Euler Characteristics of Profinite Groups [1]

January 26, 2002

Gabor Wiese

[1] This is a slightly modified version of my essay, which I wrote in spring 2000 for the Part III examination under the direction of Prof Coates at the University of Cambridge (UK). If you have comments, please mail to me at: gabor@maths.univ-rennes1.fr

Contents

1. Introduction

This essay contains an introduction to the Euler-Poincaré characteristic for the cohomology of profinite groups with coefficients in discrete modules, as well as $\mathbb{Z}_p$-modules and $\mathbb{Q}_p$-vector spaces. It also gives a treatment of the first six chapters of the recent paper by Serre *La distribution d'Euler-Poincaré d'un groupe profini* ([9]), in which a distribution is developed that describes the Euler-Poincaré characteristic. Along the way, some representation theory of finite and profinite groups is dealt with.

Although the choice of topics treated was influenced by what is needed to prove the main theorems from [9], other interesting results have been included.

The main goal of this essay is to develop in detail all the theory concerned, which goes beyond what is generally taught in basic courses on algebra, topology, groups, (co-)homological algebra and categories. Due to space and time limitations, this is not possible when giving full and detailed proofs. However, every result cited, which is necessary for the main theorems proved in chapters 3 to 5, could be proved at the stage, where it is mentioned, without referring to "deeper" theorems. In the chapters on the preliminaries (chapter 2) and the applications (chapter 6) most results are only stated, but references are given.

Next I would like to give a brief outline of the essay. In chapter 2 basic results about profinite groups and the representation theory of finite groups are listed.

Chapter 3 aims at proving that every Euler-Poincaré map (i. e. a map from the objects of a category of G-modules to a ring having the same additivity property as the Euler-Poincaré characteristic) can be uniquely described by a distribution satisfying certain conditions (theorem 3.5.10). This is a purely representation theoretic result, in which Brauer characters play the central role. The main references are [9], [1] and [11].

The first six sections of chapter 4 contain an introduction to the cohomology of profinite groups with coefficients in discrete G-modules, for which the main references are [16], [7], [8] and [13]. A slight emphasis is put on the cohomological dimension. In section 4.7 the Euler-Poincaré characteristic is introduced and a theorem (4.7.5) is derived, which states that the Euler-Poincaré characteristic can be described by a unique distribution.

Chapter 5 contains results about the cohomology of profinite groups with coefficients in finitely generated $\mathbb{Z}_p$-modules and finite dimensional $\mathbb{Q}_p$-vector spaces. In corollary 5.3.4 the Euler-Poincaré characteristic is described by a distribution. The main theorem (5.4.2) gives an explicit formula for calculating this distribution based on certain characters. The main reference for this is Serre's paper [9].

In the final chapter two results by Tate about the Euler-Poincaré characteristic of Galois groups of p-adic fields and number fields are stated in terms of distributions, without giving proofs. References for this are [9], [8] and Tate's papers [14] and [15].

2. Preliminaries

2.1. Profinite groups

In this section we list some facts about profinite groups. Proofs can be found in [7], [16], [6].

2.1.1 Theorem. *Let G be a topological group. Then the following are equivalent:*

(i) G is compact, Hausdorff and totally disconnected.

(ii) G is compact, Hausdorff and the unit 1_G has a basis of open neighbourhoods consisting of normal subgroups.

(iii) G is the projective limit of a projective system of finite groups.

2.1.2 Definition. *If one of the conditions in the theorem holds, then G is called a* **profinite group**.

If a profinite group G is the projective limit of a projective system of p-groups (cyclic groups), then G is called a **pro-p (pro-cyclic) group**.

For a profinite group G, let $\mathcal{U}_G$ denote the set of all open normal subgroups of G.

2.1.3 Proposition. *Let G be a profinite group. Then $(G : U) < \infty$ for all $U \in \mathcal{U}_G$ and $G = \varprojlim G/U$, where the projective system is formed by the projections $G/V \to G/U$ for $V \leq U$ $(U, V \in \mathcal{U}_G)$.*

2.1.4 Example.

- $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, *the integral p-adic numbers, is a pro-cyclic group. The projective system is formed by the natural projections $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ with $n \geq m \in \mathbb{N}$.*
- *The* **Prüfer group** $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$ *is a pro-cyclic group. The projective system is formed by the projections $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ for $m|n$.*
  We have $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.
- *Let L/k be a Galois extension of fields. Then $G(L/k) = \varprojlim G(K/k)$, where K runs over all finite Galois extensions K/k.*
- *A closed subgroup $H \leq G$ of a profinite group G is profinite. In fact, $H = \varprojlim HU/U = \varprojlim H/H \cap U$, where U runs over $\mathcal{U}_G$.*
- *A quotient of a profinite group G by a closed normal subgroup H is a profinite group. In fact, $G/H = \varprojlim G/HU$.*
- *Direct products of profinite groups are profinite.*
- *The projective limit of a projective system of profinite groups is a profinite group.*

A further example is that of the general linear group $\Gamma = GL_d(\mathbb{Z}_p)$ $(d \in \mathbb{N})$. We follow [2] and introduce the congruence subgroups

$$\Gamma_i := \{\gamma \in \Gamma \mid \gamma \equiv id \ (mod\ p^i)\ \},$$

which are normal and for which one can show

$$\Gamma/\Gamma_i \cong GL_d(\mathbb{Z}/p^i\mathbb{Z}).$$

These form a projective system of finite groups with limit Γ, whence Γ is profinite.

In fact, we can say more. A combinatorial argument shows that $(\Gamma_1 : \Gamma_i) = p^{d^2(i-1)}$. Thus Γ_1 is a pro-p group, which implies that Γ is virtually a pro-p group. (A profinite group is said to have a property virtually, if an open normal subgroup has it.)

We now introduce the concept of supernatural numbers, which allows us to define orders and indices of profinite groups.

2.1.5 Definition. *A* **supernatural number** *is a formal product $\prod_p p^{n(p)}$, where p runs over all primes and $n(p) \in \mathbb{N} \cup \{\infty\}$.*

The product of two supernatural numbers, their greatest common divisor (gcd) and their lowest common multiple (lcm) are defined in the obvious way.

We now apply this definition to profinite groups.

2.1.6 Definition. *Let G be a profinite group. Define the* **order** *of G by*

$$\#G = |G| = lcm\{\ |G/U| \mid U \in \mathcal{U}_G\ \}.$$

Let H be a closed subgroup of G. The **index** *of H in G is defined by*

$$(G : H) = lcm\{\ (G/U : HU/U) \mid U \in \mathcal{U}_G\ \} = lcm\{\ (G : HU) \mid U \in \mathcal{U}_G\ \}.$$

For a finite group these definition conincide with the usual ones.

2.1.7 Proposition. *Let $K \leq H \leq G$ be profinite groups. Then $(G : K) = (G : H)(H : K)$. Further, $(G : H)$ is finite if and only if H is open in G.*

2.1.8 Example.

- $|\mathbb{Z}_p| = p^\infty$
- $|\hat{\mathbb{Z}}| = \prod_p p^\infty$

2.1.9 Definition. *Let G be a profinite group and p a prime. A closed subgroup $H \leq G$ is called a* **p-Sylow subgroup**, *if H is a pro-p group and $p \not| (G : H)$.*

2.1.10 Theorem. (Sylow theorems) *Let G be a profinite group. Then*

(i) For every prime p there exists a p-Sylow subgroup of G.

(ii) Any two p-Sylow subgroups are conjugate.

(iii) Every pro-p subgroup is contained in a p-Sylow subgroup of G.

(iv) If $h : G_1 \to G_2$ is a continuous surjective homomorphism of profinite groups, then the image of a p-Sylow group is a p-Sylow group.

(v) $|G| = \prod_p |G_p|$, where G_p is any p-Sylow subgroup of G.

2.1.11 Proposition. (Classification of pro-cyclic groups) *(i) For every supernatural number $n = \prod_p p^{n(p)}$ there exists a pro-cyclic group of order n, which is unique up to isomorphism.*

(ii) For each supernatural number $n = \prod_p p^{n(p)}$ there exists a unique closed subgroup H of $\hat{\mathbb{Z}}$ of index n. Moreover, $H \cong \prod_{p \in M} \mathbb{Z}_p$, where $M = \{p \mid n(p) < \infty\}$.

(iii) Every pro-cyclic group is uniquely obtained as a quotient of $\hat{\mathbb{Z}}$.

We will often make use of the follwing proposition.

2.1.12 Proposition. *Let G be a profinite group, X any topological space and $f : G \to X$ a locally constant map. Then there is $U \in \mathcal{U}_G$, such that for all $g \in G$, f restricted to gU is constant. We will call such f* **locally constant modulo U**.

Proof. For each $g \in G$ we can find $U_g \in \mathcal{U}_G$ such that f is constant on gU_g. Since G is compact, we can choose a finite subset $g_1, \ldots, g_n$ with $G = \cup_{i=1}^{n} g_i U_{g_i}$. Now the fact that $\mathcal{U}_G$ forms a base of neighbourhoods of 1 allows us to find $U \in \mathcal{U}_G$ contained in all U_{g_i}. Let $g \in g_i U_{g_i}$, say $g = g_i u_i$ ($u_i \in U_{g_i}$). Hence $gU = g_i u_i U \subseteq g_i u_i U_{g_i} = g_i U_{g_i}$. As f is constant on each $g_i U_{g_i}$, it is constant on gU for $g \in G$. □

2.2. Some representation theory

In this section we will first introduce some notation for use throughout the essay, and then list two important results from the representation theory of finite groups.

Let k be any field.

2.2.1 Definition. *Let G be any group. A function*

$$c : G \to k$$

is called a **class function** *on G over k, if $c(g^{-1}hg) = c(h)$ for all $g, h \in G$.*

2.2.2 Definition. *For a topological group G we let*

- *$\mathcal{C}_{k,G}$ be the category of finite dimensional k-vector spaces, endowed with the discrete topology, on which G acts continuously. We often refer to its objects as G-modules.*
- *$\Sigma_{k,G}$ be a set of representatives of the simple objects in $\mathcal{C}_{k,G}$.*

If G is a finite group, the topology on the G-modules, of course, does not play any role. We shall then also call elements in $\mathcal{C}_{k,G}$ $k[G]$-modules.

2.2.3 Theorem. *Let k be any field and G a finite group.*

(i) The irreducible characters χ_E for $E \in \mathcal{C}_{k,G}$ are linearly independent over k.

(ii) Let $exp(G) = m$. If $char(k) = 0$ and k contains all m-th roots of 1, then the irreducible characters of G form a k-basis of the space of class functions on G.

Proof. For (1) see e. g. [1], theorem 17.3, and for (2) e. g. [1] chapter 9C. □

3. Euler-Poincaré distributions for discrete modules

3.1. Representations of profinite groups

In this section we introduce the concept of an Euler-Poincaré map in quite a general way. It is in that generality, however, that we will find a distribution describing it.

Let k be any field and consider a profinite group G. The action map

$$\rho : G \to End(A)$$

for $A \in \mathcal{C}_{k,G}$ is continuous and, as A is discrete, locally constant, say modulo U for $U \in \mathcal{U}_G$ (by proposition 2.1.12). Hence ρ factors through G/U and we obtain an action map

$$\rho_U : G/U \to End(A),$$

which makes A into a G/U-module A_U. We note that the order of every $\rho(g)$ in $End(A)$ is finite. Let now in addition A be simple. Suppose A_U is not simple, say $B_U \leq A_U$ ($B_U \in \mathcal{C}_{k,G/U}$). B_U becomes a G-module under the natural projection $G \to G/U$, contradicting the fact that A is simple. This establishes the first half of the next

3.1.1 Proposition. *(i) For all $A \in \Sigma_{k,G}$ there exists $U \in \mathcal{U}_G$ such that $A \in \Sigma_{k,G/U}$.*

(ii) For all $U \in \mathcal{U}_G$ the projection $G \to G/U$ gives us an injection

$$\Sigma_{k,G/U} \hookrightarrow \Sigma_{k,G}.$$

Proof. We regard $A \in \Sigma_{k,G/U}$ as a G-module via the projection. Any G-submodule of A then is automatically also a G/U - module because the action on it is inherited from A. This proves the second part. □

We now introduce the concept of Grothendieck groups.

3.1.2 Definition. *Let $\mathcal{C}$ be a category of (left) A-modules for a k-algebra A. The* **Grothendieck group** *of $\mathcal{C}$, denoted $\mathcal{G}(\mathcal{C})$, is the free abelian group with the simple objects of $\mathcal{C}$ (written $[E]$) as generators.*

Because of the uniqueness of composition series of A-modules by the Jordan-Hölder theorem, this is equivalent to defining the Grothendieck group to be the abelian group with the objects of $\mathcal{C}$ as generators, subject to the relations

$$0 \to E' \to E \to E'' \to 0 \Rightarrow [E] = [E'] + [E''],$$

where the left hand side is any exact sequence of objects in $\mathcal{C}$. By splitting exact sequences we get the following

3.1.3 Remark. *Let $E_1, \ldots, E_n \in \mathcal{C}$ such that*

$$0 \to E_1 \to E_2 \to \cdots \to E_n \to 0$$

is an exact sequence. Then $\sum_{i=1}^{n} (-1)^i [E_i] = 0$.

We are now in the position to define the objects we are interested in.

3.1.4 Definition. *Let K be any field of characteristic 0, not necessarily the same as k. Following Lang ([4], III, §8) we call a homomorphism of abelian groups*

$$c : \mathcal{G}(\mathcal{C}) \to (K, +),$$

where $(K,+)$ denotes the additive group of K, an **Euler-Poincaré map**.

To express this less technically, an Euler-Poincaré map c is any map from the objects of $\mathcal{C}$ to K, which is additive with respect to exact sequences in the following way

$$0 \to E' \to E \to E'' \to 0 \Rightarrow c(E) = c(E') + c(E'').$$

We will, of course, later see that the Euler-Poincaré characteristic of a profinite group is indeed an Euler-Poincaré map.

Returning to profinite groups we can rewrite the second part of the last proposition in terms of Grothendieck groups. To simplify notation we write $\mathcal{G}(G)$ for $\mathcal{G}(\mathcal{C}_{k,G})$ and $\mathcal{G}(G/U)$ for $\mathcal{G}(\mathcal{C}_{k,G/U})$. The next corollary is a reformulation of the second part of the last proposition.

3.1.5 Corollary. *For every $U \in \mathcal{U}_G$ there is a natural injection*

$$\iota_U : \mathcal{G}(G/U) \hookrightarrow \mathcal{G}(G).$$

We will denote the set of all Euler-Poincaré maps of the category $\mathcal{C}_{k,G}$ by $\mathcal{EP}_K(\mathcal{C}_{k,G})$, or just $\mathcal{EP}(G)$. For these we state a characterization.

3.1.6 Proposition. *An Euler-Poincaré map $c \in \mathcal{EP}(G)$ is uniquely determined by a collection $(c_U)_{U \in \mathcal{U}_G}$, where $c_U \in \mathcal{EP}(G/U)$ such that for all $U \in \mathcal{U}_G$ with $V \leq U$ we have $c_V \circ \iota_{U,V} = c_U$. Here $\iota_{U,V} : \mathcal{G}(G/U) \hookrightarrow \mathcal{G}(G/V)$ denotes the natural injection defined analogously to ι_U from last corollary.*

Proof. That every c defines such a collection is clear. Since every simple G-module A comes from a G/U-module for some $U \in \mathcal{U}_G$ by the last proposition, we must set $c(A) := c_U(A)$. The commutativity relation tells us that this is well defined. □

3.2. Brauer characters

For a field k of characteristic $p > 0$ some of the "nice" properties fail that characters over fields of characteristic zero have. Brauer characters are "lifts" into a field of characteristic zero and, indeed, help restore some of the desired properties.

Following [1] we make the following

3.2.1 Definition. *Let R be a discrete valuation ring with quotient field K, maximal ideal $\wp$ and residue field $k = R/\wp$. If $char(k) = p > 0$ and (in addition to the definition in [1]) $char(K) = 0$, we call the triple (R, K, k) a* **p-modular system**. *We call the map*

$$R \to k, x \mapsto \overline{x} = x\wp$$

reduction modulo p.

3.2.2 Example. *$(\mathbb{Z}_p, \mathbb{Q}_p, \mathbb{F}_p)$ is a p-modular system. This will be the most important p-modular system for our purposes.*

Now we fix a p-modular system (R, K, k). Let m be a positive integer with $m = p^r m'$, $(p, m') = 1$. Furthermore, let ω be a primitive m-th root of 1 in K and therefore in R. We put

$$K' := K(\omega), k' := k(\overline{\omega}).$$

Denote by $\mu_{K'}$ resp. $\mu_{k'}$ the set of m-th roots of 1 contained in K' resp. k'.

3.2.3 Remark. *Reduction modulo p defines a surjective homomorphism*

$$\mu_{K'} \to \mu_{k'}, \omega \mapsto \overline{\omega}$$

with kernel $< \omega^{p^r} >$.

This is clear. If m is now a positive integer, which is not divided by p, we get an isomorphism. We denote the inverse image of $\zeta \in \mu_{k'}$ in $\mu_{K'}$ by $\tilde{\zeta}$ and call it the **lift** of ζ.

Now we also have an isomorphism between the Galois groups $G(K'/K)$ and $G(k'/k)$, since all K'- resp. k'-automorphisms are determined by their actions on $\mu_{K'}$ resp. $\mu_{k'}$. This now implies the following remark, which is an important ingredient in the definition of Brauer characters.

3.2.4 Remark. *If a sum of $\overline{\omega}^i$'s is in k, then the respective sum of the ω^i's is in R.*

Returning to the study of groups we first have the following

3.2.5 Proposition. *Let G be a finite group. For every $g \in G$ there are unique $s, u \in < g >$ with the properties: $(p, ord(s)) = 1$, $ord(u)$ is a p-power and $g = su = us$.*

Proof. $ord(g) = p^n m$ with $(p, m) = 1$. Therefore there are integers a, b such that $ap^n + bm = 1$. Set $u := g^{bm}$ and $s := g^{ap^n}$. These clearly satisfy the properties. Given any other such pair u', s', we have $u'u^{-1} = ss'^{-1}$. Since all elements concerned commute with one another as they are in $< g >$, the order of the left hand side is divisible by a power of p (including 1) and the right hand side is not. Therefore $s = s'$ and $u = u'$. □

3.2.6 Definition. *Let G again be a finite group and p a prime.*

- *An element $g \in G$ is called a* **p-element** *if its order is a power of p.*
- *An element $g \in G$ is called a* **p'-element** *or a* **p-regular** *element if its order is not divisible by p.*
- *The set of all p-regular elements in G is denoted G_{reg}.*
- *s and u from the last proposition are called the* **p'-component** *resp. the* **p-component** *of g.*

We now generalize this notion to profinite groups.

3.2.7 Definition. *Let G now be a profinite group and p a prime. An element $g \in G$ is called* **p-regular** *if its image under all natural projections $G \to G/U$ for $U \in \mathcal{U}_G$ is p-regular in the above sense. The set of all p-regular elements is again denoted G_{reg}.*

In the language of supernatural numbers an element g is in G_{reg} if and only if its order is not divisible by p.

We have $\varprojlim (G/U)_{reg} = G_{reg}$, from which we conclude that G_{reg} is compact, as a projective limit of compact spaces is compact (cf. [6], IV, §2).

Let for the moment G be finite again and $E \in \mathcal{C}_{k,G}$ a finite dimensional G-module. For a p-regular element $g \in G$ of order m the value of its character $\chi_E(g)$ is a sum of m-th roots of 1 in k. Remark 3.2.4 thus allows us to lift this value.

3.2.8 Definition. *We define the* **Brauer character** *of the G-module $E \in \mathcal{C}_{k,G}$ with character χ_E by*

$$\phi_E : G \to R, \quad g \mapsto \begin{cases} \sum_i \tilde{\lambda}_i & \text{for } g \in G_{reg} \text{ with } \chi_E(g) = \sum_i \lambda_i \\ 0 & \text{for } g \notin G_{reg} \end{cases}$$

The fact already stated in the last section, that the action map of any representation with module in $\mathcal{C}_{k,G}$ of profinite groups is locally constant, allows us to extend this definition as follows:

3.2.9 Definition. *Let G be a profinite group and $E \in \mathcal{C}_{k,G}$ a discrete G-module with action map being constant modulo U for some $U \in \mathcal{U}_G$ such that E is also a G/U-module, denoted E_U. Define the* **Brauer character**

$$\phi_E : G \to R, \quad g \mapsto \begin{cases} \phi_{E_U}(g_U) & \text{for } g \in G_{reg} \\ 0 & \text{for } g \notin G_{reg} \end{cases}$$

where g_U is the image of g under the natural projection $G \to G/U$.

The Brauer character is well defined. Let us suppose that the action map is also locally constant modulo V for $V \in \mathcal{U}_G$. Then G/U and G/V act on E in the same way, meaning for $x \in E$ we have

$$sx = sUx = sVx \qquad (\forall x \in E, \forall s \in G_{reg}).$$

Therefore the "usual" characters are the same and hence so are their lifts.

We also point out that this definition is equivalent to the one used by Serre in [9].

The following remark is a direct consequence of the definition.

3.2.10 Remark. *The Brauer characters are locally constant functions $G \to R$.*

Next we collect some basic properties of Brauer characters.

3.2.11 Proposition. *Let G be a profinite group and $E, E', E'' \in \mathcal{C}_{k,G}$. Then*

(i) $\phi_E(1) = dim_k(E)$

(ii) $\phi_E(t^{-1}st) = \phi_E(s)$ *for all $s, t \in G$. ϕ_E therefore is a class function.*

(iii) Given an exact sequence $0 \to E' \to E \to E'' \to 0$, we have $\phi_E = \phi_{E'} + \phi_{E''}$. This implies in particular that ϕ_E only depends on the composition factors of E. In other words, we receive a well defined map $\mathcal{G}(\mathcal{C}_{k,G}) \to R$.

(iv) $\phi_{(E \otimes_k E')} = \phi_E \, \phi_{E'}$

(v) For $g \in G$ with decomposition from proposition 3.2.5 $g = su$ we have

$$\chi_E(g) = \overline{\phi_E(s)},$$

where χ_E is the "usual" character of E.

(vi) Let $k = \mathbb{F}_p$. For $s \in G_{reg}$ we have $\chi_E(s) = \chi_E(s^p)$ and $\phi_E(s) = \phi_E(s^p)$.

(vii) Let H be a finite (closed) subgroup of G. Denote by E^H the submodule fixed by all elements of H. Then

$$dim_k(E^H) = \frac{1}{|H|} \sum_{h \in H} \phi_E(h).$$

Proof. First we remark that it suffices to consider the case of a finite group G, for we have defined the value at $g \in G$ by the Brauer character of the image of g in a finite group G/U.

(i) The Brauer character here is clearly the sum on $dim_k(E)$ 1's since the endomorphism corresponding to 1 is the identity.

(ii) Analogously to the proof in characteristic zero the λ_i appearing in $\chi_E(s)$ only depend on the conjugacy class of s and therefore so do their lifts.

(iii) As in characteristic zero.

(iv) As in characteristic zero.

(v) By definition we have $\chi_E(s) = \overline{\phi_E(s)}$. The rest follows because any element of $End(E)$ with order a power of p has, written in upper diagonal form, only 1's on the diagonal, as there are no other p-th roots of 1. Therefore $\chi_E(s) = \chi_E(su)$.

(vi) For $\lambda \in \mathbb{F}_p$ we have that $\lambda^p = \lambda$. Therefore

$$\chi_E(s) = \sum_i \lambda_i = \sum_i \lambda_i^p = \chi_E(s^p).$$

Thus their lifts are also equal.

(vii) As in characteristic zero.

□

3.3. The decomposition map and an application

In this section we introduce the decomposition map, which allows us to "move" from G-modules over K to ones over k, their "decompositions". We will establish a relation between the "usual" characters over K and the Brauer characters of their decompositions. This we will do in some generality.

Fix a p-modular system (R, K, k), where K is a finite extension of $\mathbb{Q}_p$, and a profinite group G. We wish to drop the assumption of discreteness for our modules over K for the time being.

3.3.1 Definition. *Let $\mathcal{M}_{K,G}$ be the category of finite dimensional K-vector spaces, endowed with the ultrametric topology coming from the discrete valuation ring R, on which G acts continuously.*

3.3.2 Definition. *Let $E \in \mathcal{M}_{K,G}$. $L \subseteq E$ is an **R-lattice of E**, if*

- *L is a finitely generated R-submodule of E such that $L \otimes_R K = KL = E$ (allowing denominators)*
- *L is stable under the action of G.*

3.3.3 Remark. *Let $E \in \mathcal{M}_{K,G}$ and L an R-lattice of E.*

- *L is a free R-module.*
- *$\chi_M(g) = \chi_L(g)$ for all $g \in G$, where χ_M and χ_L denote the characters of M resp. L.*

Proof. L as a submodule of a vector space is torsion free, and, as R is a principal ideal domain, free.

The matrix associated (with respect to some basis of L) to the endomorphism of $x \mapsto gx$ for $x \in L$ also represents the action of g on M with respect to the same basis embedded in M. Hence the second result. □

3.3.4 Proposition. *For any $E \in \mathcal{M}_{K,G}$ an R-lattice L exists.*

Proof. Pick a K-basis $\{e_1, \ldots, e_n\}$ of E and put $N :=< e_1, \ldots, e_n >_R$ its R-span. This is in general not G-stable. Therefore we consider the subgroup

$$U := \{g \in G \mid gN \subseteq N\}.$$

Denote by α_i the continuous map $G \to E,\ g \mapsto ge_i$. We clearly have

$$U = \bigcap_{i=1}^{n} \alpha_i^{-1}(N).$$

From general facts about ultrametric vector spaces we know that $N \subseteq E$ is open. Therefore $U \subseteq G$ is open. This yields a decomposition of G into cosets modulo U:

$$G = \bigcup_{j=1}^{m} g_j U$$

for representatives g_j. Now we set $l_i := \sum_{j=1}^{m} g_j e_i$ and $L :=< l_1, \ldots, l_n >_R$, which by construction is stable under the action of G. □

Any R-lattice L can now be regarded as a G-module over k, which we denote $\overline{L}$, by reducing scalars modulo p:

$$\overline{L} = L \otimes_R k = L/\wp L.$$

From our assumptions on the p-modular system we get that $\overline{L}$ has the discrete topology and therefore is an element of $\mathcal{C}_{k,G}$.

We recall that we denote by $[A]$ the image of the G-module A in the Grothendieck group $\mathcal{G}(\mathcal{C}_{k,G})$.

3.3.5 Proposition. *Let $E \in \mathcal{M}_{K,G}$ with two R-lattices L, M. Then $\overline{L}$ and $\overline{M}$ have the same composition factors over k, i.e. $[\overline{L}] = [\overline{M}]$.*

Proof.

- special case: $\wp L \subseteq M \subseteq L$
  Hence $\wp M \subseteq \wp L \subseteq M \subseteq L$. Therefore L/M and $\wp L/\wp M$ can be regarded as isomorphic G-modules over k.

  It is clear that the following sequence of G-modules over k is exact.

  $$0 \to \wp L/\wp M \to M/\wp M \to L/\wp L \to L/M \to 0$$

  Therefore we receive

  $$[\wp L/\wp M] - [M/\wp M] + [L/\wp L] - [L/M] = 0$$

  by remark 3.1.3. Thus $[M/\wp M] = [L/\wp L]$ and the proposition is proved in this special case.

- general case: Let $< m_1, \ldots, m_n >_R$ be a generating set for M. From the relation $M \subseteq KL$, we conclude that there are $x_i \in K$ such that $x_i m_i \in L$ for all i. Multiplying these we see that a scalar multiple of M is contained in L. Since $\overline{xM} = \overline{M}$, we can assume $M \subseteq L$.

  With the same arguments we see that there is an $n \in \mathbb{N}$ such that

  $$\wp^n L \subseteq M \subseteq L.$$

  Now let $N := \wp^{n-1} M + L$. This implies $\wp^{n-1} L \subseteq N \subseteq L$ and $\wp N \subseteq L \subseteq N$. From our special case we receive $[L] = [N]$. Repeating the above procedure with N and M, we finally arrive at $[L] = [M]$, finishing this proof.

□

The above proposition now allows us to make the following

3.3.6 Definition. *The map*

$$d : \mathcal{G}(\mathcal{M}_{K,G}) \to \mathcal{G}(\mathcal{C}_{k,G})$$

sending a G-module over K to the composition factors of the reduction modulo p of any of its R-lattices is called the **decomposition map**.

This gives us the following useful consequence for the relation between "usual" and Brauer characters, which we first prove for finite groups and later generalize to profinite groups in the special case of the p-modular system $(\mathbb{Z}_p, \mathbb{Q}_p, \mathbb{F}_p)$.

3.3.7 Proposition. *Let G be a finite group and $M \in \mathcal{M}_{K,G}$ a G-module over K with character χ_M. Then*

$$\chi_M(g) = \phi_{d(M)}(g) \qquad \forall g \in G_{reg}.$$

Proof. Choose a G-stable lattice L of M. By remark 3.3.3 we have $\chi_M = \chi_L$. Denote by ρ the action map of G on L. We consider its combination with the reduction modulo p

$$\alpha : G \to GL(L) \to GL(L/\wp L).$$

Let $g \in G_{reg}$. Thus $(p, m) = 1$ for $m := ord(g)$. The "usual" character therefore looks like $\chi_{L/\wp L} = \sum_i \lambda_i$ with λ_i m-th roots of 1 in a suitable finite extension of k.

Suppose $\chi_L(g) = \sum_i \omega_i$ with ω_i m-th root of 1 in a suitable finite extension of K. Then $\overline{\omega_i} = \lambda_i$ and the definition of the lift $\omega_i = \tilde{\lambda_i}$. Hence $\chi_M(g) = \phi_{d(M)}(g)$. □

3.3.8 Lemma. *Let $L = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ (m factors). Then the order of $GL(L)$ is a supernatural number, whose part prime to p is finite.*

Proof. Consider $a_{i,j} = \sum_{k=0}^{\infty} a_{i,j,k} p^k \in \mathbb{Z}_p$ subject to the condition $0 \leq k < m \Rightarrow a_{i,j,k} = \delta_{i,j}$. Therefore the matrix $A = (a_{i,j})$ has determinant $1 + p^m x \neq 0$ (in fact, reducing modulo p^m it is the identity matrix). For each $a_{i,j,k}$ we have p choices, if $k \geq m$. Since the index of the subgroup defined by all such A has finite index in $GL(L)$, the lemma is proved. □

3.3.9 Corollary. *Consider the p-modular system $(\mathbb{Z}_p, \mathbb{Q}_p, \mathbb{F}_p)$. Let G be a profinite group and $M \in \mathcal{M}_{\mathbb{Q}_p,G}$ a G-module over $\mathbb{Q}_p$ with character χ_M. Then*

$$\chi_M(g) = \phi_{d(M)}(g) \qquad \forall g \in G_{reg}.$$

Proof. We use the notation of the proof of the proposition. The lemma now implies that $m := ord(\rho(g))$ is finite and prime to p. Hence we can use the same arguments, namely the bijective correspondence of the m-th roots of 1, as in the proposition and obtain the desired result. □

A striking consequence is that the "usual" characters over $\mathbb{Q}_p$ are thus also locally constant.

3.4. Relations between Brauer characters and class functions

In this section let G be a finite group.

3.4.1 Proposition. *The Brauer characters of the simple G-modules $E \in \mathcal{C}_{k,G}$ are linearly independent over R and K.*

Proof. It is enough to show this over R, since any linear relation of the Brauer characters over K defines a relation over R by clearing denominators. For simplicity, we number the Brauer characters in question $\phi_1, \ldots, \phi_n$ and the "usual" ones $\chi_1, \ldots, \chi_n$. Assume we are given a relation

$$\sum_{i=1}^{n} r_i \phi_i = 0 \quad r_i \in R.$$

By dividing by a generator of $\wp$ we can assume that not all r_i are in $\wp$. Reducing modulo p we therefore get a non-trivial relation over k:

$$\sum_{i=1}^{n} \overline{r_i}\,\overline{\phi_i(g)} = 0 \quad \forall g \in G_{reg}$$

Using part 5 of proposition 3.2.11 we see

$$\sum_{i=1}^{n} \overline{r_i}\chi_i(g) = 0 \quad \forall g \in G.$$

Theorem 2.2.3 now yields $\overline{r_i} = 0$ for all i, implying $r_i \in \wp$. Contradiction. □

3.4.2 Proposition. *Let $exp(G) = m$. Assume K contains all m-th roots of 1. Then the Brauer characters ϕ_E for $E \in \Sigma_{k,G}$ form a K-basis of the space of class function on G_{reg} over K.*

Proof. Let f be a class function defined on G_{reg}. We can extend it to f' class function on G, by setting $f'(g) = 0$ for $g \notin G_{reg}$. By theorem 2.2.3 we find $a_i \in K$ such that

$$f' = \sum_{i=0}^{n} a_i \chi_{M_i},$$

where $M_1, \ldots, M_n$ are the simple G-modules in $\Sigma_{K,G}$. Restricting again to G_{reg} and using proposition 3.2.11, we find

$$f = \sum_{i=0}^{n} a_i \phi_{d(M_i)}.$$

As every $\phi_{d(M_i)}$ is a linear combination of Brauer characters of simple G-modules over k, namely of the composition factors of $d(M_i)$, and keeping in mind their linear independence, the proof is complete. □

We now come to the observation which is central for our purposes. As p-modular system we now consider the special case $(\mathbb{Z}_p, \mathbb{Q}_p, \mathbb{F}_p)$. Part 6 of propostion 3.2.11 tells us $\phi_A(s^p) = \phi_A(s)$ and $\chi_A(s^p) = \chi_A(s)$ for all $s \in G_{reg}$ and $A \in \mathcal{C}_{\mathbb{F}_p,G}$.

We thus know that the above proposition is not true for $\mathbb{Q}_p$. We will, however, be able to describe the subspace of the class functions (restricted to G_{reg}) generated by the Brauer characters over $\mathbb{Q}_p$ explicitly. The next corollary shows that it is given by

$$\mathcal{H}_G := \{f : G_{reg} \to \mathbb{Q}_p \mid \text{f class function and } f(s^p) = f(s) \ \ \forall s \in G_{reg}\}.$$

We will, however, first prove the following proposition.

3.4.3 Proposition. *$\mathcal{H}_G$ is generated as a $\mathbb{Q}_p$-vector space by the restrictions to G_{reg} of the characters χ_V for $V \in \Sigma_{\mathbb{Q}_p,G}$.*

Proof. This proof is an adaption of Serre's proof in [9], given for the next corollary.

- Let K be a finite extension of $\mathbb{Q}_p$ containing all m-th roots of 1, where $m := exp(G) = m'p^r$ with $(m', p) = 1$. Further put $X := G(K/\mathbb{Q}_p)$ and $|X| = tp^n$ with $(t, p) = 1$.

  Consider the linear surjection

  $$\alpha : K \to \mathbb{Q}_p, \ x \mapsto \sum_{\sigma \in X} \sigma(x).$$

- Suppose ω is a primitive m'-th root of 1 in K, then ω^{p^i} for $i = 0, \ldots, t-1$ are all the other primitive ones.

  Galois automorphisms clearly preserve the (multiplicative) order of elements. Thus there are p^n distinct $\sigma \in X$ such that $\sigma(\omega) = \omega^{p^i}$ for each $i = 0, \ldots, t-1$.

  Hence we conclude that

  $$\alpha(\omega) = p^n \sum_{i=0}^{t-1} \omega^{p^i},$$

  which is the main ingredient in this proof.

- Let $f \in \mathcal{H}_G$. We can extend it to f' class function on G, by setting $f'(g) = 0$ for $g \notin G_{reg}$. By theorem 2.2.3 we find $a_T \in K$ such that

$$f' = \sum_{T \in \Sigma_{K,G}} a_T \chi_T.$$

- Suppose we are given $T \in \mathcal{C}_{K,G}$. Denote by T^0 the $\mathbb{Q}_p[G]$-module obtained by restriction scalars via α from T, i. e. $T^0 = T \otimes_K \mathbb{Q}_p$.

  Let now A be the matrix corresponding to the endomorphism of T given by $x \mapsto sx$ for $s \in G_{reg}$. Then the respective endomorphism of T^0 is given by $\alpha(A)$, meaning the application of α to the entries of A.

  Suppose the character of T has value on $s \in G_{reg}$ given by $\chi_T(s) = \sum_{j=1}^{l} \omega_j$. Then $\chi_T(s^{p^i}) = \sum_{j=1}^{l} \omega_j^{p^i}$.

  Now we look at the value at s of the character of T^0. From the discussion above, it is given by

$$\chi_{T^0}(s) = \sum_{j=1}^{l} \alpha(\omega_j) = \sum_{j=1}^{l} p^n \sum_{i=0}^{t-1} \omega_j^{p^i} = p^n \sum_{i=0}^{t-1} \chi_T(s^{p^i}).$$

- We make a simple calculation:

$$\begin{array}{lll} \sum_T a_T \chi_{T^0}(s) & = \sum_T a_T p^n \sum_{i=0}^{t-1} \chi_T(s^{p^i}) & = p^n \sum_{i=0}^{t-1} \sum_T a_T \chi_T(s^{p^i}) \\ & = p^n \sum_{i=0}^{t-1} f(s^{p^i}) & = |X| f(s) \end{array}$$

- We can decompose the $\mathbb{Q}_p[G]$-modules T^0 into simple ones and choose a linearly independent subset of their characters. As f and all characters take values in $\mathbb{Q}_p$, the coefficients must now be elements of $\mathbb{Q}_p$. This completes the proof.

□

3.4.4 Corollary. (Serre [9]) *The Brauer characters ϕ_S for $S \in \Sigma_{\mathbb{F}_p,G}$ form a $\mathbb{Q}_p$-basis of $\mathcal{H}_G$.*

Proof. Take $f \in \mathcal{H}_G$. By the proposition it can be written

$$f = \sum_{V \in \Sigma_{K,G}} a_V \chi_V|_{G_{reg}}$$

with $a_V \in \mathbb{Q}_p$. Now we apply proposition 3.2.11 and see

$$f = \sum_{V \in \Sigma_{K,G}} a_V \phi_{d(V)}.$$

Since every $\phi_{d(V)}$ is an integral linear combination of simple Brauer characters and since the simple Brauer characters are linearly indepent by proposition 3.4.1, the corollary is proved. □

At this point we introduce some useful objects, which allow us to find yet another basis of $\mathcal{H}_G$. We will, however, not give proofs, as they involve the introduction of more "machinery". Complete treatments can be found in [11] and [1].

First consider the general situation of a finite dimensional algebra over a field.

3.4.5 Definition. *A module homomorphism $f : E \to F$ is called* **essential** *if $f(E) = F$, but $f(E') \neq F$ for all proper submodules $E' < E$.*

A **projective cover** *of a module E is a projective module P_M together with an essential module homomorphism $P_M \to M$.*

It turns out that for every module there is a projective cover, which is unique up to isomorphism

Let us now consider a p-modular system (R, K, k). Using "idempotent lifting", one can show the following

3.4.6 Lemma. *Let P_k be a projective $k[G]$-module. There is a projective $R[G]$-module P_R, which is unique up to isomorphism, such that $P_R \otimes_R k = P_k$ (reduction modulo p).*

3.4.7 Definition. *We define the map* **e** *that sends (an isomorphism class of) a projective $k[G]$-module P_k to (the isomorphism class of) the projective $K[G]$-module $P_R \otimes_R K$.*

In a certain sense e and the decomposition map d are adjoint.
We list some properties:

3.4.8 Proposition. *(i) Let P be a projective $k[G]$-module. Then $\chi_{e(P)}(s) = 0$ for all $s \notin G_{reg}$.*

(ii) Let $S, T \in \Sigma_{k,G}$ and put $d_S = dim_k(End(S))$. Denote by P_S the projective cover of S. Then

$$\frac{1}{|G|} \sum_{s \in G} \chi_{e(P_S)}(s^{-1}) \phi_T(s) = d_S \, \delta_{S,T}.$$

We can regard the sum in (2) as a scalar product and thus conclude that the $\chi_{e(P_S)}$ for $S \in \Sigma_{k,G}$ are linearly independent. This implies the

3.4.9 Corollary. *The $\chi_{e(P_S)}|_{G_{reg}}$ for $S \in \Sigma_{\mathbb{F}_p,G}$ form a basis of $\mathcal{H}_G$.*

For use later on we record the following

3.4.10 Remark. *Take $f \in \mathcal{H}_G$ and extend it to all of G by $f(s) = 0$ for $s \notin G_{reg}$. Then there are $a_S \in \mathbb{Q}_p$ for $S \in \Sigma_{\mathbb{F}_p,G}$ such that $f = \sum a_S \chi_{e(P_S)}$.*

3.5. Application to distributions

In this section we will see how the last corollary enables us to describe Euler-Poincaré maps by certain distributions.

First we will introduce distributions on a totally disconnected compact Hausdorff space X. By $\mathcal{LC}(X, K)$ we denote the K-vector space of locally constant functions on X with values in the field K.

3.5.1 Definition. *A* **distribution on X** *is a K-linear map*

$$\mu : \mathcal{LC}(X, K) \to K, \quad f \mapsto \mu(f) =: < f, \mu > .$$

We wish to give to some examples, which will be used for the applications to Galois theory given in chapter 6.

3.5.2 Example.

- *Define the* **Dirac distribution** *of $x \in X$ by*

$$\delta_x(f) := f(x).$$

- *Let G be a profinite group. For $f \in \mathcal{LC}(X, K)$, which is locally constant modulo $U \in \mathcal{U}_G$, we set*

$$\mu(f) := \frac{1}{(G : U)} \sum_{x \in G/U} f(x).$$

This definition does not depend on the choice of U as a brief calculation shows. We call μ the **Haar distribution** *of G.*

Now consider a profinite group G and the p-modular system $(\mathbb{Z}_p, \mathbb{Q}_p, \mathbb{F}_p)$. We recall that G_{reg} is compact.

The following is clear.

3.5.3 Remark. *The maps $G_{reg} \to G_{reg}$ defined by*

- $s \mapsto g^{-1}sg$ *for* $g \in G$
- $s \mapsto s^p$

are homeomorphisms.

We will now introduce the space of distributions we are interested in and relate it to $\mathcal{H}_G$.

3.5.4 Definition. *We define $\mathcal{D}_G$ to be the space of distributions μ on G_{reg} with values in $\mathbb{Q}_p$, such that $< f \circ \alpha, \mu >=< f, \mu >$ for α any of the homeomorphisms of the above remark. We say $\mu \in \mathcal{D}_G$ is invariant under $s \mapsto g^{-1}sg$ for $g \in G$ and $s \mapsto s^p$.*

3.5.5 Proposition. *Let G be a finite group. A distribution $\mu \in \mathcal{D}_G$ is uniquely defined by its values on $\mathcal{H}_G$ and thus on the simple Brauer characters.*

Proof. Denote by α_g the conjugation by $g \in G$ and by β the map $s \mapsto s^p$. There is a positive integer n such that β^n is the identity on G_{reg}. Given $\mu \in \mathcal{D}_G$ we must find its value on $f \in \mathcal{LC}(G_{reg}, \mathbb{Q}_p,)$. This we do by averaging over all homeomorphisms in question:

$$g := \frac{1}{|G| + n}(\sum_{g \in G} f \circ \alpha_g + \sum_{i=0}^{n-1} f \circ \beta^i)$$

g is clearly an element of $\mathcal{H}_G$ and $< g, \mu >=< f, \mu >$. □

In the last section we noted different bases of $\mathcal{H}_G$. Expressing the simple Brauer characters in terms of them, we receive the following

3.5.6 Remark. *Let G be a finite group. A distribution $\mu \in \mathcal{D}_G$ is uniquely determined by its values on $\chi_V|_{G_{reg}}$ for $V \in \mathcal{C}_{\mathbb{Q}_p,G}$ and even on $\chi_{e(P_S)}|_{G_{reg}}$ for the projective covers of $S \in \Sigma_{\mathbb{F}_p,G}$.*

We can reformulate the proposition and take a slightly different point of view.

3.5.7 Remark. *For a finite group G, the Euler-Poincaré maps in $\mathcal{EP}(G)$ are in a bijective correspondence with the distributions in $\mathcal{D}_G$.*

For an Euler-Poincaré map is uniquely defined by its values on the simple G-modules and a distribution in $\mathcal{D}_G$ by its values on the Brauer characters of these simple G-modules. □

We also observe the following characterization of invariant distributions, which is more explicit:

3.5.8 Remark. (Serre [9]) *Let G be a finite group. For $\mu \in \mathcal{D}_G$ there is one and only one $\theta \in \mathcal{H}_G$ such that for all $f : G_{reg} \to \mathbb{Q}_p$*

$$< f, \mu >= \frac{1}{|G|} \sum_{g \in G} \theta(g) f(g).$$

(For $g \notin G_{reg}$ we set $\theta(g) = 0$ and give $f(g)$ any value.)

Proof. As we have seen above, μ is uniquely defined on the simple Brauer characters. We use the homeomorphisms from remark 3.5.3 to form an equivalence relation on G_{reg}. The number of equivalence classes clearly is the $\mathbb{Q}_p$-dimension of $\mathcal{H}_G$, and hence equal to the number of simple Brauer characters. We therefore have to solve the following square system of inhomogeneous linear equations

$$< \phi_{E_j}, \mu >= \sum_{i=1}^{n} \frac{|C_i|}{|G|} \phi_{E_j}(g_i)\theta(g_i),$$

where n is the number of equivalence classes and C_i is the $i-th$ one with representative g_i. E_j denotes the j-th simple $k[G]$-module. Since the simple Brauer characters are linearly independent, this system of equations has one and only one solution in the variables $\theta(g_i)$. □

In view of corollary 3.4.9, we can express the function θ as a linear combination of characters. (We use the notation from section 3.4.)

3.5.9 Remark. (Serre [9]) $\theta = \sum_{S \in \Sigma_{\mathbb{F}_p,G}} \mu(\phi_S)\frac{1}{d_S}\chi_{e(P_S)^*}$, *where* * *denotes the dual module.*

Proof. Due to the uniqueness of θ proved above, the result follows from the following calculation. Let $S \in \Sigma_{\mathbb{F}_p,G}$.

$$\begin{aligned} \frac{1}{|G|}\sum_{s\in G}\theta(s)\phi_S(s) &= \frac{1}{|G|}\sum_{s\in G}\sum_{T\in\Sigma_{\mathbb{F}_p,G}}\mu(\phi_T)\frac{1}{d_T}\chi_{e(P_S)}(s^{-1})\phi_S(s) \\ &= \sum_{T\in\Sigma_{\mathbb{F}_p,G}}\mu(\phi_T)\frac{1}{d_T}\left(\frac{1}{|G|}\sum_{s\in G}\chi_{e(P_S)}(s^{-1})\phi_S(s)\right) \\ &= \mu(\phi_S) \end{aligned}$$

□

We now return to a profinite group G. We recall that for $V \leq U$ with $U, V \in \mathcal{U}_G$ we have a natural injection $\Sigma_{k,G/U} \hookrightarrow \Sigma_{k,G/V}$. By identifying the basis of Brauer characters of $\mathcal{H}_{G/U}$ with the corresponding Brauer characters of $\mathcal{H}_{G/V}$, a natural injection of $\mathbb{Q}_p$-vector spaces $\mathcal{H}_{G/U} \hookrightarrow \mathcal{H}_{G/V}$ arises.

Since we are only concerned with locally constant functions, a distribution $\mu \in \mathcal{D}_G$ is uniquely determined by a collection $(\mu_{G/U} \in \mathcal{D}_{G/U})_{U\in\mathcal{U}_G}$ subject to the "commutativity relations"

$$V \leq U \;\Rightarrow\; \mu_{G/V}|_{\mathcal{H}_{G/U}} = \mu_{G/U},$$

where we use the above embedding $\mathcal{H}_{G/U} \hookrightarrow \mathcal{H}_{G/V}$.

By proposition 3.1.6, remark 3.5.7 and the correspondence between a basis of $\mathcal{H}_{G/U}$ and $\Sigma_{k,G/U}$, a collection of distributions $(\mu_{G/U})_{U\in\mathcal{U}_G}$ is uniquely defined by an Euler-Poincaré map in $\mathcal{EP}(G)$. This gives the principal result of this chapter:

3.5.10 Theorem. (Serre [9]) *Let $c \in \mathcal{EP}(G)$ an Euler-Poincaré map. There is one and only one distribution $\mu^c \in \mathcal{D}_G$ such that*

$$< \phi_E, \mu^c >= c(E)$$

for all $E \in \mathcal{C}_{k,G}$.

4. Cohomology of profinite groups

4.1. Definition and basic properties

We introduce continuous cohomolgy in quite a general setting, but will quickly go on to specialize.

Let G be a topological group and A a topological G-module, with the additional property that the action of G on A is continuous. Such an A is called a **continuous G-module**. (From now on the term G-module is often used instead of continuous G-module.)

4.1.1 Definition. *Let $C^n(G,A)$ be the abelian group of all continuous maps $G^n \to A$, where G^n is the n-fold product of G, equipped with the product topology. $f \in C^n(G,A)$ is called an* **n-cochain**.

We wish to form a complex consisting of the C^n.

4.1.2 Definition. *The* **coboundary operator**

$$d^n : C^n(G,A) \to C^{n+1}(G,A)$$

for $n > 0$ is defined by

$$\begin{aligned}(d^n f)(x_1,\dots,x_{n+1}) &:= x_1 f(x_2,\dots,x_{n+1}) \\ &+ \textstyle\sum_{i=1}^{n}(-1)^i f(x_1,\dots,x_{i-1},x_i x_{i+1},x_{i+2},\dots,x_{n+1}) \\ &+ (-1)^{n+1} f(x_1,\dots,x_n)\end{aligned}$$

Following the example of most of the books on this subject, I shall take the liberty of skipping the proof of the following lemma, which shows that the $C^n(G,A)$ indeed form a (co-)complex $C(G,A)$.

4.1.3 Lemma. $d^n \circ d^{n-1} = 0 \ \ \forall n > 1$

4.1.4 Definition. *The cohomology groups of the complex $C(G,A)$ are called the* **cohomology groups of G with coefficients in A**.

4.1.5 Remark. *If G acts trivially on A, then $H^1(G,A)$ is exactly the group of continuous group homomorphisms $f : G \to A$, as $df(x,y) = f(y) - f(xy) + f(x)$.*

Next, we wish to make a step towards the "long exact sequence" coming from an exact sequence of continuous G-modules A, B, C.

4.1.6 Lemma. *Consider the exact sequence*

$$0 \to A \to B \to C \to 0,$$

with maps $\alpha : A \to B$ and $\beta : B \to C$ being continuous G-homomorphisms subject to the conditions:
(i) the topology of A is induced by that of B
(ii) β has a continuous section γ, i.e. $\beta \circ \gamma = id_C$ (γ need not be a homomorphism).
Then for every $n \in \mathbb{N}$ we get an exact sequence of complexes

$$0 \to C^\bullet(G,A) \to C^\bullet(G,B) \to C^\bullet(G,C) \to 0,$$

the maps $\tilde{\alpha}$ and $\tilde{\beta}$ being given by composing the cochain with α resp. β.

Proof. We have $\tilde{\beta} \circ \tilde{\alpha}(f) = \beta \circ \alpha \circ f = 0$. Further $\tilde{\alpha}$ is injective, since condition (i) allows us to view A as a sub-G-module of B. Given a cochain $g \in C^n(G, C)$, define $f := \gamma \circ g$ a cochain in $C^n(G, B)$. $\tilde{\beta}$ is surjective, since $\beta \circ f = \beta \circ \gamma \circ g = g$. □

Following Wilson ([16]), we call an exact sequence satisfying both of these conditions **well adjusted**.

Due to the lemma, (co-)homological algebra tells us that, for every well adjusted exact sequence, there exists a "long exact sequence"

$$\cdots \to H^n(G, A) \to H^n(G, B) \to H^n(G, C) \to H^{n+1}(G, A) \to \ldots$$

(for every $n \in \mathbb{N}$) with maps $H^n(G, A) \to H^n(G, B)$ and $H^n(G, B) \to H^n(G, C)$ coming from $\tilde{\alpha}$ and $\tilde{\beta}$ and the "connecting homomorphisms" $\delta : H^n(G, C) \to H^{n+1}(G, A)$.

4.1.7 Example. *Equipping A, B and C with the discrete topology, we clearly have a well adjusted exact sequence.*

A large part of this essay is concerned with discrete modules. We are, however, also interested in the "p-adic" case of $\mathbb{Z}_p$-modules and $\mathbb{Q}_p$-vector spaces.

We have the

4.1.8 Remark.

- *Let $A \leq B$ be an open submodule. Then B/A has as quotient topology the discrete one and hence the short exact sequence*

  $$0 \to A \to B \to A/B \to 0$$

  is well adjusted.

- *Suppose A, B are finitely generated $\mathbb{Z}_p$-modules or $\mathbb{Q}_p$-vector spaces, equipped with the p-adic topology. Then*

  $$0 \to A \to B \to A/B \to 0$$

  is well adjusted.

It should be mentioned here that, if we insist on the G-modules to be k-vector spaces, the same is true for the cohomology groups.

4.2. Maps of cohomology groups

In this section, which is based on [16], we list some important, but very technical results.

We begin with a

4.2.1 Definition. *Let G_1, G_2 be profinite groups and let A_i be G_i-modules ($i = 1, 2$). A pair of maps*

$$(\theta, \varphi), \quad \theta : G_1 \to G_2, \quad \varphi : A_2 \to A_1$$

is called **compatible** *if $\varphi(\theta(x)a) = x\varphi(a) \ \ \forall x \in G_1 \ \forall a \in A_2$.*

4.2.2 Example.

(i) $\theta = id_G : G \to G$ and $\varphi : A_2 \to A_1$ continuous. Then (id_G, φ) is compatible if and only if φ is a G-module homomorphism.

(ii) Let $H \leq G$ be a closed subgroup, A a G-module and $\theta : H \hookrightarrow G$ the inclusion. Then (θ, id_A) is a compatible pair.

(iii) Let $K \lhd G$ be a closed normal subgroup and consider $\theta : G \to G/K$. For a G-module A, A^K is closed under G-action and is a G/K-module. Take the injection $\varphi : A^K \hookrightarrow A$. Then (θ, φ) are compatible.

4.2.3 Lemma. *Let $\theta : G_1 \to G_2$ and $\varphi : A_2 \to A_1$ be a compatible pair, $n \in \mathbb{N}$.*

(i) There is an induced homomorphism

$$(\theta, \varphi)^* : C^n(G_2, A_2) \to C^n(G_1, A_1)$$

given by $((\theta, \varphi)^* f)(x_1, \ldots, x_n) = \varphi f(\theta x_1, \ldots, \theta x_n)$.

(ii) The diagram

$$\begin{array}{ccc} C^n(G_2, A_2) & \to & C^n(G_2, A_2) \\ \downarrow & & \downarrow \\ C^n(G_1, A_1) & \to & C^n(G_1, A_1), \end{array}$$

where the horizontal maps are the coboundary operators and the vertical maps the $(\theta, \varphi)^*$, is commutative.

(iii) $(\theta, \varphi)^*$ induces a homomorphism $H^n(G_2, A_2) \to H^n(G_1, A_1)$, which we shall for the sake of simplicity also call $(\theta, \varphi)^*$.

Proof. (1) and (2) are easy calculations. (3) is a basic fact from cohomological algebra. The lemma and the proof can be found in [16], 9.2.1. □

We now apply the lemma to the above example and state the following

4.2.4 Definition. *Let A be a continuous G-module, $H \leq G$ a closed and $K \lhd G$ a closed normal subgroup. The homomorphism*

$$res : H^n(G, A) \to H^n(H, A)$$

induced by (2) of the example is called the **restriction** *and*

$$inf : H^n(G/K, A^K) \to H^n(G, A)$$

induced by (3) the **inflation** *homomorphism.*

4.2.5 Proposition. *Let I be a directed set of indices, $(G_i, \theta_{i,j})$ a projective system of profinite groups, $(A_i, \varphi_{j,i})$ a direct system of discrete abelian groups with A_i being a G_i-module. Set*

$$(G, \theta_i) := \varprojlim (G_i, \theta_{i,j}) \text{ and } (A, \varphi_i) := \varinjlim (A_i, \varphi_{j,i}).$$

Assume that each pair $(\theta_{i,j}, \varphi_{j,i})$ is compatible. Then

(i) There is a unique G-module structure on A such that each pair (θ_i, φ_i) is compatible.

(ii) The ablian groups $C^n(G_i, A_i)$ together with the induced maps

$$\gamma_{j,i} = (\theta_{i,j}, \varphi_{j,i})^* : C^n(G_i, A_i) \to C^n(G_j, A_j)$$

form a direct system, and the the induced maps

$$\gamma_i = (\theta_i, \varphi_i)^* : C^n(G_i, A_i) \to C^n(G, A)$$

satisfy $\gamma_j \gamma_{j,i} = \gamma_i$ for $i \leq j$.

(iii) The ablian groups $H^n(G_i, A_i)$ together with the induced maps

$$\eta_{j,i} = (\theta_{i,j}, \varphi_{j,i})^* : H^n(G_i, A_i) \to H^n(G_j, A_j)$$

form a direct system, and the the induced maps

$$\eta_i = (\theta_i, \varphi_i)^* : H^n(G_i, A_i) \to H^n(G, A)$$

satisfy $\eta_j \eta_{j,i} = \eta_i$ for $i \leq j$.

(iv) $(C^n(G,A),\gamma_i) = \varinjlim (C^n(G_i,A_i),\gamma_{j,i})$.

(v) $(H^n(G,A),\eta_i) = \varinjlim (H^n(G_i,A_i),\eta_{j,i})$.

Proof. The proof is quite technical, but uses no "deeper" results. The proposition with a complete proof can be found in [16], 9.7.2. □

The next result is of great importance to us.

4.2.6 Corollary. *Let G be a profinite group and A be a discrete G-module, $n \in \mathbb{N}$. Then*
(a) $H^n(G,A) \cong \varinjlim H^n(G/U, A^U)$, *taking the limit over $U \in \mathcal{U}_G$.*
(b) $H^n(G,A) \cong \varinjlim H^n(G,B)$, *taking the limit over all finitely generated submodules $B \leq A$.*

Proof. (a) We know $G = \varprojlim G/U$. For $V \leq U$ in $\mathcal{U}_G$ we have the inclusions $A^U \hookrightarrow A^V$, which form a direct system. In fact $A = \varinjlim A^U = \bigcup A^U$. As we have seen in the example, the maps are compatible and we can apply the last proposition.
(b) We clearly have $A = \bigcup_{B \leq A \text{ f. g.}} B = \varinjlim B$. Again the result follows from the example and the proposition. □

4.3. Coinduced modules

Here we give a short account of coinduced (also called induced) modules for a profinite group G, culminating in the statement of the Eckmann-Shapiro lemma.

We fix a closed subgroup $H \leq G$ for the rest of this section.

4.3.1 Definition. *Let A be a discrete H-module. We define the* **coinduced module** *of A to be the discrete G-module*

$$M_H^G(A) := \{f : G \to A \text{ continuous } \mid f(hx) = hf(x)\ \forall h \in H\ \forall x \in G\},$$

with respect to

- *addition:* $(f_1 + f_2)(x) := f_1(x) + f_2(x)$ *for* $x \in G$.
- *G-action:* $(gf)(x) = f^g(x) := f(xg)$ *for* $g, x \in G$.

We have to check the statements made in the definition. Let $f \in M_H^G(A)$. For $g, x \in G$ and $h \in H$ we have

$$f^g(hx) = f(hxg) = hf(xg) = h(f^g(x)).$$

Thus $f^g \in M_H^G(A)$.

$f \in M_H^G(A)$ is in particular a continuous funtion with values in a discrete space, therefore it is locally constant, say modulo $N \in \mathcal{U}_G$. Hence $f^n(x) = f(xn) = f(x)$ for all $n \in N$ and all $x \in G$. Thus the open subgroup N is contained in the stabilizer of f. In a profinite group a subgroup containing an open subset is open. Hence the stabilizer of f is open in G. This implies that $g \mapsto f^g$ is continuous, whence the G-action is continuous.

It is now clear that the coinduced module is well defined and has the properties claimed. □

4.3.2 Lemma. *The map*

$$\pi : M_H^G(A) \to A, \quad f \mapsto f(1)$$

is a surjective H-module homomorphism.

Proof. $\pi(f_1+f_2) = f_1(1)+f_2(1) = \pi(f_1)+\pi(f_2)$ and $h\pi(f) = hf(1) = f(h) = f^h(1) = \pi(f^h)$ for $h \in H$. Therefore π is an H-module homomorphism.

It is a fact of profinite groups (cf. [16], 1.3.4) that there is a continuous map $\beta : G \to H$ such that $\beta(1) = 1$ and $\beta(hx) = h\beta(x)$ for $h \in H$ and $x \in G$.

Let $a \in A$. Define $f_a : G \to A,\ x \mapsto \beta(x)a$, which clearly is continuous. Further $f_a(hx) = \beta(hx)a = h\beta(x)a = hf_a(x)$ and $f_a(1) = a$, whence $f \in M_H^G(A)$ and $\pi(f_a) = a$, implying that π is surjective. □

We wish to list the following results, which can be proved with the methods developped so far. Proofs can be found e.g. in [16].

4.3.3 Proposition. (Transitivity of coinduction) *Let $K \leq H \leq G$ be closed subgroups of G. Then*

$$M_K^H(M_H^G(A)) = M_K^H(A).$$

4.3.4 Proposition. *$M_H^G(.)$ is an exact functor.*

4.3.5 Proposition. (Eckmann-Shapiro lemma) *Let A be a discrete H-module. Then for each $n \in \mathbb{N}$ there is an isomorphism*

$$H^n(G, M_H^G(A)) \to H^n(H, A)$$

induced from the map $\pi : M_H^G(A) \to A$ above.

4.4. Some cohomological considerations

In this section we introduce some language and basic results from cohomological algebra. Our main reference is [7], II.5.

Let G be a profinite group. Denote by $\mathcal{A}_G$ the abelian category of discrete G-modules, and by $\mathcal{A}b$ the abelian category of abelian groups.

Proposition 4.2.5 implies that

$$H^q(G, .) : \mathcal{A}_G \to \mathcal{A}b$$

is a functor.

We would like to be a bit more precise.

4.4.1 Definition. *Let $\mathcal{A}$ be an abelian category. A* **cohomological functor** *$H = (H^q)_{q\in\mathbb{Z}}$ on $\mathcal{A}$ is a sequence of covariant additive functors $H^q : \mathcal{A} \to \mathcal{A}b$, which assigns to every short exact sequence $0 \to A \to B \to C \to 0$ in $\mathcal{A}$ a connecting homomorphism $\delta = \delta^n : H^n(C) \to H^{n+1}(A)$ such that the following two conditions are satisfied:*
(a) For every commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & A & \to & B & \to & C & \to & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \to & A' & \to & B' & \to & C' & \to & 0 \end{array}$$

in $\mathcal{A}$ with exact rows, the following diagram commutes for every q

$$\begin{array}{ccc} H^q(C) & \stackrel{\delta^q}{\to} & H^{q+1}(A) \\ \downarrow H^q(h) & & \downarrow H^{q+1}(f) \\ H^q(C') & \stackrel{\delta^q}{\to} & H^{q+1}(A'). \end{array}$$

(b) For each short exact sequence in $\mathcal{A}$

$$0 \to A \to B \to C \to 0,$$

the long sequence

$$\cdots \to H^{q-1}(C) \overset{\delta^{q-1}}{\to} H^q(A) \to H^q(B) \to H^q(C) \overset{\delta^q}{\to} H^{q+1}(A) \to \dots$$

is exact.

Using the theory developped so far, it is easily seen that $H^\bullet(G,.)$ and $H^\bullet(G/U,(.)^U)$ for $U \lhd G$ closed are cohomological functors for the category $\mathcal{A}_G$ of discrete G-modules, as well as for the categories of finitely generated $\mathbb{Z}_p$-modules and finitely generated $\mathbb{Q}_p$-vector spaces, on which G acts continuously and linearly, denoted by $\mathcal{M}_{\mathbb{Z}_p,G}$ and $\mathcal{M}_{\mathbb{Q}_p,G}$.

4.4.2 Definition. *Let H, F be cohomological functors on $\mathcal{A}$. A* **morphism of cohomological functors** *$\varphi : H \to F$ is a family $\varphi^q : H^q \to F^q$ $(q \in \mathbb{Z})$ of morphisms of functors (natural transformations) such that for every short exact sequence*

$$0 \to A \to B \to C \to 0$$

in $\mathcal{A}$ the following diagram commutes for all $q \in \mathbb{Z}$:

$$\begin{array}{ccc} H^q(C) & \overset{\delta^q}{\to} & H^{q+1}(A) \\ \varphi^q(C) \downarrow & & \downarrow \varphi^{q+1}(A) \\ F^q(C) & \overset{\delta^q}{\to} & F^{q+1}(A) \end{array}$$

It turns out that the restriction for a closed subgroup $H \leq G$

$$res : H^\bullet(G,.) \to H^\bullet(H,.)$$

and the inflation for a closed normal subgroup $U \lhd G$

$$inf : H^\bullet(G/U,(.)^U) \to H^\bullet(G,.)$$

are morphisms of cohomological functors on the categories $\mathcal{A}_G$, $\mathcal{M}_{\mathbb{Z}_p,G}$ and $\mathcal{M}_{\mathbb{Q}_p,G}$.

4.4.3 Definition. *Let H be a cohomological functor on $\mathcal{A}$. H is called* **positive***, if $H^q = 0$ for all $q < 0$. H is called* **effaceable** *by a subclass $\mathcal{B} \subseteq \mathcal{A}$, if H is positive and if for every $A \in \mathcal{A}$ there is a monomorphism*

$$\epsilon_A : A \to M_A, \quad M_A \in \mathcal{B}$$

with $H^q(M_A) = 0$ for all $q > 0$.

The following theorem is a very helpful tool, as it carries certain properties from dimension 0 to all other dimensions.

4.4.4 Theorem. *Let H, F be positive cohomological functors. Assume H is effaceable by the class of injectives of $\mathcal{A}$. Suppose $\varphi^0 : H^0 \to F^0$ is a morphism of functors. Then there is a unique morphism $\psi : H \to F$ such that $\varphi^0 = \psi^0$.*

Proof. [7], theorem II.5.5 □

Let H, F, E be cohomological functors on $\mathcal{A}$, such that H and F are effaceable by the class of injectives, and consider the following morphisms of functors:

$$H^0 \overset{\varphi^0}{\to} F^0, \quad F^0 \overset{\psi^0}{\to} E^0, \quad H^0 \overset{\rho^0}{\to} E^0,$$

with unique extensions φ, ψ and ρ. Then we have

$$\rho^0 = \psi^0 \circ \varphi^0 \;\Leftrightarrow\; \rho = \psi \circ \varphi$$

and

$$\varphi^0 \text{ is an isomorphism } \Leftrightarrow \; \varphi \text{ is an isomorphism.}$$

Here we would like to quote the following theorem, which allows us to apply the results above.

4.4.5 Theorem. *Let G be a profinite group and N a closed subgroup. Then the cohomological functors $H^\bullet(G,.)$ and $H^\bullet(N,.)$ are effaceable by the injectives of $\mathcal{A}_G$.*

Proof. [7], theorems II.5.10 and II.5.11 □

4.5. G-action on cohomology groups

Let G be a profinite group, $K \triangleleft G$ an open normal subgroup.

We wish to define a G-action on the cohomology groups $H^n(K,A)$ for $A \in \mathcal{A}_G$. This we do by acting on K by inner automorphisms. More precisely, let $x \in G$ and

$$\theta_x : K \to K, y \mapsto x^{-1}yx$$

be the conjugation homomorphism.

Further consider the homomorphism

$$\varphi_x : A \to A, a \mapsto xa.$$

As for $a \in A$ and $y \in K$

$$\varphi_x(\theta_x(y)a) = \varphi_x(x^{-1}yxa) = yxa = y\varphi_x(a),$$

the pair (θ_x, φ_x) is compatible.

From lemma 4.2.3 we receive induced maps

$$\overline{x}^n : H^n(K,.) \to H^n(K,.),$$

which one checks to form a morphism of cohomological functors.

Now consider $n = 0$ and $x \in K$. Let $a \in H^0(K,A) = A^K$. We have $\overline{x}^0(a) = xa = a$. Thus $\overline{x}^0$ is the identity map on K. By theorem 4.4.4 it follows that $\overline{x}^n$ is the identity for all $n \in \mathbb{N}$.

Define the maps

$$G/K \times H^n(K,A) \to H^n(K,A), \quad (x,f) \mapsto \overline{x}f.$$

As G/K is discrete, due to the strong assumption on K, the above maps make $H^n(K,A)$ into G/K-modules.

We next use theorem 4.4.4 to show that

$$res^n : H^n(G,A) \to H^n(K,A)^{G/K},$$

where res denotes the restriction.

It again suffices to check this for $n = 0$, which is obvious. We have used that $H^\bullet(K,.)^{G/K}$ is a cohomological functor, which follows from $H^\bullet(K,.)$ being one.

Now we wish to define the **corestriction**. We do this by defining it in dimension 0 and extending it to the other dimensions using theorem 4.4.4. Here K is an open subgroup of G. Put

$$cor^0 : A^K \to A^G, \; a \mapsto \sum_{g \in G/K} ga.$$

It turns out that cor^0 is a morphism of functors on $\mathcal{A}_G$. Thus theorem 4.4.4, indeed, gives us

$$cor^n : H^n(K,A) \to H^n(G,A)$$

for $n \in \mathbb{N}$.

4.5.1 Proposition. *Let K be an open normal subgroup of G. Then*

$$cor^n \circ res^n = (G : K)\, id$$

and

$$res^n \circ cor^n|_{H^n(K,A)^{G/K}} = (G : K)\, id$$

for all $n \in \mathbb{N}$.

In fact, for the first equation K need not be normal.

Proof. It is clear that $(G : K)\, id$ is a morphism of cohomological functors. Thus, it is again enough to check the equalities in dimension 0, where they are obvious. □

We would like to point out that it is possible to consider "only" closed normal subgroups K for the action of G/K on $H^n(K, A)$. Then, however, we have to use extra arguments to see that the action is continuous. A proof can be found in [16], lemma 10.2.4.

4.6. Cohomological dimension

In this section we fix a profinite group G.

4.6.1 Definition. *An abelian group A is called a* **$\mathbb{Z}$-torsion group** *if each element of A has finite order. If in addition the order of each element is a power of the prime p, A is a* **p-torsion group**.

4.6.2 Definition.

- *Let p be a prime. The* **p-cohomological dimension** *of G is defined to be*

$$cd_p(G) := \sup_{n \in \mathbb{N}} \{\ \exists p\text{-torsion } G\text{-module } A \text{ s.t. } H^n(G, A) \neq 0\ \}.$$

- *The* **cohomological dimension** *of G is*

$$cd(G) := \sup_{p \text{ prime}} \{cd_p(G)\}.$$

We now collect a few simple remarks for further use.
Since every element in a $\mathbb{Z}$-torsion group has finite order, we receive the

4.6.3 Remark. *Finitely generated $\mathbb{Z}$-torsion groups are finite.*

4.6.4 Remark. *Let A be a discrete G-module. If A is finitely generated as a G-module, then it is finitely generated as an abelian group.*

Proof. Let $a_1, \ldots, a_n$ be generators of A as a G-module. Since $A = \bigcup_{U \in \mathcal{U}_G} A^{U_i}$, there are $U_i \in \mathcal{U}_G$ such that $a_i \in A^{U_i}$. Since every U_i has finite index in G, a_i is only mapped into a finite number of $a_{i,j} \in A$ under the action of G. These generate A as an abelian group. □

4.6.5 Remark. *Let A be a finite simple G-module of order $|A| = n$. Then for every prime p dividing n we have $pA = 0$. In particular, every finite simple p-torsion module B satisfies $pB = 0$.*

Proof. There is an element x, whose order is divisible by p^r with r maximal with that property. Then the submodule pA does not contain x, as pA does not contain any element with order divisible by p^r. So $pA \neq A$ and hence by simplicity $pA = 0$. □

We will not make use of the next proposition. Since, however, it is easily proved with the methods we have at our disposal, we mention it.

4.6.6 Proposition. *Let G be a profinite group. Then*

$$cd_G = \sup_{n\in\mathbb{N}}\{\ \exists \text{ discrete } \mathbb{Z}\text{-torsion module } A \text{ s.t. } H^n(G,A)\neq 0\ \}.$$

Proof. We must show $H^n(G,A)=0$ for all $\mathbb{Z}$-torsion modules A and every integer $n > cd(G)$. By corollary 4.2.6 we have $H^n(G,A) = \varinjlim H^n(G,B)$, the limit being taken over all finitely generated submodules $B \leq A$. This reduces us to show $H^n(G,B)=0$ for all B finitely generated, hence by remark 4.6.3, finite submodules.

Assume A is simple, then by remark 4.6.5 there is a prime q with $qA=0$, hence A is a q-torsion module and by the definition of $cd(G)$ $H^n(G,A)=0$.

Now we argue by induction on the length of a composition series for A. If $B<A$ is a proper non-zero submodule, we have the short exact sequence $0\to B\to A\to B/A\to 0$. By induction hypothesis $H^n(G,B)=0=H^n(G,A/B)$. Hence the long exact sequence gives us $H^n(G,A)=0$ as desired. □

4.6.7 Proposition. *$cd_p(G) < n$ if and only if for all simple G-modules B satisfying $pB=0$ we have $H^n(G,B)=0$.*

Proof. By definition we have that $cd_p(G)<n$ is equivalent to $H^r(G,A)=0$ for all $r>n$ and for all discrete p-torsion modules A.

Using the same argument as in the last proof, the above is equivalent to $H^r(G,B)=0$ for all $r>n$ and for all simple discrete p-torsion modules B. By remark 4.6.5 the B's concerned are exactly those satisfying $pB=0$. □

We collect some properties of the p-cohomological dimension.

4.6.8 Proposition. *Let H be a closed subgroup of G and p a prime.*

(i) $cd_p(H)\leq cd_p(G)$

(ii) If p does not divide $(G:H)$, then $cd_p(H)=cd_p(G)$.

(iii) If H is a p-Sylow subgroup of G, then $cd_p(H)=cd_p(G)$.

(iv) If H is open in G and $cd_p(G)<\infty$, then $cd_p(H)=cd_p(G)$.

(v) A pro-p group G has p-cohomological dimension 0 if and only if $G=1$.

(vi) $cd_p(G)=0$ *if and only if* $p\nmid |G|$.

(vii) If $cd_p(G)\neq 0,\infty$, then $p^\infty \mid |G|$.

(viii) If G is a pro-p-group, then $cd_q(G)=0$ for every prime $q\neq p$.

(ix) If G is finite and $p\mid |G|$, then $cd_p(G)=\infty$.

(x) Assume $cd_p(G)<\infty$. If $H\leq G$ is a closed finite subgroup, then $p\nmid |G|$. In particular, G has no element of order p. Further, if G is a pro-p group, then it does not have any finite closed subgroups.

Proof. (1) If B is a discrete p-torsion H-module, then so is $M_H^G(B)$ by the definition of its elements. For $n>cd_p(G)$ we conclude using the Eckmann-Shapiro lemma that $H^n(G,M_H^G(B)) = H^n(H,B)=0$. Thus $cd_p(H)<n$.

(2) $cd_p(G)=n$. Then there is a discrete p-torsion module A such that $H^n(G,A)\neq 0$. The assumption on the index implies by proposition 4.5.1 that $res: H^n(G,A)\to H^n(H,A)$ is an injection. Consequently $H^n(H,A)\neq 0$, hence $cd_p(H)\geq n$.

(3) Follows immediately from (2).

(4) Let $cd_p(G) = n$ and A be a discrete p-torsion G-module with $H^n(G, A) \neq 0$. Fix coset representatives $\{g_1 = 1, g_2, \ldots, g_n\}$ and define G-homomorphisms

$$\alpha : M_H^G(A) \to A,\ f \mapsto \sum_{i=1}^{n} g_i^{-1} f(g_i) \quad \text{and} \quad \beta : A \to M_H^G(A),\ a \mapsto f_a,$$

where we set $f_a(1) = a$ and $f_a(g_i) = 0$ for $i = 2, \ldots, n$ and extend to cosets.

It is clear that these maps are well defined and that we have $\alpha \circ \beta = id_A$. Hence α is surjective.

Consider the short exact sequence

$$0 \to B \to M_H^G(A) \to A \to 0,$$

where the last map is given by α and B is the corresponding kernel. Now we have the following part of the long exact sequence

$$H^n(G, M_H^G(A)) \to H^n(G, A) \to H^{n+1}(G, A) = 0.$$

Since $H^n(G, A) \neq 0$, $H^n(G, M_H^G(A)) \neq 0$ and hence by the Eckmann-Shapiro lemma $H^n(H, A) \neq 0$ implying $cd_p(H) \geq n$.

(5) Assume $cd_p(G) = 0$. Consider $\mathbb{F}_p$ as a G-module under the trivial action. By remark 4.1.5 $H^1(G, \mathbb{F}_p) = 0$ means that there are no continuous homomorphisms $G \to \mathbb{F}_p$. This, however, is not true for $G \neq 1$: Let $U \in \mathcal{U}_G$, thus G/U is a finite p-group. It is a fact from finite group theory that a finite non-trivial p-group has a normal subgroup of index p. Take such $N \triangleleft (G/U)$. Consider $G \to G/U \to (G/U)/N = \mathbb{F}_p \to \mathbb{F}_p$, where the first two maps are the natural continuous projections, and the last is a non-trivial group homomorphism of $\mathbb{F}_p$.

(6) Let H be a p-Sylow subgroup of G, thus by (3) $cd_p(G) = cd_p(H)$. Furthermore, p does not divide the order of G if and only if $H = 1$. The result now follows from (5).

(7) - (10) follow immediately. □

Without proofs we list some examples.

4.6.9 Example.

- $cd_p(\mathbb{Z}_p) = 1$
- $cd_p(L) = n$ *for* $L = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ *with n factors ([16], 11.3.1)*
- $cd_p(\hat{\mathbb{Z}}) = 1$

We wish to mention at this stage the following important theorem by Serre.

4.6.10 Theorem. (Serre [12]) *Let G be a profinite group that does not contain any element of order p. Then for every open subgroup $U \leq G$ we have $cd_p(U) = cd_p(G)$.*

In view of (10) of the above proposition, the condition that G does not contain an element of order p is reasonable, as otherwise $cd_p(G) = \infty$.

An important application of this is to p-adic analytic groups (cf. Lazard [5]). We state the following corollary of Serre's theorem.

4.6.11 Corollary. (Serre, [12]) *Let G be a compact p-adic analytic group of dimension n and without an element of order p. Then $cd_p(G) = n$.*

This implies in particular the

4.6.12 Corollary. *Let $G = GL_d(\mathbb{Z}_p)$, where d and p are chosen such that G does not contain an element of order p. Then $cd_p(G) = d^2$.*

4.7. Euler-Poincaré characteristic and distribution

We now wish to define the Euler-Poincaré characteristic for a profinite group G. Fix a prime p. As G-modules we use the objects of $\mathcal{C}_{\mathbb{F}_p,G}$, i.e. $\mathbb{F}_p$-vector spaces with the discrete topology, on which G acts continuously.

(4.7.1) For the definition to make sense, we have to subject our profinite group G to a finiteness condition:
(i) $cd_p(G) < \infty$
(ii) $dim_{\mathbb{F}_p} H^n(G, A) < \infty$ for all $n \in \mathbb{N}$ and all $A \in \mathcal{C}_{\mathbb{F}_p,G}$

4.7.2 Remark. *Let $H \leq G$ be a closed subgroup. If G satisfies the finiteness conditions above, then so does H.*

Proof. (i) was proved in proposition 4.6.8. Let $A \in \mathcal{C}_{\mathbb{F}_p,H}$ be an H-module. Then the Eckmann-Shapiro lemma implies

$$H^n(G, M_H^G(A)) \cong H^n(H, A),$$

whence we conclude the finite dimensionality of $H^n(H, A)$. □

For $B \in \mathcal{C}_{\mathbb{F}_p,G}$ we note that B is finite and $pB = 0$. Hence proposition 4.6.7 implies that $H^n(G, B) = 0$ for all $n > cd_p(G)$.

Thus the sum in the following definition is finite.

4.7.3 Definition. *For a profinite group G subject to the above finiteness condition we define the Euler-Poincaré characteristic of $A \in \mathcal{C}_{\mathbb{F}_p,G}$ to be*

$$e(G, A) := \sum_i (-1)^i dim_{\mathbb{F}_p}(H^i(G, A)).$$

As announced earlier we have

4.7.4 Lemma. *The Euler-Poincaré characteristic $e(G, .)$ is an Euler-Poincaré map.*

Proof. Let $0 \to A \to B \to C \to 0$ be a short exact sequence of objects in $\mathcal{C}_{\mathbb{F}_p,G}$ (automatically well adjusted). We get the long exact sequence

$$\cdots \to H^n(G, A) \to H^n(G, B) \to H^n(G, C) \to H^{n+1}(G, A) \to \ldots$$

and therefore e.g. by splitting it

$$0 = \sum_i (-1)^i (dim_{\mathbb{F}_p} H^i(G, A) - dim_{\mathbb{F}_p} H^i(G, B) + dim_{\mathbb{F}_p} H^i(G, C)).$$

This immediately gives:

$$e(G, B) = e(G, A) + e(G, C)$$

□

We can now apply theorem 3.5.10 to get the first main theorem from [9].

4.7.5 Theorem. *For a profinite group G subject to the finiteness condition 4.7.1 there is one and only one distribution $\mu_G \in \mathcal{D}_G$ such that*

$$e(G, A) = < \phi_A, \mu_G > \quad \forall A \in \mathcal{C}_{\mathbb{F}_p,G}.$$

We call μ_G the **Euler-Poincaré distribution**.

5. p-adic cohomology of profinite groups

5.1. Cohomology with coefficients in $\mathbb{Z}_p$-modules

Up to now we have only considered cohomology with coefficients in discrete modules. We will now extend (parts of) the theory to $\mathbb{Z}_p$-modules.

Let $L \in \mathcal{M}_{\mathbb{Z}_p,G}$ be a finitely generated $\mathbb{Z}_p$-module equipped with the p-adic topology and G a profinite group, which acts on L continuously and $\mathbb{Z}_p$-linearly. We have already defined the cohomology groups $H^n(G,L)$ in 4.1 and remarked (4.1.8) that long exact sequences exist for every short one.

For the rest of this chapter we insist that G satisfies:

$$dim_{\mathbb{F}_p}(H^n(G,A)) < \infty \ \ \forall\, n \in \mathbb{N} \ \ \forall\, A \in \mathcal{C}_{\mathbb{F}_p,G}$$

Under this hypothesis we can state a useful equivalent formulation of the cohomology groups. First, however, we introduce some technical notation (cf. [3], 13.1).

5.1.1 Definition. *Let (A_i, f_{ij}) be a projective system of topological groups with its indices being natural numbers. It satisfies the* **Mittag-Leffler property**, *if for all $n \in \mathbb{N}$ there is $m \geq n$ such that for all $k \geq m$ $f_{nk}(A_k) = f_{nm}(A_m)$.*

5.1.2 Lemma. *(i) The projective system of complexes of abelian groups $C^\bullet(G, L/p^nL)$ satisfies the Mittag-Leffler property.*

(ii) Let $i \in \mathbb{N}$. The projective system $H^i(G, L/p^nL)$ satisfies the Mittag-Leffler property.

Proof. For (1) we remark that the maps

$$C^i(G, L/p^mL) \to C^i(G, L/p^nL),\ f \mapsto \pi_{n,m} \circ f$$

are surjective, where $\pi_{n,m}$ is the natural projection $L/p^mL \to L/p^nL$.

(2) Our finiteness assumption implies that $H^i(G, L/p^nL)$ are finite for all $i, n \in \mathbb{N}$.

In general, the Mittag-Leffler property is satisfied if all groups concerned are finite. This can be seen using a combinatorial argument. We use the notation of the preceding definition.

Given $n \in \mathbb{N}$, put $A := A_n$. For every element $a \in A$ either of the following is true: (i) there is $m_a > n$ such that $a \notin f_{m_a n}(A_{m_a})$ or (ii) for all $k > n$ $a \in f_{kn}(A_k)$. Let m be the maximum of the m_a's from (i). Then $f_{mk}(A_k)$ is surjective for all $k > m$, and m satisfies the requirements. □

Now we can prove the reformulation mentioned.

5.1.3 Proposition.

$$H^i(G,L) = \varprojlim H^i(G, L/p^nL),$$

where the projective limit is taken over $n \in \mathbb{N}$.

Proof. We have $L = \varprojlim L/p^nL$, the limit being taken for the natural projections $L/p^mL \to L/p^nL$ for $m \geq n$ and $n, m \in \mathbb{N}$. A map f from a topological space X to L is continuous, if and only if $\pi_n \circ f$ is continuous for all $n \in \mathbb{N}$, where $\pi_n : L \to L/p^nL$ is the natural projection. Hence

$$C^i(G,L) = \varprojlim C^i(G, L/p^nL).$$

Having established this, the above lemma contains the conditions necessary for applying [3], 13.2.3., resulting in

$$H^i(G,L) = \varprojlim H^i(G, L/p^nL).$$

□

By our finiteness assumption, the $H^i(G, L/p^nL)$ are finite dimensional vector spaces over $\mathbb{F}_p$ and hence p-groups. Consequently, $H^i(G, L)$ is an abelian pro-p-group.

5.1.4 Proposition. *The $H^i(G, L)$ are finitely generated $\mathbb{Z}_p$-modules.*

Proof.

- Denote by L_{tor} the torsion submodule of L and consider the short exact sequence $0 \to L_{tor} \to L \to L/L_{tor} \to 0$. This gives the long exact sequence

$$\begin{array}{rcccl} \cdots \to & H^{n-1}(G, L/L_{tor}) & \to & H^n(G, L_{tor}) & \to \\ \to & H^n(G, L) & \to & H^n(G, L/L_{tor}) & \to \ldots \end{array}$$

  Since L is finitely generated, L_{tor} is finite. If L_{tor} in addition is simple, then by remark 4.6.5 $pL_{tor} = 0$ and thus it is an $\mathbb{F}_p$-vector space. The finiteness assumption implies in this case that $H^n(G, L_{tor})$ is finite. By induction on the length of a composition series of a general L_{tor}, using the short exact sequence $0 \to M \to L_{tor} \to L_{tor}/M \to 0$ and its associated long one, we conclude that $H^n(G, L_{tor})$ is finite.

  Now assume that $H^n(G, L/L_{tor})$ is finitely generated. Then we conclude from the long exact sequence above that $H^n(G, L)$ is finitely generated.

  This reduces us to show that $H^n(G, L)$ is a finitely generated $\mathbb{Z}_p$-module for every torsion free L.

- Now assume L is torsion free. We therefore have the short exact sequence $0 \to L \to L \to L/pL \to 0$, where the first map is multiplication by p. The associated long exact sequence is

$$\cdots \to H^n(G, L) \to H^n(G, L) \to H^n(G, L/pL) \to \ldots,$$

  where the first map is multiplication by p of n-cochains.

  By our finiteness assumption $H^n(G, L/pL)$ is finite and thus H^n/pH^n is, too, for $H^n := H^n(G, L)$.

  The result now follows from the following lemma. □

5.1.5 Lemma. *Let L be a $\mathbb{Z}_p$-module such that L/pL is finite and thus a finite dimensional $\mathbb{F}_p$-vector space. Then $rk_{\mathbb{Z}_p}(L) \leq dim_{\mathbb{F}_p}(L/pL)$.*

Proof. Let $\{l_1, \ldots, l_n\}$ be a $\mathbb{Z}_p$-linearly independent subset of L. Assume $0 = \sum_i a_i \overline{l_i}$ with $a_i \in \mathbb{F}_p$ and with $\overline{x}$ denoting the reduction modulo p of x. Take $b_i \in \mathbb{Z}_p$ with $\overline{b_i} = a_i$. Then $\sum_i b_i l_i \in pL$, hence there are $c_i \in \mathbb{Z}_p$ with $\sum_i (b_i - pc_i) l_i = 0$. Thus $b_i = pc_i$, whence $b_i \in (p)$ and $a_i = 0$. □

5.1.6 Remark. *For $n > cd_p(G)$ we have $H^n(G, L) = 0$.*

Proof. By the last proposition $H^i(G, L) = \varprojlim H^i(G, L/p^nL) = \varprojlim 0 = 0$. □

5.2. Cohomology with coefficients in $\mathbb{Q}_p$-vector spaces

Let V be a finite dimensional $\mathbb{Q}_p$-vector space with $\mathbb{Q}_p$-linear continuous action by the profinite group G.

Again under the finiteness assumption from the last section we establish a reformulation of $H^n(G, V)$.

By proposition 3.3.4 we can choose a G-stable $\mathbb{Z}_p$-lattice L for V, i. e. $V = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L$.

5.2.1 Proposition. *For every $n \in \mathbb{N}$ we have*

$$H^i(G,V) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^i(G,L).$$

Proof. We have $V = \bigcup_n p^{-n}L$. Let $f : G^i \to V$ be a continuous map. Then $G^i = \bigcup_n f^{-1}(p^{-n}L)$ is an open covering. As G is compact, for every f there is an $n \in \mathbb{N}$ such that $f : G^i \to p^{-n}L$ is continuous. Hence $p^n f : G^i \to L$ is continuous.

Further, f is a cocycle (coboundary) if and only if $p^n f$ is a cocycle (coboundary). Hence $H^i(G,V) = \bigcup_n p^{-n}H^i(G,L) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^i(G,L)$. □

5.2.2 Remark. *For $n > cd_p(G)$ we have $H^n(G,V) = 0$.*

Proof. By remark 5.1.6 and last proposition

$$H^n(G,V) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^n(G,L) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} 0 = 0.$$

□

As for every $\mathbb{Z}_p$-module A its rank is equal to the dimension of the $\mathbb{Q}_p$-vector space $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} A$, we can conclude from proposition 5.1.4 the following

5.2.3 Remark. $dim_{\mathbb{Q}_p}(H^n(G,V)) = rk_{\mathbb{Z}_p}(H^n(G,L)) < \infty$

5.2.4 Lemma. *Let G act trivially on $\mathbb{Q}_p$. Then G acts trivially on V and*

$$H^i(G,V) = V \otimes_{\mathbb{Q}_p} H^i(G,\mathbb{Q}_p).$$

Proof. Let $g \in G$ and $v \in V$. For all $x \in \mathbb{Q}_p$ we have by the linearity of the G-action $x(gv) = g(xv) = (gx)v = xv$. Hence $gv = v$.

Choose a $\mathbb{Q}_p$-basis $\{v_1, \ldots, v_n\}$ of V. Let $f : G^i \to V$. We can write it uniquely as $f = \sum_{j=1}^n f_j v_j$ with $f_j : G^i \to \mathbb{Q}_p$. Due to the trivial action f is a cocycle (coboundary) if and only if each f_j is for the complex $C^i(G,\mathbb{Q}_p)$. Hence the result. □

5.3. Euler-Poincaré characteristic and distribution

We can now define the Euler-Poincaré characteristic for cohomology with coefficients in $\mathbb{Z}_p$- and $\mathbb{Q}_p$-modules and express it as a distribution.

We must, however, again impose the finiteness condition 4.7.1.

We first prove a general

5.3.1 Lemma. *Let L be a finitely generated $\mathbb{Z}_p$-module and consider the map $\phi : L \to L, l \mapsto pl$. Denote its kernel by L_p. Then*

$$rk_{\mathbb{Z}_p}(L) = dim_{\mathbb{F}_p}(L/pL) - dim_{\mathbb{F}_p}(L_p).$$

Proof.

- We first note that for $\mathbb{Z}_p$-modules the terms "free", "torsion free" and "p-torsion free" are equivalent; the first equivalence being a general fact for modules over principal ideal domains and the second because every element in $\mathbb{Z}_p - (p)$ is a unit. Also L_p is an $\mathbb{F}_p$-vector space.
- <u>case 1:</u> L p-torsion module
  We show: $dim_{\mathbb{F}_p}(L/pL) = dim_{\mathbb{F}_p}(L_p)$

  Suppose first that L is simple. By remark 4.6.5 we know that $pL = 0$. Thus $L_p = L$ and $L/pL = L$, yielding the result in this special case.

Next we proceed by induction on the length of a composition series of L. Let $M \leq L$ be a proper non-zero submodule. We have the following two $\mathbb{F}_p$-vector space isomorphisms: $L_p/M_p \cong (L/M)_p$ and $(L/pL)/(M/pM) \cong (L/M)/p(L/M)$. Hence

$$\begin{array}{rcccl} dim_{\mathbb{F}_p}(L_p) & = & dim_{\mathbb{F}_p}(M_p) & + & dim_{\mathbb{F}_p}((L/M)_p) \\ dim_{\mathbb{F}_p}(L/pL) & = & dim_{\mathbb{F}_p}(M/pM) & + & dim_{\mathbb{F}_p}((L/M)/p(L/M)), \end{array}$$

which implies the result.

- <u>case 2:</u> L (torsion) free module
  We show $rk_{\mathbb{Z}_p} L = dim_{\mathbb{F}_p}(L/pL)$.

  In lemma 5.1.5, we have shown $rk_{\mathbb{Z}_p} L \leq dim_{\mathbb{F}_p} L/pL$.

  Let now $\{\overline{l_1}, \ldots, \overline{l_r}\}$ be an $\mathbb{F}_p$-basis of L/pL. Suppose $0 = \sum_i a_i l_i$ with $a_i \in \mathbb{Z}_p$ not all 0. Thus $0 = \sum_i \overline{a_i}\overline{l_i}$ and hence $a_i \in (p)$ for all i. Choose the integer t maximal such that $a_i = p^t s_i$ for $s_i \in R$. In particular, there is an index j with $s_j \notin (p)$. We have $0 = p^t \sum_i s_i l_i$ and as L is free, $0 = \sum_i s_i l_i$, from which we conclude as above, that for all i $s_i \in (p)$. Contradiction.

- <u>general case:</u>
  We can write $L = L_{tor} \oplus F$ with L_{tor} a torsion module and F free.

$$\begin{aligned} dim_{\mathbb{F}_p}(L/pL) &= dim_{\mathbb{F}_p}(L \otimes_{\mathbb{Z}_p} \mathbb{F}_p) = dim_{\mathbb{F}_p}((L_{tor} \oplus F) \otimes_{\mathbb{Z}_p} \mathbb{F}_p) \\ &= dim_{\mathbb{F}_p}(L_{tor} \otimes_{\mathbb{Z}_p} \mathbb{F}_p) + dim_{\mathbb{F}_p}(F \otimes_{\mathbb{Z}_p} \mathbb{F}_p) \\ &= dim_{\mathbb{F}_p}(L_{tor}/pL_{tor}) + dim_{\mathbb{F}_p}(F/pF) \\ &= dim_{\mathbb{F}_p}((L_{tor})_p) + dim_{\mathbb{F}_p}(F/pF) \end{aligned}$$

  Hence

$$rk_{\mathbb{Z}_p}(L) = rk_{\mathbb{Z}_p}(F) = dim_{\mathbb{F}_p}(F/pF) = dim_{\mathbb{F}_p}(L/pL) - dim_{\mathbb{F}_p}(L_p).$$

□

5.3.2 Proposition. *Suppose that L is torsion free. Then*

$$\sum_i (-1)^i \, rk_{\mathbb{Z}_p}(H^i(G, L)) = \sum_i (-1)^i \, dim_{\mathbb{F}_p}(H^i(G, L/pL)) = e(G, L/pL).$$

Proof.

- Since L is torsion free, we have the short exact sequence

$$0 \to L \to L \to L/pL \to 0,$$

  where the first map is multiplication by p. Therefore there is the long exact sequence

$$\begin{array}{rlll} \cdots \to & H^i(G, L) & \to H^i(G, L) & \to H^i(G, L/pL) \to \\ \to & H^{i+1}(G, L) & \to H^{i+1}(G, L) & \to \ldots, \end{array}$$

  where the first and the last map are also multiplication by p (of the cochains).

- Write $H^i := H^i(G, L)$. Introducing $H_p^{i+1} := ker(H^{i+1} \to H^{i+1})$ (multiplication by p), which is by exactness the image of the connecting homomorphism, we receive short exact sequences

$$0 \to H^i/pH^i \to H^i(G, L/pL) \to H_p^{i+1} \to 0.$$

- We make a brief calculation:

$$\begin{aligned} e(G, L/pL) &= \sum_i (-1)^i \, dim_{\mathbb{F}_p}(H^i(G, L/pl)) && (1)\\ &= \sum_i (-1)^i \, (dim_{\mathbb{F}_p}(H^i/pH^i) + dim_{\mathbb{F}_p}(H_p^{i+1})) && (2)\\ &= \sum_i (-1)^i \, (dim_{\mathbb{F}_p}(H^i/pH^i) - dim_{\mathbb{F}_p}(H_p^i)) && (3)\\ &= \sum_i (-1)^i \, rk_{\mathbb{Z}_p}(H^i) && (4) \end{aligned}$$

We have reordered the (finite) sum to get from (2) to (3) and have applied the lemma above for (3) $\Rightarrow$ (4).

□

With this proposition, the fact that $\mathbb{Z}_p$-lattices are free (remark 3.3.3) and the equality $dim_{\mathbb{F}_p}(H^i(G, V)) = rk_{\mathbb{Z}_p}(H^i(G, L))$ in mind, we make the following

5.3.3 Definition. • *Let L be a torsion free $\mathbb{Z}_p$-module, on which G acts continuously. Define the* **Euler-Poincaré characteristic** *of L to be*

$$e(G, L) := \sum_i (-1)^i \, rk_{\mathbb{Z}_p}(H^i(G, L)).$$

- *Let V be a $\mathbb{Q}_p$-vector space, on which G acts $\mathbb{Q}_p$-linearly and continuously. Set*

$$e(G, V) := \sum_i (-1)^i \, dim_{\mathbb{F}_p}(H^i(G, V)).$$

Note that by remarks 5.1.6 and 5.2.2, all sums appearing are finite under the conditions on G.

We can now rewrite this in terms of the Euler-Poincaré distribution μ_G introduced in section 4.7.

5.3.4 Corollary. *In the notation of the definition we have*

- $e(G, L) =< \chi_L|_{G_{reg}}, \mu_G >$
- $e(G, V) =< \chi_V|_{G_{reg}}, \mu_G >$

Proof. By corollary 3.3.9 we have $\chi_L(g) = \chi_V(g) = \phi_{d(V)}(g)$ for all $g \in G_{reg}$. The rest is clear by the remarks made above. □

5.4. Relating Euler-Poincaré distribution to $H^i(U, \mathbb{Q}_p)$

Let G be a profinite group satisfying the finiteness conditions 4.7.1. Then so does every closed subgroup (by remark 4.7.2). Let $U \in \mathcal{U}_G$ act trivially (hence also continuously) on $\mathbb{Q}_p$.

In this section we study

$$H_U^i := H^i(U, \mathbb{Q}_p),$$

which are finite dimensional $\mathbb{Q}_p$-vector spaces (by remark 5.2.3). We will relate them to the Euler-Poincaré distribution.

In 4.5 we defined an action of G/U on $H^i(U, A)$ by inner automorphisms of G on U. Using

$$H^i(U, V) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \varprojlim H^i(U, L/p^n L),$$

we extend this action to the case of a $\mathbb{Q}_p$-vector space V with $\mathbb{Z}_p$-lattice L, on which G acts $\mathbb{Q}_p$-linearly and continuously.

By the same means we define a corestriction. It is clear that proposition 4.5.1 stays valid.

5.4.1 Lemma. *Let $U \in \mathcal{U}_G$. Then*

$$H^i(G,V) = H^i(U,V)^{G/U}.$$

Proof. As V as a vector space is torsion free, so are $H^i(G,V)$, $H^i(U,V)^{G/U}$. From proposition 4.5.1 we thus get that $res : H^i(G,V) \to H^i(U,V)^{G/U}$ and $cor : H^i(U,V)^{G/U} \to H^i(G,V)$ are injective. Hence the lemma. □

Consider the special case $V = \mathbb{Q}_p$. The H^i's are finite dimensional representations of G/U. Denote by h^i_U their characters and put

$$h_U := \sum_i (-1)^i \, h^i_U.$$

This has the striking consequence that we can calculate the Euler-Poincaré distribution for $\mathbb{Q}_p$-vector spaces alone from the knowledge of the h_U's.

5.4.2 Theorem. (Serre [9]) *Let $f : G_{reg} \to \mathbb{Q}_p$ be a function, which is locally constant modulo $U \in \mathcal{U}_G$. Then*

$$< f, \mu_G >= \frac{1}{(G:U)} \sum_{s \in G/U} h_U(s) f(s),$$

where we take $f(s) = 0$ for $s \notin G_{reg}$.

Proof.

- Take V as above. By definition we have

$$< \chi_V|_{G_{reg}}, \mu_G >= \sum_i (-1)^i \, dim_{\mathbb{Q}_p}(H^i(G,V)).$$

- Lemma 5.2.4 implies that the representation of G/U on $H^i(U,V)$ has character $h^i_U \chi_V$.

- Using lemma 5.4.1 for the first equality and a simple fact from the representation theory of finite groups for the second, we have

$$dim(H^i(G,V)) = dim(H^i(U,V)^{G/U}) = \frac{1}{(G:U)} \sum_{s \in G/U} h^i_U(s) \chi_V(s).$$

- Taking the alternating sum of these terms, we receive

$$< \chi_V|_{G_{reg}}, \mu_G >= \frac{1}{(G:U)} \sum_{s \in G/U} h_U(s) \chi_V(s).$$

- By remark 3.4.10 we can write $f : G_{reg} \to \mathbb{Q}_p$, which we extend as zero to all of G, as a linear combination of $\chi_{e(P_S)}$ for $S \in \Sigma_{\mathbb{F}_p,G}$. This completes the proof.

□

From remark 3.5.9 we immediately receive the

5.4.3 Corollary. (Serre [9]) *$h_U(s) = 0$ for $s \notin G_{reg}$.*

5.4.4 Corollary. (Serre [9]) *If $H \leq G$ is an open subgroup of G, then*

$$\mu_H = (G:H) \mu_G|_H.$$

Proof. We have to show

$$< f, \mu_H >= (G : H) < f, \mu_G >$$

for all $f : H_{reg} \to \mathbb{Q}_p$ (we take f to be zero outside H_{reg}).

Let $U \in \mathcal{U}_G$, $U \subseteq H$ such that f is constant modulo U. From the theorem we now receive the following formulae:

$$< f, \mu_G >= \frac{1}{(G : U)} \sum_{s \in G/U} h_U(s) f(s)$$

$$< f, \mu_H >= \frac{1}{(H : U)} \sum_{s \in H/U} h_U(s) f(s)$$

We have used that the action of H/U on $H^i(U, \mathbb{Q}_p)$ is the restriction of the one of G/U. We now immediately see, using $(G : U) = (G : H)\ (H : U)$, that

$$\begin{aligned} < f, \mu_G > &= \tfrac{1}{(G:H)} \tfrac{1}{(H:U)} \textstyle\sum_{s \in H/U} h_U(s) f(s) \\ &= \tfrac{1}{(G:H)} < f, \mu_H > . \end{aligned}$$

□

5.4.5 Corollary. *Let $H \in \mathcal{U}_G$ such that $(G : H) = p^r$. Then*

$$e(H, A) = p^r e(G, A)$$

for all $A \in \mathcal{C}_{\mathbb{F}_p, G}$.

This corollary is a generalization of the respective result for a pro-p-group G, as proved e.g. in [7], IV.5.2.

Proof. Since $(G : H) = p^r$, $G_{reg} = H_{reg}$. Let $A \in \Sigma_{\mathbb{F}_p, G}$. Via the natural injection $H \hookrightarrow G$, we can regard A as an H-module A_H, which is also simple.

Thus the Brauer characters ϕ_A and ϕ_{A_H} are the same. By definition we have $e(H, A) =< \phi_{A_H}, \mu_H >$ and $e(G, A) =< \phi_A, \mu_G >$. The last corollary now implies the result. □

6. Applications to Galois cohomology

6.1. Euler-Poincaré distribution of a p-adic field

In this section we state the Euler-Poincaré distribution of the Galois group of a p-adic number field. The result was originally obtained by Tate (cf. [14]).

Let $K/\mathbb{Q}_p$ be a finite extension of degree d. Set $G = G(\overline{K}/K)$, where $\overline{K}$ denotes an algebraic closure of K.

We have the following important

6.1.1 Proposition. $cd_p(G) = 2$

Proof. [8], Corollary II.4.3 □

This, together with theorem 2.1 in [14], implies that the finiteness conditions 4.7.1 necessary for the definition of the Euler-Poincaré characteristic are satisfied.

We can now state the

6.1.2 Theorem. *Let G be as above. Then*

$$\mu_G = -d\ \delta_1,$$

where δ_1 denotes the Dirac distribution of the unit element.

As announced, we shall not prove the theorem here. We will, however, conclude it from the following proposition, for the proof of which we refer to [9], proposition 6.2.1.

6.1.3 Proposition. *Let $G = G(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. For all $U \in \mathcal{U}_G$ we have*

$$h_U^0 = 1,\ \ h_U^1 = 1 + r_{G/U},\ \ h_U^2 = 0,$$

where $r_{G/U}$ denotes the character of the regular representation of G/U.

Proof of the theorem. Consider first $G = G(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ as in the proposition. The proposition now implies $h_U = h_U^0 - h_U^1 + h_U^2 = -r_{G/U}$. Thus $h_U(1) = -(G:U)$ and $h_U(s) = 0$ for $s \neq 1$.

Take $f : G \to \mathbb{Q}_p$, which is constant modulo $U \in \mathcal{U}_G$. By theorem 5.4.2 we have

$$< f, \mu_G > = \frac{1}{(G:U)} \sum_{s \in G/U} h_U(s) f(s) \ = \ -f(1) \ = < f, -\delta_1 > .$$

This clearly proves the theorem in the special case.

For the general case we observe that $G_K = G(\overline{\mathbb{Q}_p}/K)$ has index d in $G_{\mathbb{Q}_p} = G(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. Corollary 5.4.4 now implies

$$\mu_{G_K} = d\ \mu_{G_{\mathbb{Q}_p}} = -d\ \delta_1.$$

□

6.2. Euler-Poincaré distribution for a number field

In the last section we treated the "local" case of a p-adic field. Here we give an account of another result by Tate (cf. [15]) for a number field, the "global" case.

Let $K/\mathbb{Q}$ be a number field of degree d. Fix a prime p. Further consider a finite set S of places of K, containing all archimedean places and all places, whose residue class fields have characteristic p. This allows us to study K_S, the maximal Galois extension of K, which is unramified outside S, i. e. for all places not in S. Put $G = G(K_S/K)$.

In [9], 6.3, we find the following

6.2.1 Proposition. *If $p \neq 2$ or K is totally imaginary (i. e. K cannot be embedded into $\mathbb{R}$), then $cd_p(G) = 2$.*

Moreover, theorem 3.1 in [14], implies that the finiteness condition 4.7.1 is also satisfied in this situation, so that it makes sense to define the Euler-Poincaré characteristic.

According to [9], 6.3, theorem 2.2 of [15], can be stated as follows.

6.2.2 Theorem. *Let G be as above and $A \in \mathcal{C}_{\mathbb{F}_p,G}$. Then the Euler-Poincaré characteristic is given by*

$$e(G, A) = \sum_{v \ arch} e_v(A).$$

For an archimedean place v we use following the notations.

- *If v is a complex place, set $e_v(A) = -dim(A)$.*
- *If v is a real place, denote by $c_v \in G$ the Frobenius automorphism corresponding to it. Further let A_v denote the submodule of A fixed by c_v. Put $e_v(A) = dim(A_v) - dim(A)$.*

For this we will prove a reformulation in terms of the Euler-Poincaré distribution.
First, however, we have to provide one more

6.2.3 Definition. *Consider two totally disconnected topological spaces X and Y, and a continuous map $h : X \to Y$.*

Let μ be a distribution on X (with values in some commutative ring), cf. section 3.5. By the **image $h\mu$** *of μ w.r.t. h we mean the distribution on Y given by*

$$< f, h\mu >:=< f \circ h, \mu >$$

for all functions f on Y.

Let v be a real archimedean place with Frobenius c_v as above. Consider the continuous map

$$h_v : G \to G,\ g \mapsto g^{-1} c_v g.$$

We denote by μ_v the image of the Haar distribution w.r.t h_v. For $f : G \to \mathbb{Q}_p$, which is constant modulo $U \in \mathcal{U}_G$, this gives explicitly:

$$< f, \mu_v > = < f \circ h_v, \mu_{Haar} > = \frac{1}{(G : U)} \sum_{s \in G/U} f(s^{-1} c_v s)$$

If in particular f is a class function, then this becomes

$$< f, \mu_v >= f(c_v).$$

6.2.4 Theorem. *For G as above, we have*

$$\mu_G = -\frac{d}{2}\delta_1 + \frac{1}{2} \sum_{v \ real} \mu_v.$$

Proof.

- Denote by ϕ_A the Brauer character of A. Thus $dim(A) = \phi_A(1)$. As A_v is the submodule of A fixed by c_v, which has order 2, (7) of proposition 3.2.11 implies $dim(A_v) = \frac{1}{2}(\phi_A(1) + \phi_A(c_v))$.

- For a place v we have by [6], Korollar 8.4,

$$[K:\mathbb{Q}] = \sum_{w|v} [K_w : \mathbb{Q}_v],$$

where w runs through all places over v. Applying this to the only archimedean place ∞ of $\mathbb{Q}$ we see

$$d = [K:\mathbb{Q}] = \sum_{w \text{ arch}} [K_w : \mathbb{R}] = \sum_{w \text{ compl}} 2 + \sum_{w \text{ real}} 1.$$

- The theorem above implies:

$$\begin{array}{rcl} e(G,A) & = & \sum_{v \text{ arch}} e_v(A) \\ & = & \sum_{v \text{ arch}} -\phi_A(1) + \sum_{v \text{ real}} \frac{1}{2}(\phi_A(1) + \phi_A(c_v)) \\ & = & -\frac{1}{2}\phi_A(1)(\sum_{v \text{ compl}} 2 + \sum_{v \text{ real}} 1) + \frac{1}{2}\sum_{v \text{ real}} \phi_A(c_v) \\ & = & -\frac{d}{2}\phi_A(1) + \frac{1}{2}\sum_{v \text{ real}} \phi_A(c_v) \\ & = & -\frac{d}{2}\delta_1(\phi_A) + \frac{1}{2}\sum_{v \text{ real}} \mu_v(\phi_A) \end{array}$$

□

References

[1] Curtis, C. and Reiner, I. *Methods of Representation Theory with Applications to Finite Groups and Orders,* Volume I, John Wiley & Sons, 1981

[2] Dixon, J. D., Du Sautoy, M.P.F., Mann, A., Segal, D. *Analytic Pro-p Groups,* 2nd Edition, Cambridge studies in advanced mathematics 61, Cambridge University Press, 1999

[3] Grothendieck, A. *Eleménts de Géométrie Algébrique,* Chapitre 0, Publ. Math. IHES 11, 1961

[4] Lang, S. *Algebra,* 3rd Edition, Addison-Wesley, 1993

[5] Lazard, M., *Groupes analytiques p-adiques,* Publ. Math. IHES 26, 1965

[6] Neukirch, J. *Algebraische Zahlentheorie,* Springer-Verlag, 1992

[7] Ribes, L., *Introduction to Profinite Groups and Galois Cohomology,* Queen's Papers in Pure and Applied Mathematics - No. 24, 1970

[8] Serre, J.-P., *Galois Cohomology,* Springer-Verlag, 1997

[9] Serre, J.-P., *La distribution d'Euler-Poincaré d'un groupe profini* in *Galois Representations in Arithmetic Algebraic Geometry,* pp. 461 – 493, edited by A. J. Scholl and R. L. Taylor, Cambridge University Press, 1998

[10] Serre, J.-P., *Local Fields,* GTM 67, Springer-Verlag, 1979

[11] Serre, J.-P., *Linear Representations of Finite Groups,* GTM 42, Springer-Verlag, 1977

[12] Serre, J.-P., *Sur la dimension cohomolgique des groupes profinis,* in Topology 3, 1965

[13] Tate, J., *Relations between K_2 and Galois Cohomology,* Inventiones Mathematicae 36, pp. 257-274, 1976

[14] Tate, J., *Duality theorems in Galois cohomology over number fields,* Proc. Int. Congress Stockholm, pp. 288-295, 1962

[15] Tate, J., *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog,* Séminaire Bourbaki 306, 1965/1966

[16] Wilson, J. *Profinite Groups,* London Mathematical Society Monographs, New Series 19, Oxford University Press, 1998