X)[n].$$

Recall that, so far, we have taken X over $\mathbb{C}$ (a Riemann surface), so that $\mathrm{Jac}(X)$ is a complex abelian variety. But, every torsion point is defined over the algebraic numbers, whence we finally get

$$\mathrm{H}^1_{\text{par}}(\Gamma_1(N),\mathbb{Z}/n\mathbb{Z})\cong\mathrm{Jac}(X_{\mathbb{Q}})(\overline{\mathbb{Q}})[n],$$

which carries a natural $G_{\mathbb{Q}}$-action. Now we replace n everywhere by l^n and pass to the projective limit:

$$\mathrm{H}^1_{\text{par}}(\Gamma_1(N),\mathbb{Z}_l)\cong T_l(\mathrm{Jac}(X_{\mathbb{Q}}))$$

and

$$\mathrm{H}^1_{\text{par}}(\Gamma_1(N),\mathbb{Q}_l)\cong V_l(\mathrm{Jac}(X_{\mathbb{Q}})).$$

Of course, these identifications are compatible with the Hecke action, so that we indeed get a $G_{\mathbb{Q}}$-action as desired.

1.4 L-functions

We will not go into detail on L-functions in this introduction and will mainly restrict ourselves to L-functions of Artin representations.

Definition 1.4.1 *Let k be a topological field. Let K be a number field and*

$$\rho: G_K\to\mathrm{GL}_n(k)$$

a global Galois representation. Suppose that $\tilde{\Phi}_{\mathfrak{p}}(\rho)\in\overline{\mathbb{Q}}[X]$, e.g. if $k=\overline{\mathbb{Q}}\subset\mathbb{C}$.

The partial L-function of *ρ is defined as the (formal)* Euler product

$$\mathcal{L}(\rho,s)=\prod_{\mathfrak{p}\text{ unramified}}\frac{1}{\tilde{\Phi}_{\mathfrak{p}}(\rho)(N(\mathfrak{p})^{-s})}.$$

If $k=\mathbb{C}$, i.e. if ρ is an Artin representation, we define the L-function of *ρ as*

$$\mathcal{L}(\rho,s)=\prod_{\mathfrak{p}}\frac{1}{\tilde{\Phi}_{\mathfrak{p}}(\rho)(N(\mathfrak{p})^{-s})}.$$

Exercise 4 illustrates the factors appearing in the L-functions. The correct choice of the factors of the L-function of an l-adic representation at ramified primes will be discussed in the chapter on the local theory. It involves Weil-Deligne representations; more precisely, at ramified primes away from l one also needs to restrict to the part where the monodromy operator is zero.

Example 1.4.2 *(1) Let K be a number field and $1 : G_K \to \mathrm{GL}_n(\mathbb{C})$ be the trivial Galois representation (i.e. $1(g) = 1$ for all $g \in G$). Then*

$$\mathcal{L}(1, s) = \zeta_K(s),$$

the Dedekind-ζ-function of K. This is a special case of (3).

(2) Let L/K be a Galois extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$. Then we have

$$\zeta_L(s) = \zeta_K(s) \prod_{\rho \neq 1} \mathcal{L}(\rho, s)^{\dim \rho},$$

where the product runs over all irreducible representations of G. This is nearly a formal consequence of the representation theory of finite groups. If time allows, we will prove it in the chapter on complex Galois representations.

(3) Let $\chi : G_{\mathbb{Q}} \to \mathbb{C}^\times$ be a 1-dimensional global Galois representation. Then $\mathcal{L}(\chi, s)$ converges absolutely for $\mathrm{Re}(s) > 1$ and satisfies the identity

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

Hence, the L-function is equal to the Dirichlet series of χ. These statements are proved in Exercise 5.

(4) Let E be an elliptic curve over $\mathbb{Q}$. Its L-function coincides with the L-function $\mathcal{L}(\rho_E, s)$, if one adds the correct factors at the ramified primes.

We now apply Exercise 4 to the Galois representations $V_i = \mathrm{H}^i_{\mathrm{et}}(E, \mathbb{Q}_\ell)$ for $i = 0, 1, 2$ with $\phi = \mathrm{Frob}_p$.

For $i = 0$ we have $V_0 = \mathbb{Q}_\ell$ with the trivial Galois action, since E has a single connected component. Thus, we obtain

$$\frac{1}{1 - X} = \exp\big(\sum_{r=1}^{\infty} \frac{X^r}{r}\big) = \exp\big(\sum_{r=1}^{\infty} \mathrm{Tr}(\mathrm{Frob}_p^r | V_0) \frac{X^r}{r}\big).$$

For $i = 2$, we note that Frob_p^r acts as multiplication by p^r on V_2, due to the twisting of Poincaré duality. This gives

$$\frac{1}{1 - pX} = \exp\big(\sum_{r=1}^{\infty} \frac{(pX)^r}{r}\big) = \exp\big(\sum_{r=1}^{\infty} \mathrm{Tr}(\mathrm{Frob}_p^r | V_2) \frac{X^r}{r}\big).$$

The most interesting case is $i = 1$. One has $V_1 = V_\ell(E)$. Writing $\#E(\mathbb{F}_p) = p + 1 - a_p$, Theorem 1.3.3 yields

$$\frac{1}{1 - a_p X + pX^2} = \exp\big(\sum_{r=1}^{\infty} \mathrm{Tr}(\mathrm{Frob}_p^r \,|V_1)\frac{X^r}{r}\big).$$

Now we use the Lefshetz fixed point formula

$$\#E(\mathbb{F}_{p^r}) = \sum_{i=0}^{2}(-1)^i\big(\,\mathrm{Tr}(\mathrm{Frob}_p^r \,|V_i)\big)$$

in order to compute the zeta-function of E:

$$\begin{aligned} Z(E,X) &= \exp\big(\sum_{r=1}^{\infty} \#E(\mathbb{F}_{p^r})\frac{X^r}{r}\big) \\ &= \exp\big(\sum_{r=1}^{\infty}\sum_{i=0}^{2}(-1)^i\big(\,\mathrm{Tr}(\mathrm{Frob}_p^r \,|V_i)\big)\frac{X^r}{r}\big) \\ &= \prod_{i=0}^{2}\big(\exp\big(\sum_{r=1}^{\infty}\big(\,\mathrm{Tr}(\mathrm{Frob}_p^r \,|V_i)\big)\frac{X^r}{r}\big)\big)^{(-1)^i} \\ &= \frac{1 - a_p X + pX^2}{(1-X)(1-pX)}. \end{aligned}$$

Hence, the number of points $\#E(\mathbb{F}_{p^r})$ for all r is encoded in $\frac{1-a_pX+pX^2}{(1-X)(1-pX)}$! Thus, computing the number of points of E over finite extensions of $\mathbb{F}_p$ reduces to computing the zeta-function $Z(E,X)$, and hence to computing a_p. Moreover, after Wiles we know that E comes from a modular form f with $a_p = a_p(f)$. So, it suffices to compute T_p on f.

(5) Let f be a newform of the form $\sum_{n=1}^{\infty} a_n q^n$ on $\Gamma_0(N)$. Its L-function is defined as

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

If one adds the correct factors at the ramified primes, one has the identity

$$\mathcal{L}(f,s) = \mathcal{L}(\rho_f, s).$$

This example will be treated in more detail in the chapter on complex Galois representations.

We finish this introductory chapter by stating a famous conjecture of Emil Artin.

Conjecture 1.4.3 (Artin Conjecture) *Let K be a number field and*

$$\rho : G_K \to \mathrm{GL}_n(\mathbb{C})$$

a non-trivial Artin representation.

Then $\mathcal{L}(\rho, s)$ admits an analytic continuation to the whole complex plane.

It is known that there always is a meromorphic continuation. The conjecture will be discussed in more detail in the chapter on complex Galois representations.

Chapter 2

General representation theory

Throughout this chapter, I try to stick to the following conventions:

- R is a ring, sometimes commutative, sometimes not.
- K/k are fields.
- k-algebras are usually called A.
- Simple modules are called S.
- A-modules are usually called V and R-modules M.

We will, however, always explain the symbols appearing. I am writing these lines only to remind myself of my own notation.

Definition 2.0.4 *Let R be a ring. We define the* centre of R *as*

$$Z(R) := \{r \in R \mid rt = tr \;\forall\; t \in R\}.$$

Let R be a commutative ring. An R-algebra is a ring homomorphism $R \to A$ such that the image of R is contained in the centre $Z(A)$ of A.
A k-algebra A is called central *if $Z(A) = k$.*

Let R be a commutative ring. Whenever we have a group representation

$$\rho : G \to \mathrm{GL}(V),$$

where V is a finitely generated R-module, we can make it into an algebra representation, i.e. an R-algebra homomorphism

$$R[G] \to \mathrm{End}_R(V).$$

This allows us to see V as an $R[G]$-module. This is the point of view that we are going to adopt throughout this chapter.

2.1 Simple and semi-simple rings and modules

We start by introducing some definitions.

Definition 2.1.1 *Let R be a ring. An R-module M is said to be* faithful *if the only $r \in R$ such that $rm = 0$ for all $m \in M$ is $r = 0$.*

Definition 2.1.2 *Let R be a ring.*

(a) The ring R is called simple *if it does not have any two-sided ideals except (0) and R.*

(b) The Jacobson radical $\mathrm{Jac}(R)$ *of R is defined as the intersection of all maximal left ideals of R.*

(c) The ring R is called semi-simple *if $\mathrm{Jac}(R) = (0)$.*

We also have the corresponding definitions for modules.

Definition 2.1.3 *Let R be a ring and M a left R-module.*

(a) M is called simple *or* irreducible *if it does not have any left R-submodules except (0) and M.*

(b) M is called semi-simple *(or* completely reducible*) if it is the direct sum of simple modules.*

(c) M is called indecomposable *if any direct sum decomposition $M \cong N \oplus P$ implies that $P = (0)$ or $M = (0)$.*

Remark 2.1.4 *In terms of matrices, a representation*

$$G \to \mathrm{GL}_n(k)$$

with k a field is irreducible if and only if the matrices cannot be conjugated into a non-trivial block form like this

$$\begin{pmatrix} \boxed{A} & \boxed{*} & \dots & \boxed{*} \\ \boxed{0} & \boxed{B} & \dots & \boxed{*} \\ \dots & \dots & \dots & \dots \\ \boxed{0} & \boxed{0} & \dots & \boxed{Z} \end{pmatrix}$$

with only zeros below the boxed diagonal. If all the $*$s are 0, a representation of the above form is semi-simple.

Definition 2.1.5 *Let R be a ring. It is called a* division ring *if all elements different from 0 are invertible.*

Remark 2.1.6 *Division rings are simple rings, since all left ideals different from (0) are the whole ring.*

Without proof we mention two classical theorems, which we will only need at one place.

Definition 2.1.7 *Let R be a ring. The* Grothendieck group $\mathcal{C}(R)$ *is defined as the free abelian group on the set of finitely generated simple left R-modules.*

Theorem 2.1.8 (Jordan-Hölder) *Let k be a field, A a k-algebra and V an A-module which is a finite dimensional k-vector space (or, more generally, V should be an R-module that is both Artinian and Noetherian).*

Then V has a composition series, i.e. a descending chain of submodules

$$V = V_0 \supsetneq V_1 \supsetneq V_2 \supsetneq \cdots \supsetneq V_n \supsetneq (0)$$

such that all subquotients V_i/V_{i+1} are simple A-modules.

Any two composition series have the same composition factors (i.e. subquotients). Hence, the Grothendieck group can also be defined as the free abelian group on the set of finitely generated left R-modules, modulo the relation $V - A - B$ for all short exact sequences $0 \to A \to V \to B \to 0$.

Proof. (See [CurtisReiner], Theorems 13.4 and 13.7.) The proof is not difficult and does not need anything of what will be developed during this lecture. Omitted. □

Theorem 2.1.9 (Krull-Schmidt) *Let k be a field, A a k-algebra and V an A-module which is a finite dimensional k-vector space (or more generally V should be an R-module such that all submodules of V are both Artinian and Noetherian). Then any decomposition*

$$V = \bigoplus_{i=1}^{n} V_i$$

into indecomposable modules has the same length n and is unique up to permutation.

Proof. (See [CurtisReiner], Theorem 14.5.) The proof is not difficult and does not need anything of what will be developed during this lecture. Omitted. □

Theorem 2.1.10 (Schur's Lemma) *Let R be a ring.*

(a) Let S be a simple R-module. Then $D = \operatorname{End}_R(S)$ is a division ring, i.e. every non-zero element is invertible.

(b) Let S, T be simple R-modules. Then

$$\operatorname{Hom}_R(S,T) \cong \begin{cases} D & \text{if } T \cong S, \\ 0 & \text{otherwise} \end{cases}$$

with D the division ring $\operatorname{End}_R(S)$.

Proof. (a) All non-zero endomorphisms are isomorphisms, since the kernel and the image are non-trivial submodules.

(b) Clear. □

Proposition 2.1.11 *Let R be a ring.*

(a) Let M be a left R-module. The following conditions are equivalent:

(i) M is semi-simple.

(ii) M is the sum of simple modules.

(iii) Every submodule N of M is a direct summand.

(b) Every submodule and every quotient of a semi-simple module is semi-simple.

Proof. Exercise 7. □

We can and will often consider R as a left R-module in the natural way. Then we have the translation table:

- Left ideals = left modules.
- Minimal left ideals = simple left modules.

Lemma 2.1.12 *Let R be a ring. Then we have the bijection*

$$\begin{aligned}\{\mathfrak{m} \subset R \text{ maximal left ideals}\} &\leftrightarrow \{M \text{ simple } R\text{-modules up to isomorphism }\}\\ \mathfrak{m} &\mapsto R/\mathfrak{m}\\ \ker(\phi_x) &\leftarrow\!\shortmid M,\end{aligned}$$

where in M we choose any non-zero element x and define $\phi_x : R \xrightarrow{r \mapsto rx} M$.

Proof. This is very easy. The maps are clearly inverses to each other and one checks that they are well-defined. □

Let us recall for the following proposition that an ideal $\mathfrak{n}$ of some ring is called *nilpotent* if there is an integer n such that $\mathfrak{n}^n = (0)$.

Proposition 2.1.13 *Let R be a ring and k a field.*

(a) The Jacobson radical $\mathrm{Jac}(R)$ is a two-sided ideal, which contains all nilpotent two-sided ideals.

(b) Suppose that R is a finite dimensional k-algebra. Then $\mathrm{Jac}(R)$ is the maximal nilpotent two-sided ideal.

(c) Suppose that R is a finite dimensional k-algebra. Then R is semi-simple as a left R-module if and only if R is semi-simple.

Proof. Exercise 8. □

Corollary 2.1.14 *Let R be a semi-simple ring. Every left R-module is semi-simple.*

Proof. By Proposition 2.1.11 quotients of semi-simple modules are semi-simple. It is clear that free modules are semi-simple, as direct sums of semi-simple modules are. Now it suffices to represent a given R-module M as the quotient of a free module. □

Remark 2.1.15 *Let R be a ring. The simple R-modules are equal to the simple $R/\operatorname{Jac}(R)$-modules.*

Indeed, let M be a simple R-module. The kernel of the map ϕ_x of Lemma 2.1.12 is a maximal ideal, and hence contains the Jacobson radical $\operatorname{Jac}(R)$. Thus, the Jacobson radical acts trivially on M. Conversely, every $R/\operatorname{Jac}(R)$-module is an R-module.

A very important example of a semi-simple ring is provided by Maschke's theorem.

Theorem 2.1.16 (Maschke) *Let k be a field and G a finite group. Then the group algebra $k[G]$ is semi-simple if and only if the order of G is coprime to the characteristic of k.*

Proof. This proof is quite easy. Omitted. □

Lemma 2.1.17 *Let K/k be a field extension and A a finite dimensional k-algebra. Consider the natural embedding $A \xrightarrow{a\mapsto 1\otimes a} K \otimes_k A$. The natural map*

$$A/\operatorname{Jac}(A) \to K \otimes_k A/\operatorname{Jac}(K \otimes_k A)$$

is an injection. In particular, if $K \otimes_k A$ is a semi-simple K-algebra, then A is already semi-simple.

Proof. We use Proposition 2.1.13 and show that $\operatorname{Jac}(K \otimes_k A) \cap A = \operatorname{Jac}(A)$. The intersection $\operatorname{Jac}(K \otimes_k A) \cap A$ is clearly nilpotent, whence we have the inclusion '$\subseteq$'. The other one is obtained from the fact that the image of any nilpotent ideal under the natural embedding lies in a nilpotent ideal, whence $\operatorname{Jac}(A)$ lands in $\operatorname{Jac}(K \otimes_k A) \cap A$. The final statement follows directly from Proposition 2.1.13. □

Lemma 2.1.18 *Let D be a finite dimensional division algebra over a field k.*

(a) $\operatorname{Mat}_r(D)$ *is the direct sum of r-copies of D^r (column vector) as a left* $\operatorname{Mat}_r(D)$*-module.*

(b) D^r *is a simple* $\operatorname{Mat}_r(D)$*-module.*

(c) $\operatorname{Mat}_r(D)$ *is a simple k-algebra with centre $Z(D)$.*

(d) $\operatorname{Mat}_r(\operatorname{Mat}_s(D)) \cong \operatorname{Mat}_{rs}(D)$.

Proof. Exercise 9. □

This lemma illustrates the following propositions.

Proposition 2.1.19 *Let R be a semi-simple ring. It has only a finite number of non-isomorphic minimal left ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$. Let*

$$R_i = \sum_{\mathfrak{a}\cong\mathfrak{a}_i} L$$

be the sum over all minimal left ideals $\mathfrak{a}$ which are isomorphic to $\mathfrak{a}_i$. Then R_i is a two-sided ideal of R. Each R_i is also a simple ring. Moreover, we have a ring isomorphism

$$R \cong \prod_{i=1}^{s} R_i.$$

If e_i is the unit in R_i, then $1 = e_1 + \cdots + e_s$. The e_i form a complete set of orthogonal idempotents.

If M is any R-module, then

$$M = \bigoplus_{i=1}^{s} R_i M = \bigoplus_{i=1}^{s} e_i M$$

and $e_i M$ is the submodule of M which consists of the sum of all its simple submodules that are isomorphic to $\mathfrak{a}_i$.

Proof. (See [Lang], Theorems 4.3 and 4.4.) Omitted. □

Corollary 2.1.20 *(a) Every simple submodule of a semi-simple ring R is isomorphic to one of the minimal left ideals of R.*

(b) A simple ring has exactly one simple module up to isomorphism. □

Proposition 2.1.21 *Let R be a simple ring. Then as an R-module, R is a finite direct sum of simple left ideals. There are no two-sided ideals except 0 and R. Any two simple left ideals are isomorphic as left R-modules via right multiplication by a suitable element in R.*

Proof. (See [Lang], Theorem 5.2.) Omitted. □

Lemma 2.1.22 *Let k be a field and V a finite dimensional k-vector space. Let R be a subalgebra of* $\mathrm{End}_k(V)$.

Then R is semi-simple if and only if V is a semi-simple R-module.

Proof. Exercise 10. □

Proposition 2.1.23 *Let R be any ring (not necessarily commutative) and M a left R-module. Then*

$$\mathrm{End}_R(M^n) \cong \mathrm{Mat}_n(\mathrm{End}_R(M)).$$

More generally: Let M be an arbitrary semi-simple R-module, say, of the form $M = \bigoplus_i S_i^{m_i}$ with S_i pairwise non-isomorphic R-modules. Then

$$\mathrm{End}_R(M) \cong \bigoplus_i \mathrm{Mat}_{m_i}(\mathrm{End}_R(S_i)).$$

Proof. (See [Kersten], Satz I.1.13.) Here is the basic idea from which everyone can easily reconstruct the proof. We associate a matrix in $\mathrm{Mat}_n(\mathrm{End}_R(M))$ to $f \in \mathrm{End}_R(M^n)$. The entry at (i, j) of the matrix is defined as

$$M \xrightarrow{\text{injection into } i\text{-th factor}} M^n \xrightarrow{f} M^n \xrightarrow{\text{projection from } j\text{-th factor}} M.$$

The final statement follows from Schur's lemma (Theorem 2.1.10). □

Definition 2.1.24 *Let R be a ring. The* opposite ring R^{opp} *is defined as the ring having the same elements as R with order of multiplication reversed, i.e. $R^{\mathrm{opp}} = \{\tilde{r} | r \in R\}$ and $\tilde{r}\tilde{s} := \widetilde{sr}$.*

Lemma 2.1.25 *(a) Let R be a ring. The ring R^{opp} is isomorphic as a ring to $\mathrm{End}_R(R)$ via mapping r to right multiplication $\tau_r : R \to R$ with $\tau_r(s) = sr$.*

(b) Let D be a division algebra. The opposite of $\mathrm{Mat}_n(D)$ is isomorphic to $\mathrm{Mat}_n(D^{\mathrm{opp}})$ via transposing the matrices.

Proof. Exercise 11. □

Theorem 2.1.26 (Wedderburn) *Let k be a field. Let A be a simple k-algebra. As a left A-module $A \cong S^r$ with the unique simple left A-module S for some integer $r \geq 1$. Let D be the division algebra $D = \mathrm{End}_A(S)$. Then*

$$A \cong \mathrm{Mat}_r(D^{\mathrm{opp}}).$$

Proof. By Lemma 2.1.25, the opposite A^{opp} is isomorphic to $\mathrm{End}_A(A)$. This, however, is the direct sum of, say, r copies of the simple left A-module S. By Proposition 2.1.23, $A^{\mathrm{opp}} \cong \mathrm{Mat}_r(\mathrm{End}_A(S))$ follows. But, by Schur's Lemma 2.1.10, $\mathrm{End}_A(S) \cong D$ for some division algebra D. Further, again by Lemma 2.1.25, A is isomorphic to $\mathrm{Mat}_r(D^{\mathrm{opp}})$, establishing the proposition. □

Corollary 2.1.27 *Let A be a semi-simple finite dimensional algebra over a field k. Then A is of the form $\prod_{i=1}^{s} \mathrm{Mat}_r(D_i)$ with D_i division algebras.*

Proof. This follows directly from Theorem 2.1.26 and Proposition 2.1.19. □

Corollary 2.1.28 *Let A be a simple algebra over a field k. Then its centre $Z(A)$ is a field K, and we can consider A as a K-algebra. As such it is central simple.*

Proof. Theorem 2.1.26 reduces the statement to Lemma 2.1.18, since the centre of a division algebra is a field. □

Theorem 2.1.29 (Skolem-Noether) *Let k be a field, A and B finite dimensional simple k-algebras and $f, g : B \to A$ two k-algebra homomorphisms. If the centre of A is equal to k, then there is a unit u in A such that for all $b \in B$*

$$g(b) = uf(b)u^{-1}.$$

Proof. (See [Kersten], Satz 8.2.) Omitted. □

Corollary 2.1.30 *Let A be a semi-simple k-algebra and $\phi \in \mathrm{Aut}_k(A)$ an automorphism that is trivial on the centre of A. Then ϕ is inner.*

Proof. By Skolem-Noether (Theorem 2.1.29) any automorphism of a central simple algebra is inner. Let $A \cong \prod A_i$ with A_i simple. Let e_i be the element of A that is the identity of A_i. All the e_i lie in the centre of A and hence are left unchanged under the application of ϕ. Thus, ϕ descends to an automorphism of A_i. Now A_i can be considered as an algebra over its centre, as such it is a central simple algebra. Hence, every restriction of ϕ is inner, and, consequently, so is ϕ. □

Corollary 2.1.31 *Let k be a field and $r \geq 1$ an integer. Then every automorphism of $\mathrm{Mat}_r(k)$ comes from conjugation by an invertible matrix.* □

2.2 Scalar extensions

Definition 2.2.1 *Let K/k be a field extension, A a finite dimensional k-algebra and V an A-module. The* scalar extension *of A* by *K is defined as the K-algebra $A_K := K \otimes_k A$ and the one of V as the A_K-module $V_K := K \otimes_k V$. In terms of the representation $A \to \mathrm{End}_k(V)$, this gives rise to $A_K \to \mathrm{End}_K(V_K)$.*

Remark 2.2.2 *Let G be a (profinite) group, k a field and V_1 and V_2 two $k[G]$-modules. The* tensor product representation *of V_1 and V_2 is defined as $V_1 \otimes_k V_2$ with the $k[G]$-action given by $g(v_1 \otimes v_2) = gv_1 \otimes gv_2$.*

In terms of representations of $k[G]$-algebras we obtain a k-algebra homomorphism

$$k[G] \xrightarrow{g \mapsto (g,g)} k[G \times G] \cong k[G] \otimes_k k[G] \to \mathrm{End}_k(V_1 \otimes_k V_2).$$

If V_2 is a 1-dimensional representation, then the tensor product representation is called a twist.

Proposition 2.2.3 *Let A be a finite dimensional semi-simple k-algebra. Then for any finite separable extension K/k, the K-algebra $K \otimes_k A = A_K$ is semi-simple.*

Proof. (See [Lang], Theorem XVII.6.2.) By Lemma 2.1.17 we may assume that K/k is a Galois extension and we let $G = \mathrm{Gal}(K/k)$. We will show that $N := \mathrm{Jac}(K \otimes_k A)$ is zero.

We let G act on $K \otimes_k A$ by $\sigma(x \otimes a) = \sigma(x) \otimes a$. We see that $\sigma N = N$ for any $\sigma \in G$, as N is maximal nilpotent by Proposition 2.1.13. Let $z \in N$ be any element. It can be written in the form $z = \sum_i^n x_i \otimes a_i$ with $\{a_1, \ldots, a_n\}$ forming a basis of A and $x_i \in K$. Now we use the trace $\mathrm{Tr}_{K/k}$ to make an element in $\mathrm{Jac}(A)$. Let $y \in K$ be any element. We have

$$\begin{aligned}\mathrm{Tr}_{K/k}(yz) = \mathrm{Tr}_{K/k}(\sum_i yx_i \otimes a_i) &= \sum_{\sigma \in G} \sum_i \sigma(yx_i) \otimes a_i \\ &= \sum_i \mathrm{Tr}_{K/k}(yx_i) \otimes a_i = 1 \otimes \sum_i \mathrm{Tr}_{K/k}(yx_i)a_i.\end{aligned}$$

This element is still in N, but also in A, and hence in $\mathrm{Jac}(A)$ by Lemma 2.1.17. It follows that it is equal to 0, whence $\mathrm{Tr}_{K/k}(yx_i) = 0$ for all i and all y. Since by separability $\mathrm{Tr}_{K/k}$ is a non-degenerate bilinear form, it follows that $x_i = 0$ for all i, whence $z = 0$, as desired. □

If A is a k-algebra and K/k a field extension, then

$$K \otimes_k \mathrm{Mat}_n(A) \cong \mathrm{Mat}_n(K \otimes_k A)$$

(see Exercise 13).

Theorem 2.2.4 *Let R be a commutative ring, let A and B be R-algebras and let V and W be A-module. Suppose that B is flat over R and V a finitely presented A-module. Then the natural map*

$$B \otimes_R \mathrm{Hom}_A(V, W) \to \mathrm{Hom}_{B \otimes_R A}(B \otimes_R V, B \otimes_R W)$$

is an R-isomorphism.

Proof. (See [Karpilovsky], Theorem 3.5.2.) Omitted. □

Lemma 2.2.5 *Let k be a field and A a k-algebra. Let K/k be a field extension. Let W be a simple A_K-module. Then there exists a simple A-module V such that W occurs as a composition factor of V_K.*

Proof. We know that W occurs as a composition factor of A_K. Let V_i be a composition series of A. Then a composition series of A_K is obtained by taking the composition factors of every $(V_i)_K$. □

Lemma 2.2.6 *Let k be a field, A a k-algebra and V_1 and V_2 two A-modules of finite k-dimension. Let K/k be a field extension. If V_1 and V_2 have a common composition factor, then so do $(V_1)_K$ and $(V_2)_K$. Conversely, if $(V_1)_K$ and $(V_2)_K$ are semi-simple and have a common composition factor, then so do V_1 and V_2.*

Proof. (See [CurtisReiner], 29.6.) Suppose first that V_1 and V_2 have a common composition factor S, i.e. a simple module occuring in the composition series. Then all the composition factors of S_K occur in the composition series of both $(V_1)_K$ and $(V_2)_K$.

Conversely, if $(V_1)_K$ and $(V_2)_K$ are semi-simple and have a common composition factor, then by Schur's lemma $\mathrm{Hom}_{A_K}((V_1)_K, (V_2)_K)$ is non-zero. Note that V_1 and V_2 are also semi-simple by Lemma 2.1.17. From Theorem 2.2.4 it follows that $\mathrm{Hom}_A(V_1, V_2)$ is also non-zero, implying that V_1 and V_2 have a common composition factor. □

We now come to the concept of Galois conjugate modules.

Definition 2.2.7 *Let K/k be a Galois extension and A a k-algebra.*

(a) The Galois group $G = \mathrm{Gal}(K/k)$ acts on the set of A_K-modules from the left as follows:

Let W be an A_K-module. For any $\sigma \in \mathrm{Gal}(K/k)$ we let ${}^{\sigma}W$ be the A_K-module whose underlying K-vector space is equal to W equipped with the A_K-action

$$(x \otimes a).{}_{\sigma}w := (\sigma^{-1}(x) \otimes a).{}_{\mathrm{old}}w$$

for all $x \in K$ and all $a \in A$.

(b) Given an A_K-module W, the decomposition group $D_W(K/k) = D_W$ is defined as the stabilizer of W, i.e. as the subgroup consisting of those $\sigma \in G$ such that ${}^\sigma W \cong W$. For some reason, [Karpilovsky] calls this the inertia group.

Remark 2.2.8 *(i) It is easy to check that the action is indeed a left action.*

(ii) If W is simple, then so is ${}^\sigma W$.

(iii) If $\sigma \in \mathrm{Gal}(K/k)$ and V is an A-module, we define the isomorphism (of k-vector spaces)

$$\sigma : V_K \xrightarrow{x\otimes v \mapsto \sigma(x)\otimes v} V_K.$$

It is easy to check that for a submodule $W \subset V_K$ the map σ defines an isomorphism of A_K-modules from ${}^\sigma W$ to $\sigma(W)$.

(iv) Suppose that W is a matrix representation of A_K, i.e. $A_K \to \mathrm{End}_K(W) = \mathrm{Mat}_n(K)$. Then the matrix representation for ${}^\sigma W$ is obtained from the one of W by applying σ^{-1} to the matrix entries.

Lemma 2.2.9 *Let k be a field and A a k-algebra. Let K/k be a Galois extension. Let V be a simple A-module. If the simple A_K-module W occurs in the composition series of V_K with multiplicity e, then so does ${}^\sigma W$ for all $\sigma \in \mathrm{Gal}(K/k)$.*

Proof. Note that ${}^\sigma V_K \cong V_K$ as A_K-modules. Thus ${}^\sigma W$, which naturally occurs in the decomposition series of ${}^\sigma V$, is isomorphic to a composition factor of V. The statement on the multiplicities follows also. □

Lemma 2.2.10 *Let K/k be a finite Galois extension. Denote by W_A the module W considered as an A-module (rather than as an A_K-module). Then there is an isomorphism of A_K-modules*

$$(W_A)_K \cong \bigoplus_{\sigma\in\mathrm{Gal}(K/k)} {}^\sigma W.$$

Proof. We give the map: $x \otimes v \mapsto (\dots, x._\sigma v, \dots) = (\dots, \sigma^{-1}(x)v, \dots)$. It is an A_K-module homomorphism. That it is an isomorphism can be reduced to the isomorphism $K \otimes_k K \cong \prod_{\sigma\in\mathrm{Gal}(K/k)} {}^\sigma K$, which is easily checked. □

Proposition 2.2.11 *Let K/k be a finite Galois extension. Let V be indecomposable and let W be an indecomposable direct summand of V_K. Then there exists an integer e such that*

$$V_K = \big(\bigoplus_\sigma {}^\sigma W\big)^e,$$

where σ runs through a system of coset representatives for $\mathrm{Gal}(K/k)/D_W$.

Proof. (See [Karpilovsky], Theorem 13.4.5.) The proof is based on the uniqueness of a decomposition into indecomposables (Krull-Schmidt theorem, Theorem 2.1.9). Decompose V_K into different indecomposables

$$V_K \cong V_1^{n_1} \oplus V_2^{n_2} \oplus \cdots \oplus V_r^{n_r}$$

with $V_1 = W$. We obtain

$$V^{[K:k]} \cong (V_K)_A \cong (V_1)_A^{n_1} \oplus (V_2)_A^{n_2} \oplus \cdots \oplus (V_r)_A^{n_r}$$

as A-modules. As a consequence, $(V_1)_A \cong V^s$ for some s. Lemma 2.2.10 yields

$$V_K^s \cong ((V_1)_A)_K \cong \bigoplus_{\sigma \in \mathrm{Gal}(K/k)} {}^{\sigma}V_1,$$

whence for every i there is $\sigma_i \in \mathrm{Gal}(K/k)$ such that $V_i = {}^{\sigma_i}V_1$. From Lemma 2.2.9, $n_1 = n_i =: e$ for all i follows. We now rewrite the first displayed equation:

$$V_K \cong W^e \oplus ({}^{\sigma_2}W)^e \oplus \cdots \oplus ({}^{\sigma_r}W)^e.$$

By assumption, all the ${}^{\sigma_i}W$ are different. Lemma 2.2.9 implies that all the Galois conjugates occur. This finishes the proof. □

Corollary 2.2.12 *Let V be simple and let W be a simple composition factor of V_K. Then there exists an integer e such that*

$$V_K = \big(\bigoplus_{\sigma} {}^{\sigma}W\big)^e,$$

where σ runs through a system of coset representatives for $\mathrm{Gal}(K/k)/D_W$.

Proof. Since V is simple, it is a simple $B := A/\operatorname{Jac}(A)$-module. Note that $B_K \cong A_K/(K \otimes_k \operatorname{Jac}(A))$ (using that K/k is flat) is also semi-simple (Proposition 2.2.3). Proposition 2.2.11 implies that $V_K = \big(\bigoplus_{\sigma} {}^{\sigma}W\big)^e$ with some indecomposable, and due to the semi-simplicity, hence simple, B_K-module W. We note that W is also a simple A_K-module. The isomorphism is also an isomorphism of A_K-modules, since $K \otimes_k \operatorname{Jac}(A) \subseteq \operatorname{Jac}(A_K)$ acts trivially. □

We draw the attention to Exercise 14.

2.3 Splitting fields

We draw the attention to Exercise 15.

Definition 2.3.1 *Let R be a ring and $T \subset R$ be a subring. We define the* centralizer of T in R *as*

$$Z_R(T) := \{r \in R \mid rt = tr \ \forall\, t \in T\}.$$

For important properties of the centralizer see Exercise 15. We include the following proposition, although it will not be needed for the subsequent proofs.

Proposition 2.3.2 *Let k be a field and consider k-algebras A, A', B, B' such that $B \subseteq A$ and $B' \subseteq A'$. Then*

$$Z_{A\otimes_k A'}(B \otimes_k B') = Z_A(B) \otimes_k Z_{A'}(B').$$

Proof. Exercise 16. □

Proposition 2.3.3 *Arbitrary scalar extension of a central simple algebra is central simple.*

Proof. (See [Kersten], Satz 5.10.) Omitted. □

Proposition 2.3.4 *Let k be a field and A a finite dimensional central simple k-algebra. Let $B \subset A$ be a simple subalgebra with $\dim_k B = n$. Then there is a k-algebra homomorphism*

$$Z_A(B) \otimes_k \mathrm{Mat}_n(k) \cong A \otimes_k B^{\mathrm{opp}}.$$

Proof. (See [Kersten], Korollar 8.4 (i).) Omitted. □

Theorem 2.3.5 *Let k be a field and D a division algebra D over k. Let K be a subfield of D.*

Then D is split by K, i.e. $D_K \cong \mathrm{Mat}_r(K)$ for some $r \geq 1$, if and only if K is a maximal subfield. In that case, r is equal to $[K : k]$ and is called the index *of D.*

Proof. This is a direct consequence of Proposition 2.3.4. For, we obtain isomorphisms

$$Z_D(K) \otimes_k \mathrm{Mat}_r(k) \cong D \otimes_k K^{\mathrm{opp}} \cong D_K.$$

If K is a maximal subfield, then $Z_D(K) = K$ by Exercise 15. If K is properly contained in a maximal subfield L, then $Z_D(K)$ properly contains L, and is hence not a field. □

Lemma 2.3.6 *Let k be a field and D a finite dimensional division algebra over k. Suppose that any maximal subfield of D is equal to k. Then $D = k$.*

In particular, there is no finite dimensional division algebra over an algebraically closed field other than the field k itself.

Proof. Let $d \in D$ be any element. Inside of D consider $k(d)$, i.e. the smallest ring containing k and d. This ring is commutative, as k is in the centre of D (by the definition of a k-algebra). So $k(d)$ is a field extension of k and thus equal to k. □

Corollary 2.3.7 *Let D be a division algebra over a field k. All its maximal subfields are isomorphic.*

Proof. This follows from Theorem 2.3.5. □

Corollary 2.3.8 (Wedderburn) *A finite division ring is a finite field.*

Proof. (See [Bourbaki], 11.1.) Let D be a finite division ring with centre k and let K be a maximal subfield of D. By Corollary 2.3.7 and basic algebra, every other maximal subfield is of the form xKx^{-1}. As every element of D is contained in some maximal subfield, it follows that

$$D^\times = \bigcup_{x \in D^\times} xK^\times x^{-1}.$$

Notice that for $x' = xt$ with $t \in K$ we have $x'K^\times x'^{-1} = xK^\times x^{-1}$. The number of distinct $xK^\times x^{-1}$ is, thus, at most equal to the number of elements in $D^\times/K^\times$. Moreover, the number of elements of $xK^\times x^{-1}$ is always equal to the number of elements of $K^\times$. Consequently, all distinct $xK^\times x^{-1}$ are pairwise disjoint. Since they all contain the unit element, the number of distinct $xK^\times x^{-1}$ has to be one. □

Corollary 2.3.9 (Wedderburn) *Let k be either an algebraically closed or a finite field. Let A be a finite dimensional semi-simple k-algebra. Then A is the direct product of matrix algebras.*

Proof. By Lemma 2.3.6 and Corollary 2.3.8 we know that the only finite dimensional division algebras over k are fields. Hence, the corollary is a consequence of Corollary 2.1.27. □

Definition 2.3.10 *Let k be a field and A a k-algebra.*

(a) An irreducible A-module V is called absolutely irreducible *(or* geometrically irreducible*) if for every extension K/k the module $V_K = K \otimes_k V$ is an irreducible $A_K = K \otimes_k A$-module.*

(b) A field extension K/k is called a splitting field of A *if every irreducible A_K-module is absolutely irreducible.*

Theorem 2.3.11 *An irreducible A-module V is absolutely irreducible if and only if*

$$\mathrm{End}_A(V) \cong k,$$

i.e. the only A-endomorphisms of V are left multiplications by an element of k.

Proof. Since the statement is about endomorphism rings, by Exercise 6 we may assume that V is a faithful module. This implies that A is a simple ring with V the only simple module (Lemma 2.1.22).

Let us now first assume that V is an absolutely irreducible A-module. Let $D = \mathrm{End}_A(V)$ and let K be a field splitting field D. By Theorem 2.1.26 we know that $A \cong \mathrm{Mat}_r(D^{\mathrm{opp}})$ and that $V \cong (D^{\mathrm{opp}})^r$. For the K-dimensions we obtain

$$n := \dim_K V_K = r \dim_k D^{\mathrm{opp}}.$$

Using Exercise 13 we have

$$\mathrm{Mat}_r(K \otimes_k D^{\mathrm{opp}}) \cong K \otimes_k \mathrm{Mat}_r(D^{\mathrm{opp}}) \cong K \otimes_k A \cong A_K \cong \mathrm{Mat}_n(K).$$

The K-dimension is thus

$$n^2 = r^2 \dim_k D.$$

Comparing with the above yields $\dim_k D = (\dim_k D)^2$, whence $\dim_k D = 1$.

Now we assume conversely that $\mathrm{End}_A(V) = D = k$. Then $A \cong \mathrm{Mat}_n(k)$ for some integer $n \geq 1$. Hence, under this isomorphism V is isomorphic to the simple module k^n, which is absolutely irreducible by Lemma 2.1.18 (a). □

Corollary 2.3.12 *Let A be a simple k-algebra. Its simple module is absolutely irreducible if and only if $A \cong \mathrm{Mat}_r(k)$ for some r.*

Proof. This follows from Theorem 2.3.11 and Wedderburn's Theorem 2.1.26, which states $A \cong \mathrm{Mat}_r(D^{\mathrm{opp}})$ with $D = \mathrm{End}_A(S)$ with S the only simple A-module. □

Proposition 2.3.13 *Let k be a field and let D be a finite dimensional division k-algebra. Then any maximal subfield of D is a separable extension of k.*

Proof. (See [Kersten], Theorem 10.2.) Omitted. □

Corollary 2.3.14 *Let k be a field and A a finite dimensional k-algebra. There is a finite separable splitting field of A.*

Proof. Let S_i be the finitely many simple A-modules and $D_i = \mathrm{End}_A(S_i)$ the corresponding division algebras. For each D_i, let K_i be the field provided by Theorem 2.3.5 such that $(D_i)_{K_i} = \mathrm{Mat}_{s_i}(K_i)$. The field K_i is finite and separable (by Proposition 2.3.13), hence the composite K of all the K_i is also a finite separable extension of k.

As the statement is about simple modules, we can work with $B := A/\operatorname{Jac}(A)$. Since K is separable, $B_K = A_K/(K \otimes_k \operatorname{Jac}(A))$ is also semi-simple by Proposition 2.2.3. We have $B = \prod_i B_i$ and each B_i is of the form $\mathrm{Mat}_{r_i}(D_i^{\mathrm{opp}})$ by Wedderburn's Theorem 2.1.26. Consequently,

$$B_K = \prod_i (B_i)_K \cong \prod_i \mathrm{Mat}_{r_i}((D_i^{\mathrm{opp}})_K) \cong \prod_i \mathrm{Mat}_{r_i}(\mathrm{Mat}_{s_i}(K)) \cong \prod_i \mathrm{Mat}_{r_i s_i}(K)$$

by Lemma 2.1.18 (d). Hence, every simple module of B_K is absolutely simple. Since the simple modules of B_K are the same as those of A_K (as $K \otimes_k \operatorname{Jac}(A) \subseteq \operatorname{Jac}(A_K)$ acts trivially), the corollary follows. □

Remark 2.3.15 *We should mention that the theory we are exposing is about the Brauer group, which, however, we do not wish to define.*

At the end of this section, we draw the reader's attention to Exercise 17, in which a simple but not absolutely simple module should be exhibited.

2.4 Character theory

Definition 2.4.1 *Let A be a k-algebra and V an A-module of finite k-dimension. After choosing a basis, every element $a \in A$ acts on V via a matrix, so it makes sense to speak of its trace.*

The character of V *is defined as the map*

$$A \longrightarrow k, \quad a \mapsto \mathrm{Tr}_V(a).$$

If K/k is a field extension and W an A_K-module, then we will often also consider the character of W as an A-module, i.e.

$$A \to A_K \xrightarrow{\chi} K.$$

We use the same notation.

Remark 2.4.2 *(i) If $B \subset A$ is a spanning set of A as a K-vector space (e.g. a basis), any character χ is uniquely determined by the values $\chi(b)$ for $b \in B$, as χ is a vector space homomorphism.*

The standard application of this concerns group algebras $A = k[G]$. Any character χ is determined by $\chi(g)$ for $g \in G$. The usual use of the word 'character' is in this sense.

Another important application is to the situation of a field extension K/k and an A_K-module W, affording a character $\chi : A_K \to K$. It is uniquely determined by its values on A (via the natural embedding $A \hookrightarrow A_K$). This will be very important in the sequel, in particular, for applications to the definability of Galois representations.

(ii) In certain cases, it makes sense and it is very useful not to consider the natural matrix action from the definition. For instance, let D be a division quaternion k-algebra, which is split over K. Then the k-dimension of the simple D-module D is 4, but, splitting the algebra $D_K = \mathrm{Mat}_2(K)$ has the consequence that D_K has a 2-dimensional simple K-module. Its trace and determinant are called the reduced trace/determinant. *They are half (resp. the square root) of the other trace (resp. determinant).*

Proposition 2.4.3 *Let k be a field of characteristic 0, A a k-algebra and V, V' two semi-simple A-modules of finite k-dimension. If the characters of V and V' are the same (i.e. if $\mathrm{Tr}_V(a) = \mathrm{Tr}_{V'}(a)$ for all $a \in A$), then V and V' are isomorphic as A-modules.*

Proof. (See [Bourbaki], p. 136.) Since the statement is about semi-simple modules, we may assume that A is a semi-simple algebra. Letting it act on $V \oplus V'$ me may further assume, using Corollary 2.1.27, that we have

$$A \cong \prod_{i=1}^{r} \mathrm{Mat}_{r_i}\big(\mathrm{End}_k(S_i)\big)$$

with the simple A-modules S_i occuring in one of V or V'.

The only question is whether the multiplicities n, n' with which a given simple module S, say $S = S_1$, appears in V and V' are equal. For that we just take the element $c \in A$ which is the identity on S and 0 elsewhere. We have $\mathrm{Tr}_V(c) = n \cdot \dim S$ and similarly for V', from which the result is clear, using that k has characteristic 0, as $n \cdot \dim S = n' \cdot \dim S$ follows. □

Theorem 2.4.4 (Burnside-Frobenius-Schur) *Let A be a finite dimensional k-algebra. The characters of the simple A-modules are k-linearly independent, if k is a splitting field of A or k is of characteristic* 0.

Proof. (See [CurtisReiner], 27.8.) Since all the modules in question are simple and thus $\mathrm{Jac}(A)$ acts trivially, we may assume that A is semi-simple. By Corollary 2.1.27 we have

$$A \cong \prod_{i=1}^{r} \mathrm{End}_k(S_i) \cong \prod_{i=1}^{r} \mathrm{Mat}_{r_i}(D_i^{\mathrm{opp}})$$

with $D_i = \mathrm{End}_A(S_i)$ for the simple A-modules S_i.

Assume first that k is a splitting field. Then the decomposition becomes

$$A \cong \prod_{i=1}^{r} \mathrm{Mat}_{r_i}(k).$$

The characters of the simple modules $S_i \cong k^{r_i}$ are now obviously linearly independent, since in A we can choose elements that are zero in all matrix algebras except one, where we put a single 1 on the diagonal.

Now assume that k is of characteristic 0. Let K be a splitting field of A. Let S_i for $i = 1, \ldots, r$ be the simple A-modules, and W_j for $j = 1, \ldots, s$ the simple A_K-modules. Hence, there are integers $a_{i,j}$ such that

$$(S_i)_K \cong \bigoplus_j (W_j)^{a_{i,j}}.$$

From Lemma 2.2.6 it follows that $(S_i)_K$ and $(S_{i'})_K$ do not have any composition factor in common if $i \neq i'$; hence for a given j there is a single $i =: i_j$ with $a_{i_j,j} \neq 0$. Let σ_i be the character of S_i and τ_j the character of W_j. Note that any character $\sigma_i : A \to \mathrm{End}_k(S_i) \xrightarrow{\mathrm{Tr}} k$ is equal to $A \to A_K \to \mathrm{End}_K((S_i)_K) \xrightarrow{\mathrm{Tr}} K$. It follows that $\sigma_i = \sum_j a_{i,j}\tau_j$. If we now have

$$0 = \sum_i b_i \sigma_i,$$

then we obtain

$$0 = \sum_i \sum_j b_i a_{i,j} \tau_j = \sum_j b_{i_j} a_{j_i,j} \tau_j,$$

implying $b_i = 0$ for all i, as desired. □

Corollary 2.4.5 *Absolutely irreducible modules are uniquely characterized by their characters.*

Proof. (See [CurtisReiner], 30.15.) Let S_1 and S_2 be absolutely irreducible modules. Replacing A by its image in $\mathrm{End}_k(S_1 \oplus S_2)$ if necessary, we may and do assume that k is a splitting field of A. By Theorem 2.4.4, the corresponding characters are k-linearly independent and hence different. □

This corollary, for example, tells us that simple modules are uniquely determined by their characters, when the field is algebraically closed. The most complete result about characters is the following theorem by Brauer and Nesbitt, where the assumption of the simplicity is dropped. Moreover, it also works when the field over which the algebra is defined is not the splitting field (in the proof we will see that it is no loss of generality to pass to the splitting field).

The Brauer-Nesbitt theorem says that the composition factors of a module are uniquely characterized by the character of the module. This is, of course, best possible: The characteristic polynomial does not see the difference between a diagonal matrix and a matrix with the same diagonal and some non-zero entries above the diagonal.

Theorem 2.4.6 (Brauer-Nesbitt) *Let k be any field and A a k-algebra. Let M, N be two A-modules which are finite-dimensional as k-vector spaces. If for all $a \in A$, the characteristic polynomials on M and N are equal, then M and N have the same composition factors, i.e. define the same element in the Grothendieck group.*

Proof. (See [CurtisReiner], 30.16.) For this question we may and do assume that A is a semi-simple finite dimensional k-algebra: if necessary, replace M and N by the direct sum of its composition factors; this does not change the characteristic polynomials; and, if necessary, replace A by its image in $\mathrm{End}_k(M \oplus N)$.

Assume that the action of A on M and N has the same characteristic polynomials, but that M and N are not isomorphic. By splitting off common composition factors, we also assume that M and N do not have any composition factor in common. We want to show that M and N are zero.

Let K be a Galois splitting field of A of finite degree over k. By Proposition 2.2.3, also A_K is semi-simple. The characteristic polynomials of the action of any $a \in A_K$ on M_K and N_K are the same. We again split off all common composition factors, in order to assume that M_K and N_K do not have any factor in common. We have decompositions into simple A_K-modules: $M_K \cong \bigoplus_i S_i^{e_i}$ and $N_K \cong \bigoplus_j T_j^{f_j}$. Let σ_i and τ_j be the characters corresponding to the simple modules S_i and T_j, respectively. As the characteristic polynomials are the same, we have the equality

$$\sum_i e_i \sigma_i = \sum_j f_j \tau_j .$$

By Theorem 2.4.4, it follows that e_i and f_j are all 0 in K. If the characteristic of K is zero, the proof is finished. Assume now that the characteristic of k is p, then we obtain $p \mid e_i$ and $p \mid f_j$ for all i, j.

We now crucially use that we know that the characteristic polynomials are the same and not only the traces. The above yields the existence of A_K-modules M_1 and N_1 such that $M_K \cong M_1^p$ and $N_K \cong N_1^p$. It follows that the characteristic polynomials of the A_K-action on M_1 and N_1 are the same, since taking p-th roots is unique. By Theorem 2.4.4 we again conclude that $M_1 \cong M_2^p$ and $N_1 \cong N_2^p$. Since the degree of the polynomials is divided by p in each step, we obtain a contradiction. □

Remark 2.4.7 *There are different formulations of Theorem 2.4.6:*

(i) The statement on the characteristic polynomials can also be formulated in a more fancy way. An A-module V is determined by the traces of the action of A on all exterior powers $\bigwedge^i V$ for $i = 1, \ldots, d$, where d is the dimension of V. For 2-dimensional representation this just means 'by the trace and the determinant'.

(ii) In [CurtisReiner], the statement of Brauer-Nesbitt involves characteristic roots (i.e. the roots of the characteristic polynomial) instead of characteristic polynomials. But, of course, a monic polynomial is uniquely determined by and uniquely determines its roots.

(iii) Due to Remark 2.4.2 (i), it suffices to test a basis.

To say it very clearly again: By Corollary 2.4.5, the absolutely simple A_K-modules are uniquely determined by the values of their characters at elements in A (and by $g \in G$ in case $A = k[G]$). By Theorem 2.4.6, the composition factors of any A_K-module W are uniquely determined by the characteristic polynomials at $a \in A$ (respectively, at $g \in G$ in case $A = k[G]$).

(iv) Let k be a field, G a group and V a $k[G]$-module of finite k-dimension d. If k is of characteristic 0 or if d is smaller than the characteristic of k, then by Theorem 2.4.6 the traces of powers of generators of G uniquely characterize V.

For this one uses that

$$X_1 + \cdots + X_d,\ X_1^2 + \cdots + X_d^2,\ \ldots,\ X_1^d + \cdots + X_d^d$$

generate the space of symmetric functions in the variables $X_1, \ldots, X_d$, under the above assumptions.

Corollary 2.4.8 *Up to semi-simplification, reductions of l-adic representations are unique, i.e. their images in the Grotendieck group over the finite field are unique.*

Proof. The characteristic polynomials of the reduction are the reduction of the characteristic polynomials. By Brauer-Nesbitt (Theorem 2.4.6) the characteristic polynomials determine the module over the finite field uniquely. □

There is also an alternative proof for this corollary, which I found in an article by Serre. This proof really makes use that the representation is a reduction.

Remark 2.4.9 *This would be a good place to recall class functions, orthogonality of characters, character tables, etc. We just refer to the literature.*

2.5 Definability of Galois representations

In this section we use the theory developed so far in order to determine for a given representation $\rho : G \to \mathrm{GL}_n(\overline{K})$ over which field $K \subset \overline{K}$ it can be minimally defined (after suitable conjugation).

Here is the situation we are looking at in the beginning of the section. We let k be a field, A a k-algebra and K a separable extension of k (not necessarily Galois). Let W be a simple A_K-module of finite K-dimension.

Definition 2.5.1 *We let*

$$\rho : A \to A_K \to \mathrm{End}_K(W)$$

be the representation belonging to W (considered as an A-module) and we let

$$\chi = \mathrm{Tr}(\rho) : A \to K$$

be its character.

The field $k(\rho)$ is defined as the extension of k (inside some fixed algebraic closure) that is generated by all the coefficients of all characteristic polynomials of ρ.

The field $k(\chi)$ is the extension of k that is generated by all the values of χ.

Lemma 2.5.2 *Assume that K/k is Galois and that K is a splitting field of A. Then the following statements are equivalent:*

(i) $D_W = \mathrm{Gal}(K/k)$

(ii) $k = k(\rho)$

(iii) $k = k(\chi)$

Proof. $(i) \Rightarrow (ii)$: If $D_W = \mathrm{Gal}(K/k)$, then $W \cong {}^\sigma W$ for all $\sigma \in \mathrm{Gal}(K/k)$. Consequently, the characteristic polynomials for W and ${}^\sigma W$ are the same at all $a \in A$. As the second one is obtained from the first by applying σ to the coefficients, it follows that the characteristic polynomial is invariant under $\mathrm{Gal}(K/k)$. Consequently, all its coefficients lie in k.

$(ii) \Rightarrow (iii)$: Trivial.

$(iii) \Rightarrow (i)$: As the characters of W and ${}^\sigma W$ are conjugate by σ and all their values are in k, the characters are the same. By Corollary 2.4.5 all simple A_K-modules are uniquely determined by their characters at $a \in A$, since K is a splitting field of A. Consequently, W is isomorphic to ${}^\sigma W$ for all $\sigma \in \mathrm{Gal}(K/k)$. □

Lemma 2.5.3 *If in Lemma 2.5.2 we do not assume any more that K is a splitting field of A, then the equivalence between (i) and (ii) stays correct.*

Proof. It suffices to use the Brauer-Nesbitt theorem, Theorem 2.4.6, to conclude from $k = k(\rho)$ that W and ${}^\sigma W$ are isomorphic. □

Corollary 2.5.4 *Let K/k be a separable extension, A a k-algebra, V a simple A-module and W any simple A_K-module occuring in the decomposition series of V_K.*

(a) Assume that K is a splitting field of A and $k = k(\chi)$ or

(b) assume that $k = k(\rho)$.

Then there is an integer e such that $V_K \cong W^e$.

Proof. For a Galois extension, this follows from Lemmas 2.5.2 and 2.5.3 and Corollary 2.2.12. The general case is a consequence. □

Corollary 2.5.5 *Suppose that K/k is finite Galois. We have $k(\rho) = K^{D_W}$ and also $k(\chi) = K^{D_W}$ if K is a splitting field.*

Proof. We only write out the proof for K a splitting field. Let H be the subgroup such that $k(\rho) = K^H$. We have $\sigma \in D_W \Leftrightarrow {}^{\sigma}W \cong W \Leftrightarrow \sigma(\mathrm{charpoly}(a)) = \mathrm{charpoly}(a)\ \forall a$. This is further equivalent to σ fixing $k(\rho)$ and hence to $\sigma \in H$. We used Corollary 2.4.5. If K is not a splitting field, the first statement follows from Brauer-Nesbitt, Theorem 2.4.6. □

Corollary 2.5.6 *Suppose that K/k is finite Galois. We have*

$$[k(\rho) : k]\#D_W = [K : k]$$

and

$$[k(\chi) : k]\#D_W = [K : k]$$

if K is a splitting field

Proof. This is immediate from Corollary 2.5.5. □

Corollary 2.5.7 *Let V be a simple module and suppose that k contains the values of χ. Let K be a separable splitting field. The exponent e in $V_K \cong W^e$ (see Corollary 2.5.4) is equal to the index of the division algebra $D := \mathrm{End}_A(V)$, i.e. to the square root of $\dim_k D$. By Theorem 2.3.5, e is hence equal to $[L : k]$, where L is any maximal subfield of D.*

Proof. We have

$$K \otimes_k D = K \otimes_k \mathrm{End}_A(V) = \mathrm{End}_{A_K}(V_K) = \mathrm{End}_{A_K}(W^e) = \mathrm{Mat}_e\left(\mathrm{End}_{A_K}(W)\right) = \mathrm{Mat}_e(K),$$

using Proposition 2.1.23 and Theorems 2.2.4 and 2.3.11. Thus, k-dimension of D is e^2. □

Definition 2.5.8 *Let K/k be a field extension, A a k-algebra and*

$$\rho : A_K \to \mathrm{Mat}_n(K)$$

be a representation. We say that ρ is realizable over k *if ρ is equivalent to a representation*

$$\rho_1 : A_K \to \mathrm{Mat}_n(K)$$

such that for all $a \in A$ the image $\rho_1(a)$ lies in $\mathrm{Mat}_n(k)$.

Remark 2.5.9 *If the representation ρ is $A_K \to \mathrm{End}_K(W)$, then ρ is realizable over k if and only if there exists an A-module V such that V_K is isomorphic to W as A_K-modules.*

Indeed, $W = K^n$ and $V = k^n$ for the same n.

Corollary 2.5.10 *Let W be an absolutely simple A_K-module in the above set-up. Suppose $V_K \cong W^e$. It is obviously necessary that k contains the values of χ for W to be realizable over k.*

Suppose that k contains the values of χ. Then the following statements are equivalent:

(i) *W is realizable over k.*

(ii) *$e = 1$.*

(iii) *V is absolutely simple as A_k-module.*

Proof. We have already observed the first equivalence in the preceding remark. The second equivalence follows from Theorem 2.3.11 and Corollary 2.5.7: $D = \mathrm{End}_A(V)$ has k-dimension $e = 1$ if and only if V is absolutely simple. □

Corollary 2.5.11 *Suppose k contains the values of χ. Then W is realizable over an extension F of k if and only if F splits $D = \mathrm{End}_A(V)$.*

Proof. This follows directly by applying Corollary 2.5.10 with F in the place of k. □

Definition 2.5.12 *Let ρ be a representation over k. The* Schur index of ρ *is defined as the minimum of $[K : k(\chi)]$ where K runs through the extentions of $k(\chi)$ over which ρ is realizable.*

Corollary 2.5.13 *The Schur index is less than or equal to $[F : k(\chi)]$, where F is any maximal subfield contained in D with $D = \mathrm{End}_{A_{k(\chi)}}(V)$ for any simple $A_{k(\chi)}$-module V such that W is in the composition series of V_K.*

Proof. We know that D is split by any maximal subfield F of D. Hence, $V_F = X^f$ for some simple A_F-module X. However, X is absolutely simple, since D is split by F (see the proof of Corollary 2.3.14). Consequently, $f = 1$ and $X_K = W$. □

Corollary 2.5.14 *Let K be a topological field and let $\rho : G \to \mathrm{GL}_n(\overline{K})$ be a group representation.*

(a) *If $\overline{K} = \overline{\mathbb{F}}_p$, then ρ can be realized over $\mathbb{F}_p(\chi)$.*

(b) *If $n = 2$, then ρ can be realized over an extension of degree 2 of $K(\chi)$.*

Proof. This follows from Corollary 2.5.13. For (a) we use that there is no finite non-commutative division algebra. In (b), the algebra D can only be a quaternion algebra, since after splitting it is a 2×2-matrix algebra. Its maximal subfield has degree at most 2. □

Remark 2.5.15 *(i) A theorem of Witt-Fein states $Z(\mathrm{End}_A(V)) = k(\chi)$.*

(ii) In Corollary 2.5.13 the inequality is in fact an equality. This follows from the fact that an algebra D cannot be split by fields that have a smaller degree than the biggest subfield.

Chapter 3

Local theory

3.1 Conductor

The point of view on conductors adopted in [Neukirch] and in [SerreLocalFields] is to treat all characters of some finite Galois group at once, using that the set of the characters of all irreducible representations of a finite group (over a characteristic zero field) uniquely determines the group. This point of view is very elegant and leads, for instance, to the 'Führerdiskriminantenproduktformel', which is quite famous, probably mostly due to its long name.

We, however, will be mainly interested in representations with coefficient in fields of characteristic ℓ and also in ℓ-adic representations which typically have infinite images. These two reasons lead us to adopt the point of view of considering individual characters rather than the set of all characters at once.

As a consequence, many of the proof in [SerreLocalFields] do not work without change. I have not worked out in how far one can replace characteristic zero representation theory in Serre's proofs by Brauer's modular representation theory. Instead, I wrote some of the proofs myself, in particular, those for computing the conductor of an induced representation and the fact that conductor exponents are integers. However, the largest part of this section is still quite close to Serre's treatment, as will be obvious to the reader.

Ramification groups

For this section let L/K be a finite Galois extension of local fields (complete with respect to a discrete valuation v_K, with valuation ring $\mathcal{O}_K$, maximal ideal (valuation ideal) $\mathfrak{p}_K = (\pi_K)$, perfect residue field $\mathbb{F}_K = \mathcal{O}_K/\mathfrak{p}_K$ such that $v_K(K) = \mathbb{Z}$, and similarly for L). We have

$$v_L|_K = e_{L/K} v_K$$

with $e_{L/K}$ the ramification index. We put $f_{L/K} = [\mathbb{F}_L : \mathbb{F}_K]$. We write G for $\mathrm{Gal}(L/K)$.

Definition 3.1.1 *Let $s \geq -1$ be a real number. The s-th* ramification group (in lower numbering) *is defined as*

$$G_s = G(L/K)_s = \{\sigma \in \mathrm{Gal}(L/K) | v_L(\sigma a - a) \geq s + 1 \forall a \in \mathcal{O}_L\}.$$

In terms of absolute values, and hence of distances, the definition means, roughly speaking, that $\sigma \in G_s$ if σa stays as close to a as indicated by s.

Example 3.1.2 *We look at some particular cases:*

(i) If $s = -1$, then it is clear that $G_{-1} = \mathrm{Gal}(L/K)$.

(ii) If $s = 0$, then it is easy to see that G_0 is the inertia group of the extension L/K.

(iii) If $s = 1$, then G_1 is the wild inertia group. This will become clear in a moment.

Lemma 3.1.3 *The G_s are normal subgroups of $G = \mathrm{Gal}(L/K)$.*

Proof. Let $\sigma \in G_s$ and $\tau \in G$. Then we have, using that τ does not change the valuation of an element:

$$v_L(\tau^{-1}\sigma\tau a - a) = v_L(\tau^{-1}(\sigma\tau a - \tau a)) = v_L(\sigma(\tau a) - \tau(a)).$$

As $\tau\mathcal{O}_L = \mathcal{O}_L$, the lemma follows. □

Interpretation of the G_s

Lemma 3.1.4 *Let L/K be as above, but assume that L/K is totally ramified, i.e. $e_{L/K} = [L : K]$. Then $\mathcal{O}_K[\pi_L] = \mathcal{O}_L$.*

Proof. It turns out that the characteristic polynomial (in $\mathcal{O}_K[X]$) of π_L is an Eisenstein polynomial and hence irreducible. For details, see Serre: Corps Locaux, p. 30. □

Proposition 3.1.5 *Let L/K any finite Galois extension of local fields. Then there is $x \in \mathcal{O}_L$ such that $\mathcal{O}_K[x] = \mathcal{O}_L$.*

Proof. (Note that we insisted that the residue fields $\mathbb{F}_L$ and $\mathbb{F}_K$ are perfect. For this proof we only need that the extension $\mathbb{F}_L/\mathbb{F}_K$ is separable.) Let π be any uniformiser of L, i.e. $(\pi) = (\pi_L)$. Write $e = e_{L/K}$ and $f = f_{L/K}$.

Claim: If $x \in \mathcal{O}_L$ such that $\mathbb{F}_L = \mathbb{F}_K(\bar{x})$, then $\{x^j\pi^i | j = 0, \ldots, f-1, i = 0, \ldots, e-1\}$ generate $\mathcal{O}_L$ as $\mathcal{O}_K$-module. (We denote by $\bar{x}$ the image of x modulo $\mathfrak{P}_L$.)

Every $y \in \mathcal{O}_L/\pi_K\mathcal{O}_L = \mathcal{O}_L/(\pi^e)$ has a representative of the following form:

$$\begin{aligned} y &= \epsilon_0 + \pi y_1 \\ &= \epsilon_0 + \pi_L(\epsilon_1 + \pi_L y_2) \\ &= \ldots \\ &= \epsilon_0 + \pi_L\epsilon_1 + \pi_L^2\epsilon_2 + \cdots + \pi_L^{e-1}\epsilon_{e-1}. \end{aligned}$$

with ϵ_i in a system of representatives of $\mathcal{O}_L/(\pi) = \mathbb{F}_L$ and $y_i \in \mathcal{O}_L$. All ϵ_i can be uniquely written as $\mathbb{F}_K$-linear combinations of $\bar{x}^0, \bar{x}^1, \ldots, \bar{x}^{f-1}$. Hence, the set in the claim generates $\mathcal{O}_L/\pi_K\mathcal{O}_L$ as $\mathcal{O}_K$-module. The claim is now a direct consequence of Nakayama's lemma.

Now we want to choose a good x. For this we choose any $y \in \mathcal{O}_L$ such that $\mathbb{F}_L = \mathbb{F}_K(\bar{y})$. Let $\bar{m} \in \mathbb{F}_K[X]$ be the minimal polynomial of $\bar{y}$ and choose any lift $m \in \mathcal{O}_K[X]$ of $\bar{m}$. If $v_L(m(y)) = 1$, then choose $x := y$. If not, then let $x := y + \pi_L$. In both cases we have $v_L(m(x)) = 1$. For in the second case, we can use the Taylor expansion

$$m(x) = m(y + \pi_L) = m(y) + \pi_L m'(y) + \pi_L^2 z$$

for some $z \in \mathcal{O}_L$. Note that $m'(y)$ is a unit, since its reduction is non-zero in $\mathbb{F}_L$, as $\bar{m}$ is separable. Thus, $v_L(m(x)) = 1$. Choosing the uniformiser $\pi = m(x)$, the proposition now follows from the claim with x and π. □

Definition 3.1.6 *Suppose $\mathcal{O}_L = \mathcal{O}_K[x]$. For $\sigma \in G$ let*

$$i_{L/K}(\sigma) = i_G(\sigma) = v_L(\sigma x - x).$$

Lemma 3.1.7 *Let $\sigma \in G$. We have*

$$\sigma \in G_s \Leftrightarrow i_G(\sigma) \geq s + 1.$$

Hence, $G_s = \{\sigma \in G | i_G(\sigma) \geq s + 1\}$.

Proof. The implication '⇒' is clear. For the other one, we only need to note that σ acts trivially on $\mathcal{O}_L/(\pi_L)^{s+1} = \mathcal{O}_K[x]/(\pi_L)^{s+1}$ if and only if $\sigma x - x \in (\pi_L)^{s+1}$. □

Proposition 3.1.8 *For all integers $s \geq 0$ the map*

$$G_s/G_{s+1} \to U_L^{(s)}/U_L^{(s+1)}, \quad \sigma \mapsto \frac{\sigma\pi_L}{\pi_L}$$

is an injective group homomorphism. Here, $U_L^{(0)} = \mathcal{O}_L^\times$ and $U_L^{(s)} = 1 + \pi_L^s\mathcal{O}_L$ for $s \geq 1$.

Proof. It is easily checked that the map is well defined and a group homomorphism. We may assume that L/K is totally ramified. By Lemma 3.1.4, π_L generates $\mathcal{O}_L$ as $\mathcal{O}_K$-module. Hence,

$$\sigma \in G_s \ \Leftrightarrow\ i_G(\sigma) = v_L(\sigma\pi_L - \pi_L) \geq s + 1.$$

Suppose $\sigma \in G_s$ such that $\frac{\sigma\pi_L}{\pi_L} \in U_L^{(s+1)}$. Then $\sigma\pi_L = \pi_L + \pi_L^{s+2}y$ for some $y \in \mathcal{O}_L$. Thus, $\sigma \in G_{s+1}$, proving the injectivity. □

Corollary 3.1.9 *We have*

$$G_0/G_1 \hookrightarrow (\mathbb{F}_L^\times, \times)$$

and

$$G_s/G_{s+1} \hookrightarrow (\mathbb{F}_L, +).$$

Proof. By Proposition 3.1.8, it suffices to prove that

$$U_L^{(0)}/U_L^{(1)} = \mathcal{O}_L^\times/(1+\pi\mathcal{O}_L) \longrightarrow (\mathcal{O}_L/\pi_L)^\times$$

and

$$U_L^{(s)}/U_L^{(s+1)} = (1+\pi^s\mathcal{O}_L)/(1+\pi^{s+1}\mathcal{O}_L) \xrightarrow{1+\pi_L^s y \mapsto y} \mathcal{O}_L/\pi_L$$

are isomorphisms. This is straight forward. □

Corollary 3.1.10 *Galois extensions of local fields are solvable.* □

Corollary 3.1.11 *Assume that K is a finite extension of $\mathbb{Q}_p$. The wild inertia group of L/K is equal to G_1.*

Proof. For $s \geq 1$ all the quotients G_s/G_{s+1} are p-groups. However, the order of G_0/G_1 divides $p^r - 1$, for some r, and is hence coprime to p, establishing that G_1 is a p-Sylow of G_0. In fact, it is the unique p-Sylow due to the fact that G_1 is a normal subgroup of G_0. □

Change of field

It is easy to pass to subextensions:

Proposition 3.1.12 *Let L' be a field such that $L/L'/K$. Then for all $s \geq -1$*

$$G_s(L/K) \cap G(L/L') = G_s(L/L').$$

Moreover,

$$i_G(\sigma) = i_H(\sigma)$$

for $\sigma \in H = \mathrm{Gal}(L/L') \subseteq \mathrm{Gal}(L/K)$.

Proof. This follows from the definition. □

The corresponding statement for quotients is wrong. Our next aim is to work out how the numbering changes when passing from G to G/H (assuming that L'/K is Galois).

Proposition 3.1.13 *Let $L/L'/K$ be finite Galois extensions. We have*

$$e_{L/L'} i_{L'/K}(\sigma') = \sum_{\tau \in H} i_{L/K}(\sigma\tau)$$

with $H = \mathrm{Gal}(L/L')$, $\sigma \in G(L'/K)$ and $\sigma \in G(L/K)$ any element restriction to σ'.

Proof. Let $x \in \mathcal{O}_L$ and $y \in \mathcal{O}_{L'}$ such that $\mathcal{O}_L = \mathcal{O}_K[x]$ and $\mathcal{O}_{L'} = \mathcal{O}_K[y]$. Define the following two polynomials:

- $g(X) \in \mathcal{O}_K[X] : g(x) = y$

- $f(X) \in \mathcal{O}_{L'}[X]$ is the minimal polynomial of x over L', hence, $f(X) = \prod_{\tau \in H}(X - \tau x)$.

Now let σ and σ' as in the statement. We first apply σ to the coefficients of f. Then all coefficients of $(\sigma f)(X) - f(X)$ are in $\mathcal{O}_{L'}$ and their L-valuation is at least $v_L(\sigma' y - y)$, as this is the lowest non-zero valuation of an element of $\mathcal{O}_{L'}$. Consequently,

$$v_L(\sigma' y - y) \leq v_L((\sigma f)(x) - f(x)) = v_L((\sigma f)(x)).$$

We shall now also establish this inequality in the opposite direction. For this note that $g(X) - y \in \mathcal{O}_{L'}[X]$ has x as a zero. Consequently, it is divisible by f, i.e.

$$g(X) - y = f(X)h(X)$$

for some $h \in \mathcal{O}_{L'}[X]$. We now apply σ again to the coefficients on both sides and obtain

$$(\sigma g)(X) - \sigma y = g(X) - \sigma y = (\sigma f)(X)(\sigma h)(X).$$

Plugging in x yields:

$$y - \sigma' y = (\sigma f)(x) \cdot (\sigma h)(x),$$

whence

$$v_L(\sigma' y - y) \geq v_L((\sigma f)(x)),$$

so that we have equality.

To finish the proof, we note that

$$(\sigma f)(x) = \prod_{\tau \in H}(x - \sigma\tau x),$$

so that

$$v_L((\sigma f)(x)) = \sum_{\tau \in H} v_L(\sigma\tau x - x).$$

Finally,

$$v_L(\sigma' y - y) = e_{L/L'} v_{L'}(\sigma' y - y),$$

completing the proof. □

Definition 3.1.14 *Let L/K be a finite Galois extension of local fields. We define the piecewise constant (step) function:*

$$\alpha_{L/K} : [-1, \infty) \to (0, 1], \quad s \mapsto \frac{1}{(G_0 : G_s)},$$

if $i \leq s < i + 1$ with $i \in \mathbb{Z}_{\geq -1}$. Further, we define the Herbrand function

$$\eta_{L_K} : [-1, \infty) \to [-1, \infty), \quad s \mapsto \int_0^s \alpha_{L/K}(u) du.$$

It is customary to write g_s for $\#G_s$, which we shall also do.

Note that $\alpha_{L/K}(s) = \frac{1}{(G_0:G_{i+1})}$ if $i \leq s < i+1$ with $i \in \mathbb{Z}_{\geq -1}$.

Remark 3.1.15 *The Herbrand function $\eta = \eta_{L/K}$ satisfies the following properties:*

(i) $\eta(0) = 0$

(ii) $\eta(-r) = -r$ *for* $-1 \leq r \leq 0$.

(iii) $\eta'(s) = \frac{g_s}{g_0} = \frac{g_{\lceil s \rceil}}{g_0}$ *for* $s \notin \mathbb{Z}$.

(iv) η *is strictly increasing and continuous.*

(v) $\eta(s) = \frac{1}{g_0}\big(g_1 + g_2 + \cdots + g_{\lfloor s \rfloor} + (s - \lfloor s \rfloor) g_{\lceil s \rceil}\big)$ *for* $s > 0$.

Proposition 3.1.16 *Let* $\theta(s) = -1 + \frac{1}{g_0}\sum_{\sigma \in G} \min\{i_{L/K}(\sigma), s+1\}$. *Then* $\eta_{L/K}(s) = \theta(s)$.

Proof. The function θ is continuous and piecewise linear. We shall compare it with η at 0 and establish that the slopes of all linear pieces coincide, yielding equality. We have

$$\min\{i_{L/K}(\sigma), s+1\} = \begin{cases} s+1 & \text{if } \sigma \in G_s \\ i_{L/K}(\sigma) & \text{if } \sigma \notin G_s. \end{cases}$$

Consequently,

$$\theta(0) = -1 + \frac{1}{g_0}\sum_{\sigma \in G} \min\{i_{L/K}(\sigma), 1\} = -1 + \frac{1}{g_0}\sum_{\sigma \in G_0} 1 = 0 = \eta_{L/K}(0).$$

For $s \notin \mathbb{Z}$, say $i < s < i+1$, we now compute the slope of θ at s:

$$\begin{aligned} \theta'(s) &= \frac{1}{g_0}\#\{\sigma \in G | s+1 < i_{L/K}(\sigma)\} && \text{(slopes are } 0 \text{ or } 1) \\ &= \frac{1}{g_0}\#\{\sigma \in G | i+2 < i_{L/K}(\sigma)\} && (\lceil s \rceil = i+1) \\ &= \frac{g_{i+1}}{g_0} = \eta'_{L/K}(s). \end{aligned}$$

The proposition follows. □

Lemma 3.1.17 *Let $L/L'/K$ be finite Galois extensions and let $H = \mathrm{Gal}(L/L')$. Let $\sigma' \in G(L'/K)$ and let $\sigma \in G(L/K)$ restricting to σ' such that $i_{L/K}(\sigma)$ is maximal (among the σ restricting to σ'). Then we have*

$$\eta_{L/L'}(i_{L/K}(\sigma) - 1) = i_{L'/K}(\sigma') - 1.$$

Proof. We have for $\tau \in H$:

$$i_{L/K}(\sigma\tau) = \min\{i_{L/K}(\tau), i_{L/K}(\sigma)\}. \tag{3.1.1}$$

For, if $i_{L/K}(\tau) < i_{L/K}(\sigma)$, then

$$i_{L_K}(\sigma\tau) = v_L(\sigma\tau x - x) = v_L((\sigma x - x) + \sigma(\tau x - x)) = i_{L/K}(\tau).$$

If, on the other hand, $i_{L/K}(\tau) \geq i_{L/K}(\sigma)$, then $\sigma, \tau \in G_{i_{L/K}(\sigma)-1}$, whence $i_{L/K}(\sigma\tau) \geq i_{L/K}(\sigma)$ and, thus, $i_{L/K}(\sigma\tau) = i_{L/K}(\sigma)$ due to the maximality of $i_{L/K}(\sigma)$, establishing Equation 3.1.1.

Using Proposition 3.1.13, we now obtain

$$i_{L'/K}(\sigma') = \frac{1}{e_{L/L'}} \sum_{\tau\in H} i_{L/K}(\sigma\tau) = \frac{1}{e_{L/L'}} \sum_{\tau\in H} \min\{i_{L/K}(\tau), i_{L/K}(\sigma)\}.$$

Noting that $e_{L/L'} = \#H_0$, $i_{L/K}(\tau) = i_{L/L'}(\tau)$ and substracting 1 yields

$$i_{L'/K}(\sigma') - 1 = -1 + \frac{1}{e_{L/L'}} \sum_{\tau\in H} \min\{i_{L/K}(\tau), i_{L/K}(\sigma)\} = \eta_{L/L'}(i_{L/K}(\sigma) - 1),$$

by appealing to Proposition 3.1.16. □

We now obtain the behaviour of ramification groups (in lower numbering) when passing to quotients.

Theorem 3.1.18 (Herbrand) *Let $L/L'/K$ be finite Galois extensions and let $H = \mathrm{Gal}(L/L')$. Then for all $s \in [-1, \infty)$ we have*

$$G_s(L/K)H/H \cong G_t(L'/K)$$

with $t = \eta_{L/L'}(s)$.

Proof. Let $\sigma \in G(L'/K)$. Then we have the equivalences:

$$\begin{aligned} \sigma' \in G_sH/H &\Leftrightarrow \exists\sigma \in G : \sigma|_L = \sigma', \sigma \in G_s \\ &\Leftrightarrow \exists\sigma \in G : \sigma|_L = \sigma', i_{L/K}(\sigma) - 1 \geq s \\ &\Leftrightarrow \eta_{L/L'}(i_{L/K}(\sigma) - 1) \geq \eta_{L/L'}(s), \end{aligned}$$

since $\eta_{L/L'}$ is srictly increasing. In the last equivalence σ is chosen as in Lemma 3.1.17, so that we further obtain:

$$\begin{aligned} \sigma' \in G_sH/H &\Leftrightarrow i_{L'/K}(\sigma') - 1 \geq \eta_{L/L'}(s) \\ &\Leftrightarrow \sigma' \in G_{\eta_{L/L'}(s)}(L'/K), \end{aligned}$$

finishing the proof. □

Next we want to change the numbering of the ramification groups so that the numbering behaves well with respect to taking quotients (it will, however, not be compatible with taking subgroups any more). We need some preparations.

Proposition 3.1.19 *Let $L/L'/K$ be finite Galois extensions of local fields. Then we have*

$$\eta_{L/K} = \eta_{L'/K} \circ \eta_{L/L'}.$$

Proof. This is a simple computation starting from the formula in Herbrand's theorem:

$$(G/H)_{\eta_{L/L'}(s)} \cong G_sH/H \cong G_s/(G_s \cap H) = G_s/H_s.$$

Thus $\frac{\#G_s}{\#H_s} = \#(G/H)_{\eta_{L/L'}(s)}$. Using the multiplicativity of the ramification index, we obtain

$$\frac{1}{e_{L/K}}\#G_s = \big(\frac{1}{e_{L/L'}}\#H_s\big) \cdot \big(\frac{1}{e_{L'/K}}\frac{\#G_s}{\#H_s}\big) = \big(\frac{1}{e_{L/L'}}\#H_s\big) \cdot \big(\frac{1}{e_{L'/K}}\#(G/H)_{\eta_{L/L'}(s)}\big).$$

Instead of comparing $\eta_{L/K}$ with $\eta_{L'/K} \circ \eta_{L/L'}$ directly, we will again compute the slopes of the two and establish that both functions take the same value at 0, namely 0. The latter is clear, as $\eta(0) = 0$ for all fields. For the following computation note $e_{L/K} = \#G_0$.

$$\begin{aligned}\eta'_{L/K}(s) &= \frac{\#G_s}{\#G_0} = \frac{1}{e_{L/K}}\#G_s \\ &= \frac{\#H_s}{\#H_0} \cdot \frac{\#(G/H)_{\eta_{L/L'}(s)}}{\#(G/H)_0} \\ &= \eta'_{L/L'}(s) \cdot \eta'_{L'/K}(\eta_{L/L'}(s)) \\ &= (\eta_{L'/K} \circ \eta_{L/L'})'(s)\end{aligned}$$

by the chain rule. This finishes the proof. □

Definition 3.1.20 *The inverse function of* $\eta_{L/K}$ *is called* $\psi_{L/K}$.

Corollary 3.1.21 *We have* $\psi_{L/K} = \psi_{L/L'} \circ \psi_{L'/K}$.

Proof. Both $\psi_{L/K}$ and $\psi_{L/L'} \circ \psi_{L'/K}$ are inverse functions to $\eta_{L/K}$. Hence, they are equal. □

Definition 3.1.22 *For* $t \geq -1$ *we define the* ramification groups (in upper numbering) *as*

$$G^t(L/K) := G_{\psi_{L/K}(t)}.$$

(Then: $G^{\eta_{L/K}(s)}(L/K) = G_s(L/K)$*.)*

Corollary 3.1.23 *The upper numbering is compatible with forming quotients, i.e. for* $L/L'/K$ *finite Galois extensions and* $H = \mathrm{Gal}(L/L')$ *we have*

$$G^t(L/L)H/H \cong G^t(L'/K)$$

for all $t \geq -1$.

Proof. We have

$$\begin{aligned}G^t(L/K)H/H = G_{\psi_{L/K}(t)}H/H &\cong (G/H)_{\eta_{L/L'}(\psi_{L/K}(t))} \\ &= (G/H)_{\eta_{L/L'}(\psi_{L/L'}(\psi_{L'/K}(t)))} \\ &= (G/H)_{\psi_{L'/K}(t)} = (G/H)^t,\end{aligned}$$

proving the statement. □

Remark 3.1.24 *(a) If L/K is unramified, then $\eta_{L/K}(s) = s$ and $\psi_{L/K}(s) = s$.*

For, $1 = g_0 = g_1 = \dots$.

(b) We have $G_0(L/K) = G^0(L/K)$ and L/K is unramified if and only if $G^0(L/K) = 0$.

(c) L/K is tamely ramified $\Leftrightarrow G_1 = 0 \Leftrightarrow G_s = 0\ \forall s > 0 \Leftrightarrow G^t = 0\ \forall t > 0$.

Definition 3.1.25 *We say that s is a* jump for the lower numbering *if $G_{s-\epsilon} \neq G_{s+\epsilon}$ for all $\epsilon > 0$. We make a similar definition for the upper numbering.*

Example: cyclotomic fields

For $r \geq 1$ we let $K_r := \mathbb{Q}_p(\zeta_{p^r})$, where ζ_{p^r} is a primitive p^r-th root of unity. Recall that the p-th cyclotomic polynomial, i.e. the minimal polynomial of ζ_p, is equal to

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \dots + X + 1.$$

The p^r-th cyclotomic polynomial is

$$\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}}) = \prod_{i=1,(i,p)=1}^{p^r-1} (X - \zeta_{p^r}^i).$$

Consequently,

$$p = \prod_{i=1,(i,p)=1}^{p^r-1} (1 - \zeta_{p^r}^i).$$

We note further that with $(i,p) = 1$

$$(1 - \zeta_{p^r}^i) = (1 - \zeta_{p^r})(1 + \zeta_{p^r} + \zeta_{p^r}^2 + \dots + \zeta_{p^r}^{i-1})$$

and that $(1 + \zeta_{p^r} + \zeta_{p^r}^2 + \dots + \zeta_{p^r}^{i-1})$ is a unit, since reduction modulo the maximal ideal of K_r is equal to i, which is a unit in $\mathbb{F}_p$. From this one obtains that

$$p\mathcal{O}_{K_r} = (1 - \zeta_{p^r})^{p^{r-1}(p-1)},$$

i.e. that $1 - \zeta_{p^r}$ is a uniformiser of K_r and that $K_r/\mathbb{Q}_p$ is totally ramified. Passing to the relative situation, we have

$$e_{K_r/K_t} = \begin{cases} (p-1)p^{r-1} & \text{if } t = 0, \\ \frac{(p-1)p^{r-1}}{(p-1)p^{t-1}} = p^{r-t} & \text{if } t > 0. \end{cases}$$

We will now compute $G_s(K_r/\mathbb{Q}_p)$, i.e. the ramification groups in lower numbering. Let $\sigma \in G := G(K_r/\mathbb{Q}_p)$. Then σ is uniquely determined by an integer $1 \leq i \leq p^r - 1$, $(i,p) = 1$ such that $\sigma\zeta_{p^r} = \zeta_{p^r}^i =: \sigma_i(\zeta_{p^r})$.

We have

$$\begin{aligned} G_s &= \{\sigma \in G | v(\sigma(1-\zeta_{p^r}) - (1-\zeta_{p^r})) \geq s+1\} \\ &= \{\sigma \in G | v(\sigma(\zeta_{p^r}) - \zeta_{p^r}) \geq s+1\} \\ &= \{\sigma_i \in G | v(\zeta_{p^r}^i - \zeta_{p^r}) \geq s+1\}, \end{aligned}$$

where $v = v_{K_r}$. Let i be given as above and let t be the unique (if $i \neq 1$) positive integer such that $i = 1 + qp^t$ with $(q,p) = 1$. This is equivalent to σ_i being an element of $\mathrm{Gal}(K_r/K_t) - \mathrm{Gal}(K_r/K_{t+1})$, since $\zeta_{p^t}^i = \zeta_{p^t}\zeta_{p^t}^{p^t q} = \zeta_{p^t}$. We compute further:

$$\begin{aligned} v(\zeta_{p^r}^i - \zeta_{p^r}) = v(1-\zeta_{p^r}^{i-1}) = v(1-\zeta_{p^r}^{qp^t}) = v(1-(\zeta_{p^{r-t}}^q)) \\ = e_{K_r/K_{r-t}} = \begin{cases} p^t & \text{if } r-t \geq 1, \\ \infty & \text{if } r = t. \end{cases} \end{aligned}$$

This means the following for $1 \neq i = 1 + qp^t$ with $(q,p) = 1$:

$$\sigma_i \in G_s \Leftrightarrow v(\sigma_i\zeta_{p^r} - \zeta_{p^r}) = p^t \geq s+1.$$

Finally, we obtain

$$G_s = \begin{cases} G(K_r/\mathbb{Q}_p) & \text{if } s = 0 \\ G(K_r/K_1) & \text{if } 0 < s \leq p-1 \\ G(K_r/K_2) & \text{if } p-1 < s \leq p^2-1 \\ \dots & \\ G(K_r/K_t) & \text{if } p^{t-1}-1 < s \leq p^t-1 \\ \dots & \\ 0 & \text{if } p^{r-1}-1 < s. \end{cases}$$

Thus, the jumps for the lower numbering occur at 0, $p-1$, $p(p-1)$, $p^2(p-1)$,$\dots$.

Next we discuss the upper numbering. For that we compute $\eta = \eta_{K_r/\mathbb{Q}_p}(s)$. We have $\eta(0) = 0$ and for $p^{t-1} - 1 < s \leq p^t - 1$ with $t \geq 1$:

$$\begin{aligned} \eta(s) &= \frac{1}{g_0}\big(g_1 + g_2 + \dots + g_{\lfloor s \rfloor} + (s - \lfloor s \rfloor)g_{\lceil s \rceil}\big) \\ &= \frac{1}{(p-1)p^{r-1}}\big((p-1)g_1 + p(p-1)g_p + \dots + p^{t-2}(p-1)g_{p^{t-2}} + (s - p^{t-1} + 1)g_{p^{t-1}}\big) \\ &= (t-1) + (s - p^{t-1} + 1)\frac{p^{r-t}}{(p-1)p^{r-1}} \\ &= (t-1) + \frac{(s+1) - p^{t-1}}{p^t - p^{t-1}}. \end{aligned}$$

We used $g_{p^t} = \#\operatorname{Gal}(K_r/K_{t+1}) = p^{r-t-1}$, whence $g_{p^t}p^t(p-1) = p^{r-1}(p-1)$. One obtains:

$$\begin{aligned}
\eta(s) = 1 &\Leftrightarrow s = p-1 \Leftrightarrow \psi(1) = p-1\\
\eta(s) = 2 &\Leftrightarrow s = p^2-1 \Leftrightarrow \psi(2) = p^2-1\\
\eta(s) = 3 &\Leftrightarrow s = p^3-1 \Leftrightarrow \psi(3) = p^3-1\\
&\dots\\
\eta(s) = r-1 &\Leftrightarrow s = p^{r-1}-1 \Leftrightarrow \psi(r-1) = p^{r-1}-1
\end{aligned}$$

Thus, we see that $G^t = \operatorname{Gal}(K_r/K_t)$. Since the jumps in the lower numbering occur at $p-1$, p^2-1, etc., the jumps for the upper numbering are precisely the natural numbers.

Conductor

Definition 3.1.26 *Let K be a local field (complete with respect to a discrete valuation with perfect residue class field). Let L/K a (possibly infinite) Galois extension. For $t \geq -1$ we define the* ramification groups in upper numbering *as*

$$G^u(L/K) = \varprojlim_{L/L'/K} G^u(L'/K),$$

where the L'/K are finite Galois.

Definition 3.1.27 *Let K be a local field of residue characteristic $p > 0$ and let*

$$\rho : G_K \to \mathrm{GL}(V)$$

be a Galois representation, where V is a finite dimensional F-vector space for a field F of characteristic different from p.

(i) The conductor exponent *$n(\rho)$ is defined as*

$$n(\rho) = \int_{-1}^{\infty} \operatorname{codim}_F(V^{\rho(G^u(L/K))})du.$$

(ii) We will see in Corollary 3.1.41 that $n(\rho)$ always is a non-negative integer. The conductor *$N(\rho)$ is defined as $\mathfrak{p}_K^{n(\rho)}$, with $\mathfrak{p}_K$ the valuation ideal of K.*

(iii) The Swan exponent *$\operatorname{sw}(\rho)$ (also called* wild exponent*) is defined as*

$$\operatorname{sw}(\rho) = \int_{0}^{\infty} \operatorname{codim}_F(V^{\rho(G^u(L/K))})du.$$

(Draw a little graph of $\operatorname{codim}_F(V^{\rho(G^u(L/K))})$.)

Remark 3.1.28 *(i) $n(\rho) = \operatorname{codim}_F V^{\rho(G_0(L/K))} + \operatorname{sw}(\rho)$.*

(ii) If V is irreducible, then $\operatorname{codim}_F V^{\rho(G(L/K))} = \dim_F V$.

One-dimensional representations

It is directly clear that the conductor of a 1-dimensional faithful representation is the u where the first (and only) jump in the upper filtration occurs.

Proposition 3.1.29 *Let K be a local field of residue characteristic p and consider a non-trivial 1-dimensional Galois representation*

$$\rho : G_K \to F^\times .$$

Then $\mathrm{sw}(\rho)$ is the minimal $u \geq 0$ such that $\rho(G^u(\overline{K}/K)) = 1$.

Proof. This is immediate from $\rho(G^u) = 1 \Leftrightarrow V^{\rho(G^u)} = V$ with $V = F$. Here $\rho(G^u) \subseteq F^\times$ acts on $V = F$ by multiplication. □

In order to let the ramification groups in upper numbering occur in a different set-up, we recall the principal result from local class field theory.

Theorem 3.1.30 *Let L/K be a Galois extension of local fields (with finite residue fields). There is a group homomorphism, the* norm residue symbol *or* Artin map $(\ ,L/K)$, *such that*

$$1 \to N_{L/K}L^\times \to K^\times \xrightarrow{(\ ,L/K)} G(L/K)^{\mathrm{ab}} \to 1$$

is an exact sequence of groups. Moreover, the norm residue symbol maps $U_K^{(n)}$ onto $G^n(L^{\mathrm{ab}}/K)$.

We will need the following result.

Theorem 3.1.31 (Hasse-Arf) *Let L/K be a finite abelian extension of local fields. If $G_s \neq G_{s+1}$ for $s \in \mathbb{Z}$, then $\eta_{L/K}(s) \in \mathbb{Z}$. In other words, the jumps in the upper ramification groups occur at integers.*

Proof. For cyclotomic fields we computed this explicitly. The same computation works for totally ramified extensions of other local base fields, using Lubin-Tate theory. The details are beyond the scope of this text. □

Corollary 3.1.32 *Let K be a local field of residue characteristic p and consider a non-trivial 1-dimensional Galois representation*

$$\rho : G_K \to F^\times$$

with finite image.

Then $\mathrm{sw}(\rho)$ is the minimal integer $u \geq 0$ such that $U_K^{(u)} \in \ker\big((\ ,L/K)\big)$, where L is such that $G_L = \ker(\rho)$.

Proof. This follows by combining Hasse-Arf, Proposition 3.1.29 with the principal theorem of local class field theory. □

We also give an infinite version of Hasse-Arf.

Corollary 3.1.33 *Let L/K be a (possibly infinite) abelian extension of a local field K. Then the jumps in the upper ramification groups occur at integers, i.e. if $G^{u-\epsilon}(L/K) \neq G^{u+\epsilon}(L/K)$ for all $\epsilon > 0$, then $u \in \mathbb{Z}$.*

Proof. For L/K finite, the statement follows from Hasse-Arf's theorem, since $u = \eta_{L/K}(s)$ with s a jump in the lower filtration.

Now let L/K be arbitrary and assume that the jump u does not occur at an integer. Then there are u' and u'' such that $s < u' < u < u'' < s + 1$ for one $s \in \mathbb{Z}$. Since for all finite Galois L'/K inside L the jumps occur at integers, we have

$$G^{u'}(L'/K) = G^{u''}(L'/K).$$

Consequently, passing to the projective limit yields $G^{u'}(L/K) = G^{u''}(L/K)$, a contradiction. □

Induced representations

We first recall the definition of induced representations.

Definition 3.1.34 *Let $H \leq G$ be a subgroup and V an $R[H]$-representation, where R is any commutative unitary ring. The* induction from H to G of V *(more correctly, the* coinduction*) is defined as*

$$\mathrm{Ind}_H^G(V) = \mathrm{Hom}_{R[H]}(R[G], V)$$

with the natural left G-action: $(g.f)(h) = f(hg)$ for $g, h \in G$.

Remark 3.1.35 *We have $\left(\mathrm{Ind}_H^G(V)\right)^G \cong V^H$, by sending a function f to its value at 1.*

In terms of Galois representation induction works as follows. Let V be a Galois representation of the field L (local or global field) with coefficients in the field F, i.e. V is an $F[G_L]$-module. Take a subfield K of L; then G_L is a subgroup of G_K. We then put

$$\mathrm{Ind}_L^K(V) = \mathrm{Hom}_{F[G_L]}(F[G_K], V),$$

where the homomorphisms are now supposed to be continuous. Alternatively, we could replace G_L by a finite quotient (if the Galois representation V has finite image).

We now compute the conductor of a local induced representation. For this, we will have to use Hilbert's theorem on differents.

Theorem 3.1.36 (Hilbert) *Let L/K be a finite Galois extension of local fields with finite residue fields. Let $G = G(L/K)$. Then $\mathfrak{D}_{L/K} = \mathfrak{p}_L^d$ with $d = \sum_{i \geq 0}(\#G_i - 1)$, where $\mathfrak{D}_{L/K}$ is the different of L/K.*

Taking $N_{L/K}$ and using $v_K \circ N_{L/K} = f_{L/K} v_L$, this yields

$$v_K(\mathfrak{d}_{L/K}) = f_{L/K} d.$$

Proof. The proof needs some preparations, for which we do not have any time. A proof can be found in [SerreLocalFields] or [Neukirch]. □

Theorem 3.1.37 *Let K be a local field with finite residue field. Let L/K be a finite Galois extension and V an $F[G_L]$-representation, i.e. $\rho : G_L \to \mathrm{GL}(V)$ for some finite dimensional F-vector space V.*

Then

$$n(\mathrm{Ind}_K^L(\rho)) = \dim(V) v_K(\mathfrak{d}_{L/K}) + f_{L/K} n(\rho),$$

where $\mathfrak{d}_{L/K}$ denotes the discriminant of L/K and $f_{L/K}$ is the residue degree.

Proof. The usual proof uses Frobenius reciprocity for characters and to the best of my knowledge must be handled with care when the characteristic of F is non-zero. Hence, I prefer to give a very explicit direct proof which is based on the use of Mackey's formula (see [MFII]). Write G for G_K and H for G_L. Since H and G^u are normal subgroups of G, Mackey's formula considerably simplifies and reads

$$\mathrm{Res}^G_{G^u} \mathrm{Ind}^G_H(V) = \prod_{g \in G/(G^u H)} {}^g\mathrm{Ind}^{G^u}_{G^u \cap H} \mathrm{Res}^H_{G^u \cap H}(V).$$

We will from now on stop writing Res if it is clear from the context. Before computing the G^u-invariants, we discuss the groups involved in the formula. We have

$$G/(G^u H) \cong (G/H)/(G^u H/H) \cong (G/H)/(G/H)^u.$$

Since we prefer not to pass to finite groups, we need a limit process for the next statement.

$$\begin{aligned} G^u \cap H = (\varprojlim_{M/L} G(M/K)^u) \cap H \qquad & = \varprojlim_{M/L} (G(M/K)^u \cap G(M/L)) \\ = \varprojlim_{M/L} (G(M/K)_{\psi_{M/K}(u)} \cap G(M/L)) \qquad & = \varprojlim_{M/L} G(M/L)_{\psi_{M/K}(u)} \\ = \varprojlim_{M/L} G(M/L)^{\eta_{M/L}(\psi_{M/K}(u))} \qquad & = \varprojlim_{M/L} G(M/L)^{\eta_{M/L}(\psi_{M/L}(\psi_{L/K}(u)))} \\ = \varprojlim_{M/L} G(M/L)^{\psi_{L/K}(u)} \qquad & = H^{\psi_{L/K}(u)}, \end{aligned}$$

where M/L runs through all extensions M of L that are Galois over K. This is justified, since the set of such forms a cofinal subset of the set of all Galois extension M/K, and also of the set of all Galois extensions M/L.

From Mackey's formula and Remark 3.1.35, we obtain

$$\left(\mathrm{Ind}_K^L(V)\right)^{G^u} = \prod_{g \in (G/H)/(G/H)^u} V^{H^{\psi_{L/K}(u)}}.$$

Now, it is just a question of computing. First, we have

$$\begin{aligned} \mathrm{codim} \left(\mathrm{Ind}_K^L(V)\right)^{G^u} &= \#(G/H) \dim V - \frac{\#(G/H)}{\#(G/H)^u} \dim V^{H^{\psi_{L/K}(u)}} \\ &= \#(G/H)(\dim V - \frac{1}{\#(G/H)^u} \dim V^{H^{\psi_{L/K}(u)}}). \end{aligned}$$

Recall that $\eta'_{L/K}(s) = \frac{\#(G/H)_s}{\#(G/H)_0}$ and correspondingly $\psi'_{L/K}(u) = \frac{\#(G/H)_0}{\#(G/H)^u}$. Now we use the substitution rule, the above computation and Hilbert's theorem on the different and get

$$\begin{aligned}
n(\rho) &= \int_{-1}^{\infty} \operatorname{codim} V^{H^v} dv \\
&= \int_{-1}^{\infty} \operatorname{codim} V^{H^{\psi_{L/K}(u)}} d\psi_{L/K}(v) \\
&= \#(G/H)_0 \int_{-1}^{\infty} \operatorname{codim} V^{H^{\psi_{L/K}(u)}} \frac{1}{(G/H)^u} du \\
&= \#(G/H)_0 \int_{-1}^{\infty} (\dim V - \dim V^{H^{\psi_{L/K}(u)}}) \frac{1}{(G/H)^u} du \\
&= \#(G/H)_0 \int_{-1}^{\infty} \big(\dim V (\frac{1}{(G/H)^u} - 1) + (\dim V - \dim V^{H^{\psi_{L/K}(u)}} \frac{1}{(G/H)^u})\big) du \\
&= e_{L/K} \dim V \int_{-1}^{\infty} (\frac{1}{(G/H)^u} - 1))du + \frac{1}{f_{L/K}} \int_{-1}^{\infty} \operatorname{codim}(\operatorname{Ind}_K^L(V))^{G^u} du \\
&= \dim(V) \int_{-1}^{\infty} (\frac{1}{(G/H)_v} - 1))\#(G/H)_v dv + \frac{1}{f_{L/K}} n(\operatorname{Ind}_K^L(V)) \\
&= \frac{\dim(V)}{f_{L/K}} v_K(\mathfrak{d}_{L/K}) + \frac{1}{f_{L/K}} n(\operatorname{Ind}_K^L(V)).
\end{aligned}$$

This establishes the theorem. □

Generalities on conductor exponents

Proposition 3.1.38 *Let K be a local field and F an algebraically closed topological field. Let $\rho : G_K \to \mathrm{GL}_n(F)$ be an irreducible Galois representation with finite image. Let L be the smallest extension of K such that $\rho|_{G_L}$ is unramified, i.e. let $G_M = \ker(\rho)$, then $L = M^{G(M/K)_0}$.*

Then $n(\rho) = n(\rho|G_L)$.

Proof. Let $H = G(M/L) = G_0 = G^0$. For $u \in (0, \infty)$ we have

$$G^u = H \cap G^u = H \cap G_{\psi_{M/K}(u)} = H_{\psi_{M/K}(u)} = H^{\eta_{M/L} \circ \psi_{M/L} \circ \psi_{L/K}(u)} = H^{\psi_{L/K}(u)} = H^u,$$

since L/K is unramified. This immediately implies the claim. □

The case of restriction to the maximal tamely ramified extension is treated in Exercise 19.

Proposition 3.1.39 *Let K be a local field and F an algebraically closed topological field. Let $\rho : G_K \to \mathrm{GL}(V)$ be a Galois representation with V an F-vector space.*

Then $n(\rho) = n(\rho^{\mathrm{ss}})$.

Proof. In terms of matrices $\dim V^{G^u}$ is the minimum number of 1's on the diagonal of the Jordan normal form of each $g \in G^u$, which is clearly independent of the semi-simplification. □

Conductor exponents are integers

The following is adapted from a proof in Serre's book on linear representations of finite groups.

Proposition 3.1.40 *Let K be a local field of residue characteristic p and F an algebraically closed topological field. Assume that the characteristic of F is different from p. Let $\rho : G_K \to \mathrm{GL}_n(F)$ be an irreducible Galois representation with finite image.*

Then ρ is of the form $\mathrm{Ind}_{G_L}^{G_K}(W)$ for some finite extension L of K and W a representation of G_L with abelian image of inertia, i.e. W corresponds to a representation $\rho_1 : G_L \to \mathrm{GL}(W)$ and $\rho_1(I_L)$ is an abelian group.

Proof. Let $G = G_K/\ker(\rho)$. Let V be the F-vector space underlying ρ.

We distinguish two possibilities:

(I) $G_1 \subseteq Z(G)$

(II) There is minimal $s \geq 1$ with $G_s \not\subseteq Z(G)$ and $G_{s+1} \subseteq Z(G)$.

In case (I), the exact sequence

$$0 \to G_1 \to G_0 \to G_0/G_1 \to 0$$

has abelian kernel and cokernel and is split, whence G_0 is an abelian group. In that case, we are finished.

Now we assume that we are in case (II). The group G_s is a p-group. Moreover, as above, the sequence

$$0 \to G_{s+1} \to G_s \to G_s/G_{s+1} \to 0$$

is split with abelian kernel and cokernel, implying that G_s is abelian. Now we use that the characteristic of F is different from p. In that case, Maschke's theorem shows that

$$V|_{G_s} = \bigoplus_{i=1}^{r} W_i \text{ with } W_i = V_i^{e_i},$$

i.e. the restriction of V to G_s is the direct product of pairwise non-isomorphic irreducible representations of G_s. As F is algebraically closed, each V_i is 1-dimensional.

The quotient G/G_s acts on the set $\{W_1, \ldots, W_r\} = \{1, \ldots, r\}$ through its action on V, i.e. we transport the G-action on V to an action on the direct sum: For $\sigma \in G$, consider the G_s-module σW_i. It is of the form W_j for some j, since $\sigma V_i = V_j$ due to irreducibility of the V_i and then $e_i = e_j$. It is clear that σW_i only depends on the class of σ modulo G_s. The permutation is transitive, as for each i, the orbit $\sum_{\sigma \in G/G_s} \sigma W_i$ is a sub-G-module of V.

Next we notice that $r > 1$. Otherwise, $V|_{G_s} = W_1$ and the action of G_s would be through scalars which we excluded above.

Let now H be the kernel of the permutation representation on $\{1, \ldots, r\}$. In other words, this means for fixed i

$$\{1, \ldots, r\} = \{\sigma W_i | \sigma \in G/H\}.$$

From this we conclude

$$V = \mathrm{Ind}_H^G(W_1).$$

Now we continue as above, replacing G by H and V by W_1. We have the alternatives (I) or (II). In the first case, $H_1 \subset Z(H)$, whence H_0 is abelian, and we are done. In case (II), we obtain by the same procedure

$$V_1 = \mathrm{Ind}_{H_1}^H(U_1),$$

yielding

$$\rho = \mathrm{Ind}_H^G \mathrm{Ind}_{H_1}^H(U_1) = \mathrm{Ind}_{H_1}^G(U_1).$$

Continuing like this, we will at some point be in case (I). □

Corollary 3.1.41 *Conductor exponents of representations as in Proposition 3.1.40 are integers.*

Proof. By Proposition 3.1.40, we have

$$\rho = \mathrm{Ind}_{G_L}^{G_K}(W)$$

with W corresponding to some representation

$$\rho_1 : G_L \to \mathrm{GL}(W)$$

and abelian image of inertia. Let M be such that $G_M = \ker(\rho_1)$. Put $H = \mathrm{Gal}(M/L)$. We have that H_0 is abelian. By Proposition 3.1.38 we know

$$n(\rho_1) = n(\rho_1|_{H_0}).$$

As H_0 is abelian, the jumps in the $(H_0)^u$ occur only at integers by Hasse-Arf. Consequently, $n(\rho_1)$ is an integer.

The formula for the conductor of an induced representation (Theorem 3.1.37) yields that $n(\rho)$ is also an integer. □

Conductors of ℓ-adic and mod ℓ-representations

Proposition 3.1.42 *The Swan exponent of a ℓ-adic Galois representation is the same as the Swan exponent of the mod ℓ reduction.*

More precisely: Let $F/\mathbb{Q}_\ell$ and $K/\mathbb{Q}_p$ finite extensions with $\ell \neq p$. Let $\rho : G_K \to \mathrm{GL}(V)$ be a Galois representation with V an F-vector space of finite dimension. Let $\overline{\rho}$ (with $\overline{V}$ an $\mathbb{F}$-vector space for $\mathbb{F}$ the residue field of F) be the reduction of ρ mod ℓ.

Then $\mathrm{sw}(\rho) = \mathrm{sw}(\overline{\rho})$ and $n(\rho) = n(\overline{\rho}) + \mathrm{codim}_F V^{\rho(G_0)} - \mathrm{codim}_F \overline{V}^{\overline{\rho}(G_0)}$.

Proof. The second statement is a direct consequence of the first, on which we now concentrate. First note that for all $u > 0$, the group $\rho(G^u)$ is finite, as it is a pro-p group inside $\mathrm{GL}(V)$ with V having the ℓ-adic topology.

Let $T \subset V$ be an integral lattice with $\rho : G_K \to \mathrm{GL}(T)$ (possibly after conjugation). So, T is a free $\mathcal{O}_F$-module such that $T \otimes_{\mathcal{O}_F} F = V$ and $T \otimes_{\mathcal{O}_F} \mathbb{F} = \overline{V}$. Let π be a uniformizer of F. Consider the short exact sequence of $\mathcal{O}_F$-modules:

$$0 \to T \xrightarrow{\cdot\pi} T \to T \otimes_{\mathcal{O}_F} \mathbb{F} \to 0.$$

Its associated long exact sequence in cohomology gives:

$$0 \to T^{\rho(G^u)} \xrightarrow{\cdot\pi} T^{\rho(G^u)} \to \overline{V}^{\rho(G^u)} \to \mathrm{H}^1(\rho(G^u), T) = 0,$$

since the group order is finite and invertible in $\mathcal{O}_F$. This yields:

$$T^{\rho(G^u)} \otimes_{\mathcal{O}_F} \mathbb{F} \cong \overline{V}^{\overline{\rho}(G^u)}.$$

Due to flatness, we have

$$T^{\rho(G^u)} \otimes_{\mathcal{O}_F} F = \mathrm{H}^0(\rho(G^u), T) \otimes_{\mathcal{O}_F} F = \mathrm{H}^0(\rho(G^u), T \otimes_{\mathcal{O}_F} F) = \mathrm{H}^0(\rho(G^u), V) = V^{\rho(G^u)}.$$

Putting these together, we find

$$\dim_F V^{\rho(G^u)} = \mathrm{rk}_{\mathcal{O}_F} T^{\rho(G^u)} = \dim_{\mathbb{F}} \overline{V}^{\overline{\rho}(G^u)},$$

from which the proposition is obvious. □

Corollary 3.1.43 *Conductor exponents of ℓ-adic representations of local fields of residue characteristic $p \neq \ell$ are integers.*

Proof. The Swan conductor of the ℓ-adic representation equals the Swan conductor of the reduction of the representation mod ℓ, which satisfies the requirements of Corollary 3.1.41. □

Globalisation

Definition 3.1.44 *Let K be a global field and $\rho : G_K \to \mathrm{GL}(V)$ be a Galois representation with V a finite dimensional F-vector space. For every finite prime $\mathfrak{p}$ of K fix an embedding $K \hookrightarrow \overline{\mathbb{Q}}_p$, with respect to which we will embed $G_{K_\mathfrak{p}}$ into G_K.*

The (Artin) conductor *of ρ is defined as*

$$N(\rho) = \prod_{\mathfrak{p}, (\mathfrak{p}, \mathrm{char}(F))=1} \mathfrak{p}^{n(\rho|_{G_{K_\mathfrak{p}}})}.$$

(If $\mathrm{char}(F) = 0$, then the product runs through all primes of K.)

In words, the conductor stores information on the ramification of ρ outside the characteristic of F.

3.2 Weil-Deligne representations

We now fix the notation for all this section.

Let K be a finite extension of $\mathbb{Q}_p$. Let G_K be the absolute Galois group of K, which is filtered by $I_K = G_0$, its inertia group, and $P_K = G_1$, the wild inertia group. Denote by $K^{\mathrm{unr}} = \overline{\mathbb{Q}}_p^{I_K}$ the maximal unramified extension of K and by $K^{\mathrm{tr}} = \overline{\mathbb{Q}}_p^{P_K}$ the maximal tamely ramified extension of K, both considered inside some fixed $\overline{\mathbb{Q}}_p$. Moreover, let $K^{\mathrm{tr},\ell}$ be the maximal pro-ℓ-extension of K^{unr} inside K^{tr} for primes $\ell \neq p$. As before, we denote by $\mathcal{O}_K$ the integers of K (for other fields with a similar notation). Let $\mathbb{F}$ be the residue field of $\mathcal{O}_K$. Put $q = \#\mathbb{F} = p^f$.

Whenever we consider an ℓ-adic representation in this section, we will have $p \neq \ell$.

Tamely ramified extensions

We now describe the structure of the Galois group of $K^{\mathrm{tr},\ell}/K$ and also of K^{tr}/K.

By definition of the inertia group we have the exact sequence

$$0 \to I_K \to G_K \to G(\overline{\mathbb{F}}_p/\mathbb{F}) \to 0.$$

The latter group is generated by Frob_q, the *geometric Frobenius*, which is the inverse of the arithmetic Frobenius sending x to x^q (this is unfortunate but standard). This choice gives an isomorphism

$$G(K^{\mathrm{unr}}/K) \cong G(\overline{\mathbb{F}}_p/\mathbb{F}) \cong \widehat{\mathbb{Z}}, \;\; \mathrm{Frob}_q \mapsto 1.$$

Lemma 3.2.1 *Choose a uniformiser $\pi \in \mathcal{O}_K$. Then the field K^{tr} is obtained from K^{unr} by adjoining $\pi^{1/m}$ for all m with $(p, m) = 1$. In particular, the field $K^{\mathrm{tr},\ell}$ is obtained by adjoining to K^{unr} all π^{1/ℓ^n}.*

Proof. Adjoining an m-th root ($p \nmid m$) of any element of $\mathcal{O}_K$ results in a tamely ramified extension (its Galois group is a subgroup of $\mathbb{Z}/m\mathbb{Z}$, as K^{unr} contains the m-th roots of unity). It is a fact that any tamely ramified extension of a local p-adic field can be obtained by adjoining m-th roots for $p \nmid m$. Finally, the m-th roots ($p \nmid m$) of any unit ϵ of $\mathcal{O}_K$ are in K^{unr}, as $x^m - \epsilon$ splits into m different factors over $\overline{\mathbb{F}}_p$, which implies that adjoining $(\epsilon\pi^a)^{1/m}$ to F^{unr} is the same as adjoining $\pi^{a/m}$. □

As $\pi \in K$, we can also consider the field $K_1 := K(\pi^{1/\ell^n} | n \in \mathbb{N})$, so that we have $K^{\mathrm{tr},\ell} = K^{\mathrm{unr}}K_1$. This means that the exact sequence

$$0 \to G(K^{\mathrm{tr},\ell}/K^{\mathrm{unr}}) \to G(K^{\mathrm{tr},\ell}/K) \to G(K^{\mathrm{unr}}/K) \to 0$$

is split, thus obtaining a description of $G(K^{\mathrm{tr},\ell}/K)$ as the semi-direct product

$$G(K^{\mathrm{tr},\ell}/K) = G(K^{\mathrm{tr},\ell}/K^{\mathrm{unr}}) \rtimes G(K^{\mathrm{unr}}/K),$$

for the conjugation action of $G(K^{\mathrm{unr}}/K)$ on $G(K^{\mathrm{tr},\ell}/K^{\mathrm{unr}})$.

Definition 3.2.2 *Let $\ell \neq p$ be a prime. Define*

$$\mathbb{Z}_\ell(1) = \varprojlim_n \mu_{\ell^n}(\overline{\mathbb{Q}}_p).$$

We have that $\mathbb{Z}_\ell(1)$ is a $\mathbb{Z}_\ell$-module via $z.\big((\zeta_{\ell^n})_n\big) = (\zeta_{\ell^n}^z)_n$. In fact, it is a $\mathbb{Z}_\ell$-torsor.

Lemma 3.2.3 *The canonical map*

$$t_\ell : G(K^{\mathrm{tr},\ell}/K^{\mathrm{unr}}) \to \mathbb{Z}_\ell(1), \;\; \sigma \mapsto (\frac{\sigma(\pi^{1/\ell^n})}{\pi^{1/\ell^n}})_n$$

is an isomorphism. □

Let us choose an isomorphism (of profinite groups) $\mathbb{Z}_\ell(1) \cong \mathbb{Z}_\ell$ and compose t_ℓ with it, thus obtaining an isomorphism $r_\ell : G(K^{\mathrm{tr},\ell}/K^{\mathrm{unr}}) \to \mathbb{Z}_\ell$. Let us call u the topological generator in $G(K^{\mathrm{tr},\ell}/K^{\mathrm{unr}})$, which satisfies $r_\ell(u) = 1 \in \mathbb{Z}_\ell$.

We could also have chosen any other topological generator u, but then we would have to “divide” by its image in $\mathbb{Z}_\ell$ later on. That seems more conceptual, but makes the formulae more complicated.

Lemma 3.2.4 *Let $\sigma \in G(K^{\mathrm{tr},\ell}/K^{\mathrm{unr}})$. We have*

$$\sigma \circ \mathrm{Frob}_q = \mathrm{Frob}_q \circ \sigma^q.$$

Proof. Via the split, Frob_q is an element in $G(K^{\mathrm{tr},\ell}/K_1) \subseteq G(K^{\mathrm{tr},\ell}/K)$. So it fixes in particular all π^{1/ℓ^n}. However, on roots of unity that are in the unramified tower it acts as $\zeta_{\ell^n} \mapsto \zeta_{\ell^n}^{1/q}$ (as it does so on the residue field).

Let $n \in \mathbb{N}$. We have:

$$\mathrm{Frob}_q^{-1} \circ \sigma \circ \mathrm{Frob}_q(\pi^{1/\ell^n}) = \mathrm{Frob}_q^{-1}\big(\sigma(\pi^{1/\ell^n})\big) =$$
$$\mathrm{Frob}_q^{-1}\big(\frac{\sigma(\pi^{1/\ell^n})}{\pi^{1/\ell^n}}\pi^{1/\ell^n}\big) = \big(\frac{\sigma(\pi^{1/\ell^n})}{\pi^{1/\ell^n}}\big)^q \pi^{1/\ell^n} = \sigma^q(\pi^{1/\ell^n}).$$

The last equality follows from

$$\sigma^q(\pi^{1/\ell^n}) = \sigma^{q-1}(\frac{\sigma(\pi^{1/\ell^n})}{\pi^{1/\ell^n}}\pi^{1/\ell^n}) = \frac{\sigma(\pi^{1/\ell^n})}{\pi^{1/\ell^n}}\sigma^{q-1}(\pi^{1/\ell^n}) = \cdots = \big(\frac{\sigma(\pi^{1/\ell^n})}{\pi^{1/\ell^n}}\big)^q \pi^{1/\ell^n}.$$

This finishes the proof. □

Summarizing the above, we obtain the following proposition.

Proposition 3.2.5 *There is an isomorphism*

$$G(K^{\mathrm{tr},\ell}/K) \cong \mathbb{Z}_\ell(1) \rtimes \widehat{\mathbb{Z}},$$

where the action of $1 \in \widehat{\mathbb{Z}}$ on $\mathbb{Z}_\ell(1)$ is given by raising to the q-th power. □

Semi-stable ℓ-adic representations

Definition 3.2.6 *A continuous ℓ-adic representation*

$$\rho : G_K \to \mathrm{GL}(V)$$

(with V a finite dimensional F-vector space with $F/\mathbb{Q}_\ell$ and $\ell \neq p$) is called semi-stable, *if the inertia group I_K acts unipotently, i.e. for all $\sigma \in I_K$ there is an integer n such that $(\rho(\sigma) - 1)^n = 0$.*

As any unipotent subgroup of $\mathrm{GL}(V)$, e.g. the upper triangular matrices with ones on the diagonal, is a pro-ℓ group, the representation factors through $G(K^{\mathrm{tr},\ell}/K)$.

Proposition 3.2.7 *Every ℓ-adic representation as above becomes semi-stable after passing to a suitable finite extension K'/K. One says that it is* potentially semi-stable.

Proof. As the wild part of I_K can only have a finite image, we can assume that it acts trivially. The profinite group I_K/P_K is the direct product of the groups $\mathbb{Z}_q(1)$ for q running through the primes different from p. The product of $\mathbb{Z}_q(1)$ for primes $q \neq \ell, p$ has a finite image, so we can also assume that it is trivial.

From the relation $\mathrm{Frob}_q^{-1}\,\sigma\,\mathrm{Frob}_q = \sigma^q$ for $\sigma \in G(K^{\mathrm{tr},\ell}/K^{\mathrm{unr}})$ it follows that $\rho(\sigma)$ and $\rho(\sigma^q)$ have the same eigenvalues. From this it is clear that the eigenvalues of $\rho(\sigma)$ can only be roots of unity. So the unipotent part of $G(K^{\mathrm{tr},\ell}/K^{\mathrm{unr}})$ is open of finite index in it. Passing to a finite extension K'/K we can hence assume that the inertia group acts unipotently. □

Recall that we made two choices above, namely that of a uniformiser $\pi \in \mathcal{O}_K$ and that of an isomorphism $\mathbb{Z}_\ell(1) \cong \mathbb{Z}_\ell$ (i.e. choosing a topological generator of $\mathbb{Z}_\ell(1)$ correpsonding to 1, resp. a topological generator of $G(K^{\mathrm{tr},\ell}/K^{\mathrm{unr}})$). Let us fix these choices for the time being.

Assume that ρ is a semi-stable ℓ-adic representation as above. We have the following data:

- A continuous action of $G(K^{\mathrm{unr}}/K)$ on an ℓ-adic vector space V, coming from ρ via the split. In $G(K^{\mathrm{unr}}/K)$ we have a special element, the geometric Frobenius: $\varphi = \rho(\mathrm{Frob}_q) : V \to V$. It is an isomorphism, describing the action of $G(K^{\mathrm{unr}}/K)$ uniquely.

- A unipotent endomorphism $U = \rho(u) : V \to V$.

  For any unipotent endomorphism one can define its logarithm

  $$\log(U) = -\sum_{n \geq 1} \frac{(1-U)^n}{n}$$

  (the sum is finite). It is a nilpotent endomorphism.

  Let $N = \log(U) : V \to V$. Given ρ, the endomorphism N is uniquely determined (remembering our choices).

  As we have $\varphi^{-1}U\varphi = U^q$, using that $\log(\varphi^{-1}U\varphi) = \varphi^{-1}\log(U)\varphi$, we obtain

  $$N\varphi = q\varphi N.$$

Theorem 3.2.8 *Subject to the choices made above, there is a bijection between the semi-stable ℓ-adic representations $\rho : G_K \to \mathrm{GL}(V)$ and the set of tuples $(\widetilde{\rho}, N)$ with $\widetilde{\rho} : G(K^{\mathrm{unr}}/K) \to \mathrm{GL}(V)$ a continous representation and $N : V \to V$ a nilpotent endomorphism satisfying $N\varphi = q\varphi N$, where φ is $\rho(\mathrm{Frob}_q)$ with Frob_q a geometric Frobenius element.*

Proof. We have seen that the tuple associated above is unique.

Let us construct a representation ρ out of $(\widetilde{\rho}, N)$. It is clear that ρ restricted to the prime-to-ℓ-parts of I_K has to be trivial, and restricted to $G(K^{\mathrm{tr},\ell}/K_1) \cong G(K^{\mathrm{unr}}/K)$ has to be given by $\widetilde{\rho}$.

Recall the continuous isomorphism $r_\ell : G(K^{\mathrm{tr}}/K^{\mathrm{unr}}) \to \mathbb{Z}_\ell$. It involved choices and was made in such a way that $r_\ell(u) = 1$. From it we obtain a continuous homomorphism

$$\rho|_{G(K^{\mathrm{tr}}/K^{\mathrm{unr}})} : G(K^{\mathrm{tr}}/K^{\mathrm{unr}}) \to \mathrm{GL}(V), \quad x \mapsto \exp(r_\ell(x)N),$$

where $\exp$ is defined via the usual power series expansion, which is a finite sum, since N is nilpotent.

The commutativity relation implies that ρ is well-defined. One checks (e.g. on the dense subset $\{u^n\}$) that these constructions are inverses to each other. □

Remark 3.2.9 *More conceptually, one can get rid of the choices by considering N not as a map $V \to V$, but as the map $V \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(1) \to V$ defined by $N(v \otimes 1) = (\frac{1}{t_\ell(g)} \log(\rho(g)))v$, which is independent of the choice of $g \in G(K^{\mathrm{tr},\ell}/K^{\mathrm{unr}})$.*

Remark 3.2.10 *Most of the above fails if $\ell = p$. In particular, the image of the representation will in general not be a semi-direct product.*

Weil-Deligne representations

The idea behind Weil-Deligne representations is to 'forget' the topology, but to retain enough information to uniquely identify a given ℓ-adic representation. We recall that throughout $\ell \neq p$.

Definition 3.2.11 *The* Weil group W_K *of the p-adic local field K is defined as*

$$\{\ \sigma \in G_K \mid \exists n \in \mathbb{Z} : \overline{\sigma} = \mathrm{Frob}_q^n\ \},$$

where we write $\overline{\sigma}$ for the image of σ in $G(\overline{\mathbb{F}}_p/\mathbb{F})$.

In words, the Weil group is the subgroup of G_K (as a group, not as a topological group) of those elements that map to a power of the geometric Frobenius element in the Galois group of the residue extension.

Definition 3.2.12 *Let F be an algebraically closed field of characteristic 0. A pair (ρ, N) consisting of a group homomorphism $\rho : W_K \to \mathrm{GL}(V)$ and nilpotent endomorphism $N : V \to V$, where V is a finite dimensional F-vector space (with the discrete topology), is called a* Weil-Deligne representation of K over F *if for all $g \in W_K$, whose image in $G(\overline{\mathbb{F}}_p/\mathbb{F}) \subseteq G(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ equals $(\mathrm{Frob}_p)^{\alpha(g)}$, one has*

$$N\rho(g) = p^{\alpha(g)}\rho(g)N.$$

(We are again considering Frob_p *to be the geometric Frobenius.)*

A Weil-Deligne representation is called F-semi-simple *(that's a different* F *meaning 'Frobenius') if the underlying representation of* W_K *is semi-simple (in the usual sense).*

Remark 3.2.13 *There is an algebraic group over* F*, called the* Weil-Deligne group, *whose representations are precisely those above. Thus the name.*

Proposition 3.2.14 *Every* ℓ*-adic representation* $\rho : G_K \to \mathrm{GL}(V)$ *gives a unique Weil-Deligne representation of* K *over* $\overline{\mathbb{Q}}_\ell$*, which we denote as* $\mathrm{WD}(\rho)_{\overline{\mathbb{Q}}_\ell}$.

Proof. Let us first extend scalars of V to $\overline{\mathbb{Q}}_\ell$. We know that ρ is potentially semi-stable. Let hence K'/K be a finite Galois extension so that $\rho|_{G_{K'}}$ is semi-stable. Above we have constructed a homomorphism $I_K/P_K \to \mathbb{Z}_\ell$, namely r_ℓ. Now we use $s_\ell : I_K \to I_K/P_K \to \mathbb{Z}_\ell$. We let u be a topological generator of $I_{K'}$. Let furthermore, $N = \frac{-\log(\rho(u))}{s_\ell(u)}$, which is nilpotent and satisfies the necessary commutativity relation (same proof as already presented above).

We now define the Weil-Deligne representation $\mathrm{WD}(\rho)_{\overline{\mathbb{Q}}_\ell}$ to be associated with ρ as follows. First choose some Φ lifting the geometric Frobenius, so that every element in the Weil group W_K can be written as $\Phi^n\sigma$ with $\sigma \in I_K$. We let

$$\mathrm{WD}(\rho)_{\overline{\mathbb{Q}}_\ell}(\Phi^n\sigma) = \rho(\Phi^n\sigma)\exp(s_\ell(\sigma)N).$$

Then for example one has $\mathrm{WD}(u^n) = \rho(u^n)\exp(-s_\ell(u^n)/s_\ell(u)\log(\rho(u))) = 1$, so $I_{K'}$ acts trivially. Hence, only the Frobenius action and the action of $I_K/I_{K'}$ is remembered by $\mathrm{WD}(\rho)_{\overline{\mathbb{Q}}_\ell}$ and the action of $I_{K'}$ is 'put' into N.

We remark without proof that the associated Weil-Deligne representation up to isomorphism is independent of the choices made (i.e. of Φ and of the identification $\mathbb{Z}_\ell(1) \cong \mathbb{Z}_\ell$ used in the homomorphsim s_ℓ). □

Remark 3.2.15 *For the sake of completeness we mention that one can equip* W_K *with a topology. For this, we consider the exact sequence*

$$0 \to I_K \to G_K \xrightarrow{\mathrm{pr}} \widehat{\mathbb{Z}} \to 0,$$

and the exact sequence (of subgroups of the former)

$$0 \to I_K \to W_K \xrightarrow{\mathrm{pr}} \mathbb{Z} \to 0.$$

On $\mathbb{Z}$ *we put the discrete topology, so that* $\mathbb{Z}$ *is dense in* $\widehat{\mathbb{Z}}$*. We consider* W_K *as* $\mathrm{pr}^{-1}(\mathbb{Z}) \subset G_K$ *with the subspace topology. Then the Weil group* W_K *is dense in* G_K *and* I_K *carries its original topology.*

The main reason for putting the mentioned topology on W_K *is that one then has a natural bijection between the set of continuous representations* $W_K \to \mathrm{GL}_d(\mathbb{Q}_\ell)$ *with the discrete topology on* $\mathbb{Q}_\ell$ *together with a nilpotent operator* N *subject to the commutativity rule above and the set of continuous* ℓ*-adic representations* $W_K \to \mathrm{GL}_d(\mathbb{Q}_\ell)$*. In the latter set one has the proper subset obtained from the* ℓ*-adic representations* $G_K \to \mathrm{GL}_d(\mathbb{Q}_\ell)$ *by restricting to* W_K.

3.3 Serre's conjecture

Whereas in the previous section the case $\ell \neq p$ was treated, we now have to move to $\ell = p$. This is much more difficult and, in general, requires Fontaine's theory. We shall, however, only treat the so-called fundamental characters. These suffice for a formulation of the weight in Serre's conjecture.

Fundamental characters

Let $K/\mathbb{Q}_p$ be a finite extension with residue field $\mathbb{F}_q$. By the discussion in the previous section, we have an explicit isomorphism

$$t : G(K^{\mathrm{tr}}/K^{\mathrm{unr}}) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell(1) \cong \varprojlim_{m,(m,p)=1} \mu_m(\overline{\mathbb{Q}}_p) \cong \varprojlim_{m,(m,p)=1} \mu_m(\overline{\mathbb{F}}_p) \cong \varprojlim_{n} (\mathbb{F}_{p^n}^\times).$$

Moreover, conjugation by Frob_q on $G(K^{\mathrm{tr}}/K^{\mathrm{unr}})$ translates to raising to the q-th power.

Definition 3.3.1 *A character*

$$\phi : G(K^{\mathrm{tr}}/K^{\mathrm{unr}}) \to \overline{\mathbb{F}}_p^\times$$

is said to be of level n *if* $n \geq 1$ *is the minimal* m *such that* ϕ *factors through* $\mathbb{F}_{p^m}^\times$*, i.e.*

$$\phi : G(K^{\mathrm{tr}}/K^{\mathrm{unr}}) \xrightarrow{\text{projection} \circ t} \mathbb{F}_{p^m}^\times \hookrightarrow \overline{\mathbb{F}}_p^\times.$$

The projection is the natural one on $\varprojlim_n (\mathbb{F}_{p^n}^\times)$*. (A character is of level* n *if its order divides* $p^n - 1$ *and not* $p^m - 1$ *for any smaller* m*.)*

The fundamental characters (for K) of level n *are the* n *characters*

$$I_t = G(K^{\mathrm{tr}}/K^{\mathrm{unr}}) \xrightarrow{t} \varprojlim_{r} (\mathbb{F}_{p^r}^\times) \twoheadrightarrow \mathbb{F}_{p^n}^\times \xrightarrow{\tau_i} \overline{\mathbb{F}}_p^\times,$$

where $\tau_1, \ldots, \tau_n$ *are the* n *embeddings of* $\mathbb{F}_{p^n}$ *into* $\overline{\mathbb{F}}_p$*.*

Remark 3.3.2 *The fundamental characters of level* n *are* $\{\psi, \psi^p, \psi^{p^2}, \ldots, \psi^{p^{n-1}}\}$ *for some fixed fundamental character* ψ*, since the embeddings* τ_i *are given by the* p*-power Frobenius.*

Every character of I_t *of level at most* n *is the* i*-th power of* ψ *for a unique* $0 \leq i < p^n - 1$*, since the definition of* ϕ *only differs from* ψ *by the fact that* $\mathbb{F}_{p^n}^\times \hookrightarrow \overline{\mathbb{F}}_p^\times$ *need not come from a field embedding but is allowed to be any group homomorphism. As* $\mathbb{F}_{p^n}^\times$ *is cyclic, it is uniquely determined by the image of a generator, which has order* $p^n - 1$*.*

Note that by Exercise 20, the level 1 fundamental character for $K = \mathbb{Q}_p$ is the cyclotomic character.

The weight in Serre's conjecture

We now adopt the situation of Serre's conjecture, i.e. 2-dimensional mod p representations of $G_{\mathbb{Q}}$. The weight reflects the ramification of the representation at p. Hence, in this section we consider Galois representations

$$\rho_p : G_p \to \mathrm{GL}(V)$$

with a 2-dimensional $\overline{\mathbb{F}}_p$-vector space V, where we write G_p for $G_{\mathbb{Q}_p}$. By V^{ss} we denote the semi-simplification of ρ_p, i.e. of V seen as a representation of G_p.

Lemma 3.3.3 *The image of ρ_p is of the form $\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\}$ or $\{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)\}$ (after conjugation).*

Proof. We have seen above that local Galois groups are solvable. The only finite solvable subgroups of $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ are of the claimed form. This follows from Dickson's classification of the subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$. □

Corollary 3.3.4 *On V^{ss}, the wild inertia group P_p acts trivially.*

Furthermore, the tame inertia group, i.e. the quotient $I_t = I_p/P_p = G(\mathbb{Q}_p^{\mathrm{tr}}/\mathbb{Q}_p^{\mathrm{unr}})$ acts on V^{ss} through two characters ϕ_1, ϕ_2, i.e.

$$\rho_p|_{I_t} : I_t \to \mathrm{GL}(V^{\mathrm{ss}})$$

is given as $\rho_p(\sigma) = \begin{pmatrix} \phi_1(\sigma) & 0 \\ 0 & \phi_2(\sigma) \end{pmatrix}$ (after conjugation).

Proof. The first statement immediately follows from Lemma 3.3.3, since in $\{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)\}$ there is no non-trivial element of p-power order.

For the second statement note that I_t is a profinite group of order coprime to p, meaning that no finite quotient has order divisible by p. Hence, by Maschke's theorem, its representation theory over $\overline{\mathbb{F}}_p$ is semi-simple. As I_t is furthermore abelian, the action of I_t is diagonalisable, i.e. given by two characters, as claimed. □

Proposition 3.3.5 *The characters ϕ_1, ϕ_2 are either both of level 1 or of level 2. In the latter case, $\phi_1 = \phi_2^p$, $\phi_2 = \phi_1^p$ and V is an irreducible G_p-representation.*

Proof. Above we have seen that conjugation by Frob_p on $I_t = G(\mathbb{Q}_p^{\mathrm{tr}}/\mathbb{Q}_p^{\mathrm{unr}})$ means raising to the p-th power. Thus, there is a matrix such that conjugating $\begin{pmatrix} \phi_1(\sigma) & 0 \\ 0 & \phi_2(\sigma) \end{pmatrix}$ by it equals raising to the p-th power. If a conjugate of a diagonal matrix is still diagonal, then only the diagonal entries can have been permuted (e.g. look at the Jordan form). Consequently, the set $\{\phi_1, \phi_2\}$ is stable under taking p-th powers. If $\phi_1^p = \phi_1$, then ϕ_1 is of level 1. Then also ϕ_2 is of level 1.

If $\phi_1^p = \phi_2$, then V is irreducible. For, if it were not, then there would be a G_p-invariant 1-dimensional subspace on which G_p acts through a character. Hence, ϕ_1 and ϕ_2 would be of level 1. □

Definition 3.3.6 *Let $K/\mathbb{Q}_p$ be a finite Galois extension and denote by K^{tr} and K^{unr} the maximal tamely ramified, respectively unramified subextensions of K. Assume that $G(K^{\mathrm{tr}}/K^{\mathrm{unr}}) = (\mathbb{Z}/p\mathbb{Z})^\times$ and that $G(K/K^{\mathrm{tr}})$ is an elementary abelian group of exponent p (i.e. $(\mathbb{Z}/p\mathbb{Z})^m$). Then $K^{\mathrm{tr}} = K^{\mathrm{unr}}(\zeta_p)$ and by Kummer theory there are $x_1, \dots, x_m \in K^{\mathrm{unr}}$ such that $K = K^{\mathrm{tr}}(x_1^{1/p}, \dots, x_m^{1/p})$.*

Then K is called little ramified *if all the x_i can be chosen among the units of K^{unr}. Otherwise, K is called* very ramified.

Now we are ready to define the weight in Serre's conjecture. We point out that what we present here is the *minimal weight* discussed by Edixhoven, i.e. the weight that one should use when formulating Serre's conjecture with Katz modular forms over $\overline{\mathbb{F}}_p$ rather than reductions of holomorphic modular forms.

Definition 3.3.7 *Denote by ψ, ψ^p the two fundamental characters of level 2 and by χ the cyclotomic character.*

Let $\rho_p : G_p \to \mathrm{GL}(V)$ be a Galois representation with V a 2-dimensional $\overline{\mathbb{F}}_p$-vector space. Define ϕ_1, ϕ_2 as above. The minimal weight *$k(\rho_p)$ of ρ_p is defined as follows.*

(I) Suppose ϕ_1, ϕ_2 are of level 2. After interchanging ϕ_1 and ϕ_2 there are unique integers $0 \le a < b \le p-1$ such that

$$\phi_1 = \psi^{a+pb} \text{ and } \phi_2 = \psi^{b+ap}.$$

Let

$$k(\rho_p) = 1 + pa + b.$$

(II) Suppose ϕ_1, ϕ_2 are of level 1.

(1) Suppose that ρ_p is tamely ramified, i.e. $\rho_p(P_p) = 0$. There are unique integers $0 \le a \le b \le p-2$ such that $\phi_1 = \chi^a$ and $\phi_2 = \chi^b$. Let

$$k(\rho_p) = 1 + pa + b.$$

(2) Suppose that ρ_p is not tamely ramified. Then there are unique integers $0 \le \alpha \le p-2$ and $1 \le \beta \le p-1$ such that

$$\rho_p|_{I_p} \cong \begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix}.$$

Let $a = \min(\alpha, \beta)$ and $b = \max(\alpha, \beta)$.

(a) Suppose $\beta \neq \alpha + 1$. Let

$$k(\rho_p) = 1 + pa + b.$$

(b) Suppose $\beta = \alpha + 1$. Let K be the extension of $\mathbb{Q}_p$ such that $G_K = \ker(\rho_p)$.

(i) Suppose K is little ramified. Let

$$k(\rho_p) = 1 + pa + b.$$

(ii) Suppose K is very ramified. Let

$$k(\rho_p) = 1 + pa + b + (p-1).$$

Serre's conjecture

We finish this course by giving the full statement of Serre's conjecture.

Theorem 3.3.8 (Serre's conjecture: Khare, Wintenberger, Kisin, Taylor, et al.) *Given any irreducible odd Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$. There is a (Katz) modular form on $\Gamma_1(N(\rho))$ of weight $k(\rho|_{G_{\mathbb{Q}_p}})$ such that its attached mod p Galois representation is isomorphic to ρ.*

Exercises

Exercise 1 *Prove Proposition 1.1.5.*

Exercise 2 *Prove Proposition 1.1.6.*

Exercise 3 *Prove Proposition 1.3.1.*

Exercise 4 *Let ϕ be an endomorphism of a finite dimensional k-vector space. Show that there is the identity of formal power series*

$$\exp\big(\sum_{r=1}^{\infty}\mathrm{Tr}(\phi^r)\frac{X^r}{r}\big)=\frac{1}{\det(1-\phi X)}.$$

Exercise 5 *Prove the statements made in Example 1.4.2 (3).*

Exercise 6 *Let V be an A-module for a k-algebra A. Assume that V is finite dimensional as a k-vector space. Let B be the image of the natural map $A \to \mathrm{End}_k(V)$. Show that V is a faithful B-module and that*

$$\mathrm{End}_A(V)\cong\mathrm{End}_B(V).$$

We will use this exercise to assume in questions about $\mathrm{End}_A(V)$ that V is a faithful A-module.

Exercise 7 *Prove Proposition 2.1.11. You may use the fact that by Zorn's lemma R contains maximal left ideals.*

Exercise 8 *Prove Proposition 2.1.13.*

Exercise 9 *Prove Lemma 2.1.18*

Exercise 10 *Prove Lemma 2.1.22.*

Exercise 11 *Prove Lemma 2.1.25. For (b) use transposed matrices.*

Exercise 12 *Find a counterexample to the statement in Proposition 2.2.3, dropping the separability assumption.*

Exercise 13 *Let R be a k-algebra and K/k a field extension. Prove*

$$\mathrm{Mat}_n(R) \otimes_k K \cong \mathrm{Mat}_n(R \otimes_k K).$$

Exercise 14 *Let $\mathbb{H}$ be the Hamiltonian quaternion algebra over $k = \mathbb{R}$ and let V be its simple module. Let $K = \mathbb{C}$. Write down an explicit embedding of $\mathbb{H}$ into $\mathrm{Mat}_2(\mathbb{C})$ and compute e in Corollary 2.2.12.*

Exercise 15 *(a) $Z_R(R) = Z(R)$.*

(b) $Z_R(T)$ is a subring of R.

(c) $T \subseteq Z_R(T)$ if and only if T is commutative.

(d) $T = Z_R(T)$ if and only if T is a maximal commutative subring.

Exercise 16 *Prove Proposition 2.3.2.*

Exercise 17 *Let k be a finite field $\mathbb{F}_q$. Exhibit an example of a 2-dimensional irreducible group representation over k which is not absolutely irreducible.*

Exercise 18 *Prove Part (iv) of Remark 2.4.7.*

Exercise 19 *Let K be a local field and F an algebraically closed topological field. Let $\rho : G_K \to \mathrm{GL}_n(F)$ be an irreducible Galois representation with finite image. Let L be the smallest extension of K such that $\rho|_{G_L}$ is tamely ramified, i.e. let $G_M = \ker(\rho)$, then $L = M^{G(M/K)_1}$.*

Then $n(\rho) = q \cdot n(\rho|G_L)$ with q the number of elements of G_0/G_1.

Exercise 20 *Let $K = \mathbb{Q}_p$. The level 1 fundamental character is the cyclotomic character.*

Bibliography

[Bourbaki] Algèbre, Ch. VIII

[CurtisReiner] Curtis, Reiner. *Representation theory of finite groups and associative algebras.* Wiley Classics, 1988.

[Gouvea] Gouvea. *Deformations of Galois Representations.*

[Karpilovsky] Karpilovsky. *Group Representations Volume 1, Part A: Background Material*. North Holland.

[Lang] Lang. *Algebra*, Third Edition, Addison Wesley.

[Neukirch] Neukirch. *Algebraische Zahlentheorie*, Springer.

[RibetStein] Ribet, Stein. *Lectures on Serre's conjectures.*

[SerreAbelian] Serre. *Abelian l-adic representations and elliptic curves.*

[SerreLocalFields] Serre. *Corps locaux.* Hermann.

[DDT] H. Darmon, F. Diamond, R. Taylor. *Fermat's Last Theorem*.

[Diamond-Im] F. Diamond and J. Im. *Modular forms and modular curves*, in *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*, 39–133, Amer. Math. Soc., Providence, RI, 1995.

[Hartshorne] R. Hartshorne. *Algebraic geometry*, Springer, New York, 1977.

[Kersten] I. Kersten. *Brauergruppen von Körpern*, Aspekte der Mathematik, Vieweg, Braunschweig, 1990.

[Serre] J.-P. Serre. *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Duke Mathematical Journal **54**, No. 1 (1987), 179–230.

[Silv] Silverman, Joseph H. *The arithmetic of elliptic curves.* Graduate Text in Mathematics, 106. Springer-Verlag, 1992.

[MF] Wiese, G. *Vorlesung über Modulformen.* Lecture notes, Universität Duisburg-Essen, Sommersemester 2007, http://maths.pratum.net

[MFII] Wiese, G. *Computational Arithmetic of Modular Forms.* Lecture notes, Universität Duisburg-Essen, Wintersemester 2007/2008, http://maths.pratum.net