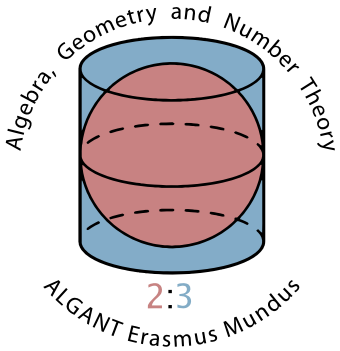
On Galois extensions generated by radicals

Zordan, M.

Michele Zordan
July 5, 2010

On Galois extensions generated by radicals



Master's thesis defended on June 28, 2010.
Written under the supervision of
Prof. Hendrik Lenstra

Mathematisch Instituut
Universiteit Leiden

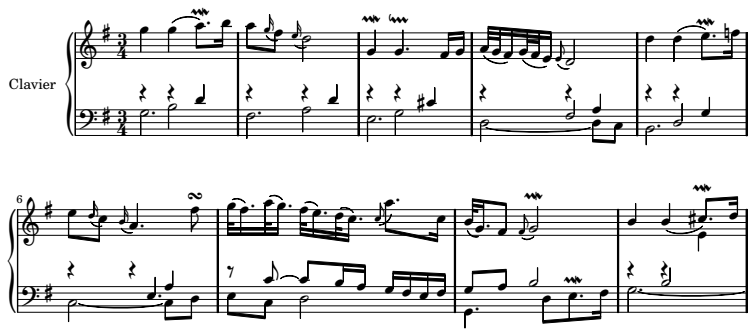
Facoltà di Scienze MM.FF.NN.
Università degli Studi di Padova

Aria con 30 Variazioni

"Goldbergsche Variationen"

Johann Sebastian Bach (1685-1750)

Aria BWV 988



Contents

Introduction

In this report we shall prove the following theorem.

THEOREM 1. *Consider a field K and $n = p^k$ for p a prime number and $k \in \mathbb{Z}_{>0}$. Let $E \supseteq K$ be a finite Galois extension of K such that the subgroup $\mu \subseteq E^*$ of all n-th roots of 1 has order n. Let $G = \mathrm{Gal}(E/K)$. We define two sets:*

$$S_1 = \{ghg^{-1}h^{-i} | g, h \in G,\ i \in \mathbb{Z},\ h(\zeta) = \zeta,\ g(\zeta) = \zeta^i \text{ for all } \zeta \in \mu)\},$$
$$S_2 = \{g^2 | g \in G,\ g(\zeta) = \zeta^{-1} \text{ for all } \zeta \in \mu)\}.$$

Let L be the largest intermediate field between K and E generated by n-th radicals of K, i.e.

$$L = K(\alpha \in E^* | \alpha^n \in K).$$

Then:

$$\mathrm{Gal}(E/L) = \langle S_1 \rangle \cdot \langle S_2 \rangle.$$

Given a field K, a Galois extension $E \supseteq K$ and $n \in \mathbb{Z}$, we say that $\alpha \in E^*$ is an n-th radical of K when $\alpha^n \in K$.
Problems in Galois theory can be approached either from the field-theoretic point of view or from the group-theoretic side. We shall choose the second; we shall look for a purely group-theoretical criterion to decide whether a certain extension is generated by n-th radicals of the base field. Equivalently, we shall try to decide whether the extension E is the splitting field of a *collection* of polynomials $\{x^n - a_i\}_{i \in I}$ with $a_i \in K$. In the end this quest for a criterion will allow us find a generating set for the Galois group of the largest intermediate field generated by radicals, as Theorem 1 shows. The pivot of the discussion will be the link between the group of n-th radicals and the group of cocycles $\mathrm{Z}^1(G, \mu)$, defined in 1.4. Namely, we will base our discussion on the following.

PROPOSITION 2. *Consider a field K and $n \in \mathbb{Z}_{>0}$. Let $L \supseteq K$ be a finite Galois extension of K such that the subgroup $\mu \subseteq L^*$ of all n-th roots of 1 has order n. Then, the extension L is the splitting field of a* collection *of polynomials $\{x^n - a_i\}_{i \in I}$ with $a_i \in K$* if and only if

$$\bigcap_{c \in \mathrm{Z}^1(G,\mu)} \ker c = \{1\}.$$

We will first forget about the Galois problem and we will concentrate on collecting sufficient wisdom about cocycles. The first chapter is devoted to this task; more explicitly, we will link the condition appearing in Proposition 2 with the splitting of certain exact sequences. The natural tool in this situation, then, will be the second cohomology group $\mathrm{H}^2(\Gamma, \mu)$ where $\Gamma = \mathrm{Gal}(K(\mu)/K)$, or more in general $\Gamma \leq \mathrm{Aut}(\mu)$. In this context we will see a beautiful description of Tate cohomology groups of a certain type of modules. That is, we shall prove the following theorem.

THEOREM 3. *Let μ be a cyclic group of order $n = p^k$ where p is a prime number and $k \in \mathbb{Z}_{>0}$, and $\Gamma \leq \mathrm{Aut}(\mu)$.*

1. *If* $n = 2^k$ *with* $k \geq 2$ *and there is* $g \in \Gamma$ *such that* $g(\zeta) = \zeta^{-1}$ *for all* $\zeta \in \mu$*; then* $\hat{\mathrm{H}}^q(\Gamma, \mu)$ *has order* 2 *for all* $q \in \mathbb{Z}$.
2. *Otherwise* μ *is* cohomologically trivial *as a* Γ*-module.*

These cohomology groups have already been computed in [**3**] (see page 453). However the theorem appearing there is not correct, namely the case of non-trivial cohomology is wider than how it is described in [**3**].
In the second chapter, we shall use results from the first chapter. We shall prove Proposition 2 here above and finally we will be able to prove the above mentioned theorem. As a pleasant detour, we shall see a corrected version of the aforesaid theorem in [**3**]. That correction is put there because the statement of the corrected theorem will refer to fields, while the first chapter is only about group theory.
We will also set a step forward towards dropping the hypothesis of n being a power of a prime. Concerning this point, it must be said that, once dropped the hypothesis of n being a power of a prime, we shall not have anymore a generating set for the Galois group $\mathrm{Gal}(E/L)$ as in Theorem 1, this leaves spaces to further investigation.
The very last section will contain a generalization of the main theorem to infinite Galois extensions; thus profinite groups will be called in.

Regarding what is needed to understand this report: we shall try to set our notation defining all important objects we will need. For reasons of briefness we will avoid to give the definitions of cohomology groups and Tate cohomology groups, however all what we need is easily recovered from [**1**] and [**7**]. For the last section, but only for it, a bit of infinite Galois theory is needed. We shall refer to [**4**].

In the end, I am really grateful to my advisor prof. Hendrik W. Lenstra, for his crucial advices, and for his wittiness in finding my mistakes, I also thank him for his endless patience and care in reading my drafts many times, and for his ability in correcting my style. I also thank dr. Ronald van Luijk and dr. Bart de Smit who agreed to form my reading committee and suggested me further valuable improvements. I also thank Sep Thijssen for using Theorem 1 in his Master's thesis [**6**] at the Radboud University of Nijmegen. This has given value to my effort. I also thank him for putting my family name next to the word theorem, I am extremely pleased for this honour.

CHAPTER 1

Group cohomology

We briefly fix conventions to be used throughout all this report.

1.1. Definition. Let G, N be groups. A *left action* of G on N is a group homomorphism $\varphi : G \to \mathrm{Aut}(N)$. In this situation, we also say that G *acts* on N, and for all $g \in G$ and $n \in N$, we write

$$^g n = \varphi(g)(n).$$

Moreover we denote with N^G the group of G-*invariants* in N, that is:

$$N^G = \{n \in N |\, ^g n = n \text{ for all } g \in G\}.$$

1.2. Definition. Let G be a group. A (left) G-module μ is an abelian group together with a left action of G on μ.

1.3. Definition. Let G, N, N' be groups, and let G act on N and N'. A G-homomorphism between N and N' is a group homomorphism $\varphi : N \to N'$ such that, for all $g \in G$ and $n \in N$:

$$\varphi(^g n) = {}^g\varphi(n).$$

We denote the set of all G-homomorphisms $N \to N'$ with $\mathrm{Hom}_G(N, N')$.

1. Cocycles

We give a general definition of *cocycle*:

1.4. Definition. Let G and N be two groups with G acting on N. A function $c : G \to N$ is a *cocycle*, if for arbitrary $g, h \in G$:

$$c(gh) = {}^g c(h)c(g).$$

We denote the set of all cocycles $G \to N$ with $\mathrm{Z}^1(G, N)$.
For $n \in N$ the function $G \to N$ defined by

$$g \mapsto {}^g n n^{-1}$$

is called a *coboundary*. We denote the set of all coboundaries with $\mathrm{B}^1(G, N)$, and we have $\mathrm{B}^1(G, N) \subseteq \mathrm{Z}^1(G, N)$.

1.5. Remark. The definition we are giving does not agree with the definition appearing in chapter 5 of [**5**]. We took this decision because 1.11 requires our definition to be true. Actually our cocycles are inverses of cocycles defined in [**5**].
When N is commutative we get the usual definition of a cocycle. In this case, $\mathrm{Z}^1(G, N)$ with the pointwise multiplication is a group and we have $\mathrm{B}^1(G, N) \leq \mathrm{Z}^1(G, N)$.

As for usual cocycles, the kernel of a cocycle is a subgroup of the domain.

1.6. Lemma. *Let G and N be two groups with G acting on N and let $c : G \to N$ be a cocycle. The* kernel

$$\ker c = \{g \in G | c(g) = 1\}$$

of c is a subgroup of G.

PROOF. We have

$$c(1) = c(1 \cdot 1) = {}^1c(1)c(1) = c(1)^2,$$

so $c(1) = 1$. If $g \in G$ and $c(g) = 1$ then

$$1 = c(1) = c(g^{-1}g) = {}^{g^{-1}}c(g)c(g^{-1}) = c(g^{-1})$$

where the last equality holds because $c(g) = 1$; thus K is closed under inverses. Finally, when $g, h \in \ker c$ we have

$$c(gh) = {}^g c(h)c(g) = {}^g 1 \cdot 1 = 1,$$

and so $gh \in K$, and hence K is a subgroup. □

We need another definition:

1.7. DEFINITION. Let N, G, H be groups. An *extension* of N by H is a short exact sequence

$$1 \longrightarrow N \xrightarrow{\varepsilon} G \xrightarrow{\pi} H \longrightarrow 1\ .$$

The group G, equipped with ε and π, is also called an extension of N by H.

1.8. DEFINITION. Let N, H be groups. Let G_1 and G_2 two extensions of N by H. We say that G_1 is *equivalent* to G_2 if there is a group homomorphism $\varphi : G_2 \to G_1$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G_1 & \longrightarrow & H & \longrightarrow & 1 \\ & & \| & & \uparrow{\scriptstyle\varphi} & & \| & & \\ 1 & \longrightarrow & N & \longrightarrow & G_2 & \longrightarrow & H & \longrightarrow & 1. \end{array}$$

1.9. DEFINITION. Consider an extension

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1\ .$$

We say that the extension (or the short exact sequence) *splits*, when there is an action ψ of H on N, such that G is equivalent to the *standard splitting exact sequence*,

$$1 \longrightarrow N \longrightarrow N \rtimes_\psi H \longrightarrow H \longrightarrow 1.$$

1.10. REMARK. The homomorphism φ of the previous definition is both injective and surjective, because of the commutativity of the diagram. Hence φ is actually an isomorphism so the relation described above is an equivalence relation. Moreover if we have a splitting short exact sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & H & \longrightarrow & 1 \\ & & \| & & \uparrow{\scriptstyle\varphi} & & \| & & \\ 1 & \longrightarrow & N & \longrightarrow & N \rtimes_\psi H & \longrightarrow & H & \longrightarrow & 1, \end{array}$$

then $G = N_0H_0$ where $N_0 = \varphi(N) = \operatorname{im}\varepsilon$ and $H_0 = \varphi(H)$, considering $N \leq N \rtimes_\psi H$ and $H \leq N \rtimes_\psi H$.

1.11. LEMMA. *Consider a short exact sequence of groups:*

$$1 \longrightarrow N \xrightarrow{\varepsilon} G \xrightarrow{\pi} H \longrightarrow 1.$$

We define an action of G on N: for all $g \in G$ and $n \in N$

$${}^g n = \varepsilon^{-1}(g\varepsilon(n)g^{-1}).$$

Then the following are equivalent:

1. The sequence splits.

2. There is a group homomorphism $\sigma : H \to G$ such that $\pi\sigma = \mathrm{id}_H$.
3. There is a cocycle $c : G \to N$ such that $c\varepsilon = \mathrm{id}_N$.

PROOF. We prove that 1 implies 3. Suppose the sequence splits. We have an action of H on N and a commutative diagram as in the definition. We write $G = N_0H_0$ with $H_0 = \varepsilon(N)$ and $H_0 = \varphi(H)$. Now we can define a map:

$$\begin{aligned} c : \ N_0H_0 &\longrightarrow N \\ n_0h_0 &\longmapsto \varepsilon^{-1}(n_0). \end{aligned}$$

It is easily seen that c is a cocycle according to our definition of action of G on N. We prove that 3 implies 2. Let $c : G \to N$ be a cocycle that is the identity on $N_0 \leq G$. We can consider the subgroup $H_0 = \ker c$. Since c is the identity on N_0, we have that $H_0 \cap N_0 = \{1\}$, therefore $\pi_{|H_0}$ is injective. Furthermore, consider $\pi(g) \in H$. If we define $h = \varepsilon(c(g))^{-1}g \in H_0$ then $gh^{-1} = \varepsilon(c(g)) \in N_0$. This implies that $\pi(h) = \pi(g)$. Therefore $\pi_{|H_0}$ is also surjective; thus it is an isomorphism and we can define $\sigma = \pi^{-1}_{|H_0}$.
Last, we prove that 2 implies 1. If $\sigma : G/N \to G$ is as in 2, then we can define an action of H on N in the following way: for every $h \in H$ and $n \in N$,

$${}^h n = \varepsilon^{-1}(\sigma(h)\varepsilon(n)\sigma(h)^{-1}).$$

Using the fact that $\pi\sigma = \mathrm{id}_H$ and that σ is a group homomorphism, we see that

$$\begin{aligned} \varphi : \ N \rtimes H &\longrightarrow G \\ (n, h) &\longmapsto \varepsilon(n)\sigma(h) \end{aligned}$$

defines a group homomorphism. This homomorphism defines an equivalence of our short exact sequence with the standard splitting exact sequence. □

1.12. LEMMA. *Let G be a group and $N \trianglelefteq G$, and let μ be a G-module. Let $c : N \to \mu^N$ be a G-homomorphism (G acting by conjugacy on N). Then:*

$$H_c = \{(c(x), x^{-1}) | x \in N\}$$

is a normal subgroup of $\mu^N \rtimes G$.

PROOF. Consider the following map:

$$\begin{aligned} f_c : \ N &\longrightarrow \mu^N \rtimes G \\ x &\longmapsto (c(x)^{-1}, x). \end{aligned}$$

This is a group homomorphism, namely for $x, x' \in N$, we have

$$(c(x)^{-1}, x)(c(x')^{-1}, x') = (c(x^{-1})c(x'^{-1}), xx') = (c(xx')^{-1}, xx')$$

because μ is an abelian group. Since, $H_c = \operatorname{im} f_c$, we have that $H_c \leq \mu^N \rtimes G$.
Now we want to show that H_c is normal. Consider $G \leq \mu^N \rtimes G$ acting by conjugacy on $\mu^N \rtimes G$; consider also G acting on N by conjugacy. We have that f_c is G-equivariant for these actions. This implies that H_c is stable under the conjugation by elements of $G \leq \mu^N \rtimes G$. Furthermore, as μ is abelian, we have $\mu^N \leq \mathrm{Z}(\mu^N \times N) \subseteq \mathrm{N}(H_c)$. Therefore, the *normalizer* $\mathrm{N}(H_c)$ contains both μ^N and G, hence $\mathrm{N}(H_c) = \mu^N \rtimes G$. □

1.13. PROPOSITION. *Let G be a group and $N \trianglelefteq G$, and let μ be a G-module. In addition let $c : N \to \mu^N$ be a G-homomorphism (G acting by conjugacy on N). Consider $H_c = \{(c(x), x^{-1}) | x \in N\}$, and define*

$$E_c = \frac{\mu^N \rtimes G}{H_c}.$$

Then we have:

1. *There are group homomorphisms:* $\iota_c : \mu^N \to E_c$ *and* $\pi_c : E_c \to G/N$ *defined by*

$$\iota_c : m \mapsto (m,1)H_c \qquad\qquad \pi_c : [(m,g)] \mapsto gN$$

and $\psi : G \to E_c$ *defined by*

$$\psi : x \mapsto [(1,x)] = (1,x)H_c$$

such that in the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \xrightarrow{\pi} & G/N & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle \psi} & & \| & & \\ 1 & \longrightarrow & \mu^N & \xrightarrow{\iota_c} & E_c & \xrightarrow{\pi_c} & G/N & \longrightarrow & 1 \end{array} \tag{1.1}$$

all squares are commutative and the bottom row is a short exact sequence.

2. *The bottom row splits if and only if* c *extends to a cocycle* $\tilde{c} : G \longrightarrow \mu^N$.

Proof. Thanks to 1.12, the group E_c is well defined. Moreover it is easy to see that ψ and ι_c are group homomorphisms. We have that ι_c is injective because $H_c \cap \mu^N = \{1\}$ in $\mu^N \rtimes G$. Moreover, for $x \in N$ we have $\iota_c(c(x)) = (c(x),1)H_c = (1,x)H_c = \psi(x)$.
The map π_c is a well-defined group homomorphism that has kernel $\mu^N H_c/H_c$, and its image is clearly G/N. Hence the diagram (1.1) commutes and the bottom row is a short exact sequence.

We still have to prove that the bottom row splits if and only if c extends to a cocycle $\tilde{c} : G \longrightarrow \mu^N$. Suppose the bottom row splits; then by lemma 1.11 we have a cocycle $q : E_c \to \mu^N$ that is the identity on μ^N. Therefore we can consider $q \circ \psi$. It is a cocycle because ψ is a group homomorphism; and since

$$\psi(x) = (1,x)H_c = (c(x),1)H_c$$

for all $x \in N$, we easily have that $q(\psi(x)) = c(x)$ for all $x \in N$.
Conversely let $\tilde{c} : G \to \mu^N$ a cocycle extending c. Let $\mu^N \rtimes G$ act on μ^N as defined in 1.11. We define $q : \mu^N \rtimes G \to \mu^N$ as $q(m,g) = m\tilde{c}(g)$. We have that q is a cocycle: consider $(m,g),(m',g') \in \mu^N \rtimes G$ then

$$q(m\,{}^g m', gg') = m\,{}^g m' \tilde{c}(g)\,{}^g \tilde{c}(g') = q(m,g)\,{}^{(m,g)} q(m',g').$$

Moreover, since $\tilde{c}$ extends c, for each $(c(x)^{-1},x) \in H_c$ it holds

$$q(c(x)^{-1},x) = c(x)^{-1}c(x) = 1.$$

Therefore q is constant on cosets of H_c and it induces a well-defined cocycle $\bar{q} : E_c \to \mu^N$, which indeed has the property that if $m \in \mu^N$ and $(m,1)H_c \in E_c$ then $\bar{q}((m,1)H_c) = q(m,1) = m$. Therefore the bottom row splits. □

1.14. Definition. Let G be a group and let μ be G-module. We define

$$\mathrm{C}(G,\mu) = \bigcap_{q \in \mathrm{Z}^1(G,\mu)} \ker q.$$

1.15. Lemma. *Let* G *be a group. Let* μ *be a* G*-module on which* G *acts via* φ. *Define* $N = \ker\varphi$ *and consider* G *acting by conjugacy on it. For* $c \in \mathrm{Hom}_G(N,\mu)$ *consider* E_c *as described in 1.13. Then we have that for* $q \in \mathrm{Z}^1(G,\mu)$ *the restriction* $q_{|N}$ *is a* G*-homomorphism, and*

$$\mathrm{C}(G,\mu) = \bigcap_{\substack{c \in \mathrm{Hom}_G(N,\mu) \\ E_c \text{ splits}}} \ker c.$$

PROOF. We have N acting trivially on μ, *i.e.* $\mu^N = \mu$. Therefore every cocycle $q \in \mathrm{Z}^1(G,\mu)$, restricted to N, defines a G-homomorphism $N \to \mu$. In fact, for $x \in N$ and $g \in G$ we can compute

$$q({}^g x) = {}^{gx}q(g^{-1})q(gx) = {}^g q(g^{-1})\,{}^g q(x)c(g) = {}^g q(x)\,{}^g q(g^{-1})q(g) = {}^g q(x).$$

Proposition 1.13 says that for every $c \in \mathrm{Hom}_G(N,\mu)$ such that E_c splits, we have $c = \tilde{c}_{|N}$ for a $\tilde{c} \in \mathrm{Z}^1(G,\mu)$. This implies that:

$$\bigcap_{q \in \mathrm{Z}^1(G,\mu)} \ker q_{|N} = \bigcap_{\substack{c \in \mathrm{Hom}_G(N,\mu) \\ E_c \text{ splits}}} \ker c.$$

Finally $N = \cap_{q \in \mathrm{B}^1(G,\mu)} \ker q \subseteq \mathrm{C}(G,\mu)$, this implies that:

$$\mathrm{C}(G,\mu) = \bigcap_{q \in \mathrm{Z}^1(G,\mu)} \ker q_{|N}$$

and we are done. □

1.16. THEOREM. *Let μ be a G-module, with φ the action of G on μ and $N = \ker\varphi$ (with G acting on N by conjugacy). Then we have that:*

1. *There is a cocycle $q \in \mathrm{Z}^1(G,\mu)$ such that*

$$N \cap (\ker q) = \{1\}$$

if and only if there is an injective *G-homomorphism $c : N \to \mu$, such that the short exact sequence*

$$1 \longrightarrow \mu \xrightarrow{\iota_c} E_c \xrightarrow{\pi_c} G/N \longrightarrow 1\ ,$$

defined by c as in 1.13, splits.

2. *We have that*

$$\mathrm{C}(G,\mu) = \{1\},$$

if and only if there are G-homomorphisms $\{c_i : N \to \mu\}_{i\in I}$, such that
   i. *we have $\bigcap_{i\in I} \ker c_i = \{1\}$;*
   ii. *the short exact sequence defined by c_i as in 1.13, splits for all $i \in I$.*

PROOF. By 1.15, there is a cocycle $q \in \mathrm{Z}^1(G,\mu)$ such that

$$N \cap (\ker c) = \{1\}$$

if and only if there is a injective G-homomorphism $c : N \to \mu$ extending to a cocycle $\tilde{c} : G \to \mu$. By 1.13, we notice that this homomorphism extends to a cocycle $\tilde{c} : G \to \mu$ if and only if the short exact sequence

$$1 \longrightarrow \mu \xrightarrow{\iota_c} E_c \xrightarrow{\pi_c} G/N \longrightarrow 1\ ,$$

defined by c as in 1.13, splits.

The other equivalence is an immediate consequence of 1.15. □

The theorem we have just proved, leads us to investigate whether a certain extension of μ by G splits or not. To decide when that extension splits, the most appropriate tool is the group $\mathrm{H}^2(G/N,\mu)$. In the following we shall focus on the computation of cohomology groups we need. We are interested in calculating $\mathrm{H}^2(\Gamma,\mu)$ when μ is a cyclic group of order n (for $n \in \mathbb{Z}_{>0}$) and Γ acts faithfully on it, that is to say that $\Gamma \subseteq \mathrm{Aut}(\mu)$.

2. Notations and definitions of group cohomology

In the following section we shall use group cohomology to investigate extensions of the type (1.1). In this section we recall some basics of group cohomology and we give the necessary background to prove the statements that will appear in the next section. All definitions of cohomology groups and other basics are well explained in [**1**].

1.17. Definition. Let G be a finite group. A G-module A is *cohomologically trivial* when, for every subgroup $H \leq G$, we have $\hat{\mathrm{H}}^q(H, A) = \{1\}$, for all $q \in \mathbb{Z}$.

1.18. Lemma. *Let R be any ring, and G a finite group. The G-module $R[G]$ is cohomologically trivial.*

Proof. We give R the trivial G-module structure and we notice that $R[G] \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], R)$. As it is explained in [**1**], the G-module structure on $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], R)$ is defined as follows: for $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], R)$ and for all $g \in G$ we set $g.\varphi(g^{-1}-) = \varphi(g^{-1}-)$ (R is a trivial G-module).
When G is finite, there is a natural G-module homomorphism which maps $a = \sum_G r_g g \in R[G]$ to φ_a defined by $\varphi_a(g) = r_g$. This is an isomorphism too. Therefore $R[G]$ is a co-induced G-module, which implies that it is cohomologically trivial. □

Let $H \leq G$ be groups. Consider, now, the forgetful functor $\rho : G\text{-mod} \to H\text{-mod}$. It is exact, and hence we can consider the ∂-functor $S_* = \mathrm{H}_*(H, \rho(-))$, and the ∂-functor $T^* = \mathrm{H}^*(H, \rho(-))$. For A an arbitrary G-module, projections $\vartheta_A : A_H \to A_G$ define a natural transformation $\vartheta : S_0 \to -_G$, and on the other hand, injections $\kappa_A : A^G \to A^H$ define a natural transformation $\kappa : -^G \to T^0$. By the fact that derived functors are universal ∂-functors, the following definition makes sense (see [**7**] 6.7 for the positive (*resp.* negative) part, the negative (*resp.* positive) part is straightforward from the other).

1.19. Definition. Let $H \leq G$ be finite groups.

1. We define $\mathrm{Res} : \hat{\mathrm{H}}^*(G, -) \to \hat{\mathrm{H}}^*(H, -)$ to be the *unique* system of morphisms of functors
$$\{\mathrm{Res}^q : \hat{\mathrm{H}}^q(G, -) \to \hat{\mathrm{H}}^q(H, -)\}_{q \in \mathbb{Z}}$$
such that: for all short exact sequences of G-modules
$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$
   i. For all $q \in \mathbb{Z}$ the following diagram commutes:
$$\begin{array}{ccc} \hat{\mathrm{H}}^q(G, C) & \xrightarrow{\partial} & \hat{\mathrm{H}}^{q+1}(G, A) \\ \downarrow{\scriptstyle \mathrm{Res}^q} & & \downarrow{\scriptstyle \mathrm{Res}^{q+1}} \\ \hat{\mathrm{H}}^q(H, C) & \xrightarrow{\partial} & \hat{\mathrm{H}}^{q+1}(H, A) \end{array}$$
   where the ∂'s are the morphisms in the long exact sequence of Tate cohomology.
   ii. Res^0 is induced by the embedding $A^G \to A^H$.
2. We define $\mathrm{Cor} : \hat{\mathrm{H}}^*(H, -) \to \hat{\mathrm{H}}^*(G, -)$ to be the *unique* system of morphisms
$$\{\mathrm{Cor}^q : \hat{\mathrm{H}}^q(H, -) \to \hat{\mathrm{H}}^q(G, -)\}_{q \in \mathbb{Z}}$$
such that: for all short exact sequences of G-modules
$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

i. For all $q \in \mathbb{Z}$ the following diagram commutes:

$$\begin{array}{ccc} \hat{\mathrm{H}}^q(H, C) & \xrightarrow{\partial} & \hat{\mathrm{H}}^{q+1}(H, A) \\ \downarrow{\scriptstyle \mathrm{Cor}^q} & & \downarrow{\scriptstyle \mathrm{Cor}^{q+1}} \\ \hat{\mathrm{H}}^q(G, C) & \xrightarrow{\partial} & \hat{\mathrm{H}}^{q+1}(G, A) \end{array}$$

where the ∂'s are the morphisms in the long exact sequence of Tate cohomology.

ii. Cor^{-1} is induced by the projection $A_H \to A_G$.

1.20. Definition. Let G be a finite group, the *norm element* $N_G \in \mathbb{Z}[G]$ (or only N when there is not ambiguity) is $N_G = \sum_{g \in G} g$.

1.21. Lemma. *Let G be a finite group, the subgroup $(\mathbb{Z}[G])^G \leq \mathbb{Z}[G]$ is the ideal $N\mathbb{Z} = (N)$.*

Proof. Take $a = \sum_{g \in G} n_g g \in (\mathbb{Z}[G])^G$, then $ga = a$ for all $g \in G$. Therefore all n_g's are the same; this means that $a = nN$, for some $n \in N$. □

We need some general facts concerning projective resolutions of $\mathbb{Z}$ as a C_m-module, when C_m is a cyclic group of order $m \in \mathbb{Z}_{>0}$. Let c be a generator of C_m; the norm element N in $\mathbb{Z}[C_m]$ is $N = \sum_{i=1}^m c^i$.

1.22. Lemma. *Consider $\mathbb{Z}$ acted upon trivially by C_m. Let c be a generator of C_m, then a projective resolution of $\mathbb{Z}$ is:*

$$\cdots \xrightarrow{c-1} \mathbb{Z}[C_m] \xrightarrow{N} \mathbb{Z}[C_m] \xrightarrow{c-1} \mathbb{Z}[C_m] \xrightarrow{N} \mathbb{Z}[C_m] \xrightarrow{c-1} \mathbb{Z}[C_m] \longrightarrow 0 \ ,$$

where N and $c-1$ are multiplication on the left by N and $c-1$ respectively.

Proof. Let $\varepsilon : \mathbb{Z}[C_m] \to \mathbb{Z}$ be the *augmentation morphism*, we have to prove that the following augmented complex is exact:

$$\cdots \xrightarrow{N} \mathbb{Z}[C_m] \xrightarrow{c-1} \mathbb{Z}[C_m] \xrightarrow{N} \mathbb{Z}[C_m] \xrightarrow{c-1} \mathbb{Z}[C_m] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0 \ .$$

First, it is clear that $I = \mathrm{im}(c-1) \subseteq \ker \varepsilon$. Vice versa if $a = \sum_{i=1}^m \alpha_i c^i \in \ker \varepsilon$ then $\sum_{i=1}^m \alpha_i = 0$ and this implies that $a = cb - b$ where $b = \sum_{i=1}^m \beta_i c^i$, with

$$\begin{aligned} \beta_1 &= -\alpha_1 \\ \beta_2 &= -(\alpha_1 + \alpha_2) \\ \beta_3 &= -(\alpha_1 + \alpha_2 + \alpha_3) \\ &\cdots \end{aligned}$$

Lemma 1.21 says that

$$(\mathbb{Z}[C_m])^{C_m} = N\mathbb{Z} \subseteq \mathbb{Z}[C_m];$$

moreover, the natural map $\pi : N\mathbb{Z} = (\mathbb{Z}[C_m])^{C_m} \to (\mathbb{Z}[C_m])_{C_m} \cong \mathbb{Z}$ sends N to m. This implies that $N\mathbb{Z} \cap I = (0)$, therefore:

$$\ker N = \{a \in \mathbb{Z}[C_m] | Na \in I\}.$$

Since $\mathbb{Z}[C_m]/I \cong \mathbb{Z}$ is a domain, I is a prime ideal. Thus $Na \in I$ if and only if $a \in I$. Hence it holds that $\ker N = \mathrm{im}(c-1)$.
Finally we have $N(c-1) = 0$ so $\mathrm{im}\, N \subseteq \ker(c-1)$, but every $g \in \mathbb{Z}[C_m]$, with $ag - g = 0$, is an invariant so it is in $\mathrm{im}\, N$, hence $\mathrm{im}\, N = \ker(c-1)$. □

This resolution permits us to perform the following computation.

1.23. Proposition. *Let A be a C_m-module being finite and cyclic as an abelian group, where C_m is a cyclic group of order m. Then for all $q \in \mathbb{Z}$, the cohomology group $\hat{\mathrm{H}}^q(C_m, A)$ is isomorphic to $A^{C_m}/N(A)$.*

Proof. By lemma 1.22 we are reduced to calculate the cohomology of this complex:

$$\cdots \xrightarrow{c-1} A \xrightarrow{N} A \xrightarrow{c-1} A \xrightarrow{N} A \xrightarrow{c-1} A \longrightarrow 0 \,.$$

The complex is periodic therefore we shall have $\hat{\mathrm{H}}^i(C_m, A) = \hat{\mathrm{H}}^{i+2}(C_m, A)$. Furthermore the Herbrand quotient $h_0/h_1 = 1$, this means that $\hat{\mathrm{H}}^0(C_m, A) = A^{C_m}/N(A)$ and $\hat{\mathrm{H}}^1(C_m, A)$ are cyclic groups of the same order. Thus they are isomorphic. □

3. Cyclic group acted upon faithfully

We shall be able to compute explicitly $\mathrm{H}^2(G/N, \mu)$ when $n = p^k$ is a power of a prime number, this will give us a simple condition in G to decide if the extension of μ by G splits.
Let μ be a cyclic group (written additively) of order $n = p^k$ where p is a prime number and $k \in \mathbb{Z}_{>0}$. We think of $\mathrm{Aut}(\mu)$ being equal to $(\mathbb{Z}/p^k\mathbb{Z})^*$. We shall consider $\Gamma \leq \mathrm{Aut}(\mu)$, and we shall consider μ a Γ-module in the following way: for $\gamma \in \Gamma$ and $m \in \mu$

$$^{\gamma}m = \gamma(m).$$

When $p = 2$, we choose $\delta = -1 + 2^k\mathbb{Z} \in \mathrm{Aut}(\mu)$ of order 2 and we write:

$$\Delta = \langle \delta \rangle.$$

1.24. Remark. When $p = 2$ and $k \geq 2$, we have that $\hat{\mathrm{H}}^0(\Delta, \mu) = \mu^{\Delta}$ has order 2, hence by 1.23 we have that $\hat{\mathrm{H}}^q(\Delta, \mu)$ has order 2, for all $q \in \mathbb{Z}$.

We shall see the following.

1.25. Theorem. *Let μ be a cyclic group of order $n = p^k$ where p is a prime number and $k \in \mathbb{Z}_{>0}$, and $\Gamma \leq \mathrm{Aut}(\mu)$.*

1. *If $n = 2^k$ with $k \geq 2$ and $\delta \in \Gamma$ then $\hat{\mathrm{H}}^q(\Gamma, \mu)$ has order 2 for all $q \in \mathbb{Z}$. Moreover $\mathrm{Res} : \hat{\mathrm{H}}^q(\Gamma, \mu) \to \hat{\mathrm{H}}^q(\Delta, \mu)$ is an isomorphism for q even and $\mathrm{Cor} : \hat{\mathrm{H}}^q(\Delta, \mu) \to \hat{\mathrm{H}}^q(\Gamma, \mu)$ is an isomorphism for q odd.*
2. *Otherwise μ is* cohomologically trivial *as a Γ-module.*

Before proving this theorem it is convenient to restate it in another form.
Consider the ring homomorphism $\pi : \mathbb{Z}/p^{k+1}\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ defined by $\pi : z + p^{k+1}\mathbb{Z} \mapsto z + p^k\mathbb{Z}$. It has got kernel $p^k\mathbb{Z}/p^{k+1}\mathbb{Z}$ which has order p, and moreover it induces a surjective group homomorphism $f : \left(\mathbb{Z}/p^{k+1}\mathbb{Z}\right)^* \to \left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$ whose kernel is $1 + \ker \pi$ which has still order p.
We recall a fact whose proof can be found in chapter 4 of [**2**].

1.26. Lemma. *Let μ be a cyclic group of order p^k where p is a prime number and $k \in \mathbb{Z}_{>0}$, then:*

1. *When $p \neq 2$, $\mathrm{Aut}(\mu)$ is a cyclic group of order $(p-1)p^{k-1}$.*
2. *When $p = 2$ and $k = 1$ then $\mathrm{Aut}(\mu) = \{1\}$, when $k = 2$ we have $\mathrm{Aut}(\mu) = \Delta$. While when $p = 2$ and $k > 2$ we have that $\mathrm{Aut}(\mu) = \Delta \times \langle 5 + 2^k\mathbb{Z} \rangle$, and every subgroup $\Gamma \leq \mathrm{Aut}(\mu)$ is either cyclic or $\Delta \times B$ with $B \leq \langle 5 + 2^k\mathbb{Z} \rangle$ cyclic.*

1.27. Lemma. *Let f be as defined before; $f^{-1}(\Gamma)$ is not cyclic if and only if $p = 2$, the exponent $k \geq 2$ and $\delta \in \Gamma$.*

PROOF. If $p \neq 2$ or $k < 2$, then $f^{-1}(\Gamma)$ is cyclic because $\operatorname{Aut}\mu$ itself is cyclic. Moreover when $p = 2$ and $k \geq 2$ we have

$$f(-1 + 2^{k+1}\mathbb{Z}) = \delta \qquad f(1 + 2^k + 2^{k+1}\mathbb{Z}) = 1 + 2^k\mathbb{Z}$$

therefore $\delta \in \Gamma$ if and only if

$$-1 + 2^{k+1}\mathbb{Z} \in f^{-1}(\Gamma) \qquad 1 + 2^k + 2^{k+1}\mathbb{Z} \in f^{-1}(\Gamma).$$

This is equivalent to say that $f^{-1}(\Gamma)$ is not cyclic. In fact, $1+2^k \equiv 5^{2^{k-2}} \mod 2^{k+1}$, thus by 1.26 we can conclude. □

Thanks to this lemma we can restate 1.25.

1.28. THEOREM. *Let μ be a cyclic group of order $n = p^k$ where p is a prime number and $k \in \mathbb{Z}_{>0}$, and $\Gamma \leq \operatorname{Aut}(\mu)$.*

1. *If $f^{-1}(\Gamma)$ is cyclic then μ is* cohomologically trivial *as a Γ-module .*
2. *Otherwise $\hat{\mathrm{H}}^q(\Gamma, \mu)$ has order 2 for all $q \in \mathbb{Z}$. More precisely,* $\mathrm{Res} : \hat{\mathrm{H}}^q(\Gamma, \mu) \to \hat{\mathrm{H}}^q(\Delta, \mu)$ *is an isomorphism for q even and* $\mathrm{Cor} : \hat{\mathrm{H}}^q(\Delta, \mu) \to \hat{\mathrm{H}}^q(\Gamma, \mu)$ *is an isomorphism for q odd. In particular $\hat{\mathrm{H}}^q(\Gamma, \mu)$ has order 2 for all $q \in \mathbb{Z}$.*

PROOF. Throughout this proof, for $z \in \mathbb{Z}$, we shall write $[z] = (z \mod n)$.
In the first case we have that Γ is a cyclic group of order dividing $(p-1)p^{k-1}$. Moreover $f^{-1}(\Gamma)$ is cyclic, so we can write $f^{-1}(\Gamma) = \langle c \mod p^{k+1}\rangle$ for some $c \in \mathbb{Z}$ such that $\Gamma = \langle [c] \rangle$.
Now we want to use 1.18, so we have to construct a suitable short exact sequence. We can choose η a generator of μ, and define:

$$v : \quad \mathbb{Z}[\Gamma] \longrightarrow \mu$$
$$\textstyle\sum_{i=1}^{\#\Gamma} a_i [c]^i \longmapsto \sum_{i=1}^{\#\Gamma} a_i c^i \eta.$$

This is a morphism of Γ-modules; therefore, for $K = \ker v$, we have a short exact sequence:

$$0 \longrightarrow K \longrightarrow \mathbb{Z}[\Gamma] \xrightarrow{v} \mu \longrightarrow 0 \ . \tag{1.2}$$

and indeed we have that $K = (p^k, [c] - c)$, ideal of $\mathbb{Z}[\Gamma]$.
Now, since $\mathbb{Z} \cap K = (p^k) \leq (p)$, the exact sequence (1.2) induces an exact sequence:

$$0 \longrightarrow K_p \longrightarrow \mathbb{Z}_{(p)}[\Gamma] \xrightarrow{\bar{v}} \mu \longrightarrow 0 \ ,$$

where $K_p = (p^k, [c] - c) \subseteq \mathbb{Z}_{(p)}[\Gamma]$ that is $K_p = \ker \bar{v}$.
We have defined c is such a way that $f^{-1}(\Gamma) = \langle c \mod p^{k+1}\rangle$. This group has order $p\,\#\Gamma$, and hence we see that

$$p^k \mid\mid 1 - c^{\#\Gamma} = [c]^{\#\Gamma} - c^{\#\Gamma}.$$

This means that we can write

$$[c]^{\#\Gamma} - c^{\#\Gamma} = mp^k$$

with $p \nmid m$. This implies that m is invertible in $\mathbb{Z}_{(p)}$ and consequently that p^k is a multiple of $[c] - c$. Hence $K_p = ([c] - c) \subseteq \mathbb{Z}_{(p)}[\Gamma]$; and since $[c] - c$ is not a zero-divisor , the following is an exact sequence of Γ-modules:

$$0 \longrightarrow \mathbb{Z}_{(p)}[\Gamma] \xrightarrow{[c]-c} \mathbb{Z}_{(p)}[\Gamma] \xrightarrow{\bar{v}} \mu \longrightarrow 0 \ .$$

Now it suffices to note that $\mathbb{Z}_{(p)}[\Gamma]$ is cohomologically trivial by 1.18; and hence μ is cohomologically trivial too. This proves the first point.

Now, consider the case $f^{-1}(\Gamma)$ not cyclic, then $p = 2$ and $\Gamma = \mathrm{B} \times \Delta$ for B a cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. Moreover 1.27 implies that $f^{-1}(\mathrm{B})$ is cyclic. We define the following modules:

$\nu = \mu$	as a B-module,
$\mathbb{Z}$	Δ-module with the trivial action,
$\mathbb{Z}_-$	Δ-module with the non-trivial action.

We also notice that if M is a B-module and M' is a Δ-module then the tensor product $M \otimes_{\mathbb{Z}} M'$ is naturally a Γ-module, and for instance $\mu = \nu \otimes_{\mathbb{Z}} \mathbb{Z}_-$.
We have two short exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}[\Delta] & \longrightarrow & \mathbb{Z}_- & \longrightarrow & 0 \\ & & & & a + b\delta & \longmapsto & a - b & & \\ 0 & \longrightarrow & \mathbb{Z}_- & \longrightarrow & \mathbb{Z}[\Delta] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0\ . \\ & & & & a + b\delta & \longmapsto & a + b & & \end{array}$$

The two sequences split over the integers. This means that tensoring on the left by ν gives again two new short exact sequences:

$$0 \longrightarrow \nu \otimes_{\mathbb{Z}} \mathbb{Z} \longrightarrow \nu \otimes_{\mathbb{Z}} \mathbb{Z}[\Delta] \longrightarrow \mu \longrightarrow 0 \tag{1.3}$$

$$0 \longrightarrow \mu \longrightarrow \nu \otimes_{\mathbb{Z}} \mathbb{Z}[\Delta] \longrightarrow \nu \otimes_{\mathbb{Z}} \mathbb{Z} \longrightarrow 0\ . \tag{1.4}$$

By the fact that $f^{-1}(\mathrm{B})$ is cyclic, we have that B is cohomologically trivial. Furthermore, specializing what we have done before to $p = 2$, there is a short exact sequence:

$$0 \longrightarrow \mathbb{Z}_{(2)}[\mathrm{B}] \longrightarrow \mathbb{Z}_{(2)}[\mathrm{B}] \longrightarrow \nu \longrightarrow 0\ .$$

Now $\mathbb{Z}[\Delta]$ is a free $\mathbb{Z}$-module, in particular it is torsion-free and therefore *flat*. Thus tensoring on the right by $\mathbb{Z}[\Delta]$ is an exact functor and

$$0 \longrightarrow \mathbb{Z}_{(2)}[\Gamma] \longrightarrow \mathbb{Z}_{(2)}[\Gamma] \longrightarrow \nu \otimes_{\mathbb{Z}} \mathbb{Z}[\Delta] \longrightarrow 0$$

is an exact sequence of Γ-modules. Therefore, by 1.18, we have that $\nu \otimes_{\mathbb{Z}} \mathbb{Z}[\Delta]$ is cohomologically trivial.
Using twice the long exact sequence of cohomology on sequences (1.3) and (1.4), we easily get that for every q there are two exact sequences

$$\hat{\mathrm{H}}^q(\Gamma, \nu \otimes_{\mathbb{Z}} \mathbb{Z}[\Delta]) \longrightarrow \hat{\mathrm{H}}^q(\Gamma, \mu) \xrightarrow{\partial_q} \hat{\mathrm{H}}^{q+1}(\Gamma, \nu \otimes_{\mathbb{Z}} \mathbb{Z}) \longrightarrow \hat{\mathrm{H}}^{q+1}(\Gamma, \nu \otimes_{\mathbb{Z}} \mathbb{Z}[\Delta])$$

$$\hat{\mathrm{H}}^q(\Gamma, \nu \otimes_{\mathbb{Z}} \mathbb{Z}[\Delta]) \longrightarrow \hat{\mathrm{H}}^q(\Gamma, \nu \otimes_{\mathbb{Z}} \mathbb{Z}) \xrightarrow{\partial'_q} \hat{\mathrm{H}}^{q+1}(\Gamma, \mu) \longrightarrow \hat{\mathrm{H}}^{q+1}(\Gamma, \nu \otimes_{\mathbb{Z}} \mathbb{Z}[\Delta])\ .$$

and since $\nu \otimes_{\mathbb{Z}} \mathbb{Z}[\Delta]$ is cohomologically trivial, we have that

$$\partial_q \circ \partial'_{q+1} : \qquad \hat{\mathrm{H}}^q(\Gamma, \mu) \longrightarrow \hat{\mathrm{H}}^{q+2}(\Gamma, \mu)$$

is an isomorphism.
We notice that $N_\Gamma \mu = N_\Delta \mu = \{0\}$, therefore $\hat{\mathrm{H}}^0(G, \mu) = \mathrm{H}^0(G, \mu)$ and $\hat{\mathrm{H}}^{-1}(G, \mu) = \mathrm{H}_0(G, \mu)$ for $G = \Delta, \Gamma$. Therefore $\mathrm{Res} : \hat{\mathrm{H}}^0(\Gamma, \mu) \to \hat{\mathrm{H}}^0(\Delta, \mu)$ is nothing but the injection $\mu^\Gamma \to \mu^\Delta$. Since μ^Δ has order 2, and B consists of automorphisms of μ, we have that $\mu^\Gamma = \mu^\Delta$, so we have the isomorphism. Furthermore we have that $I_\Delta = (-2)$. Thus $I_\Delta \mu = -2\mu = 2\mu$; moreover we clearly have that $I_\Gamma \mu \neq \mu$ because I_Γ consists only of even numbers. As $I_\Delta \subseteq I_\Gamma$ and 2μ is the maximal subgroup of μ, the projection $\mu / I_\Delta \mu \to \mu / I_\Gamma \mu$ is the identity. Hence we have the isomorphism.

By definition, Res and Cor commute with ∂ and ∂'. We have just proved that $\mathrm{Res} : \hat{\mathrm{H}}^0(\Gamma,\mu) \to \hat{\mathrm{H}}^0(\Delta,\mu)$ and $\mathrm{Cor} : \hat{\mathrm{H}}^{-1}(\Delta,\mu) \to \hat{\mathrm{H}}^{-1}(\Gamma,\mu)$ are isomorphisms. The fact that $\partial_q \circ \partial'_{q+1}$ is always an isomorphism guarantees that the statement is true for the other levels too.
Finally, by 1.24 we conclude also that $\hat{\mathrm{H}}^q(\Gamma,\mu)$ has order 2 for all $q \in \mathbb{Z}$. □

4. Extensions

Let H be a group and let N be an H-module (written multiplicatively) on which H acts via φ. Consider an extension E of N by H. Since N is abelian, the short exact sequence

$$1 \longrightarrow N \xrightarrow{\varepsilon} E \xrightarrow{\pi} H \longrightarrow 1$$

induces an action of H on N. Namely, for $n \in N$ and $h \in H$ we can pick $g \in E$ such that $\pi(g) = h$ and define:

$$\varepsilon({}^h m) = g\varepsilon(n)g^{-1}.$$

The fact that N is abelian guarantees that this is a well-defined action.

1.29. Definition. Let H be a group and let N be an H-module on which (written multiplicatively) H acts via φ. We say that the extension

$$1 \longrightarrow N \xrightarrow{\varepsilon} E \xrightarrow{\pi} H \longrightarrow 1$$

is an extension of N by H *as an H-module* when the action of H on N induced by the exact sequence is φ *i.e.* when: for $n \in \mu$ and $g \in E$

$$g\varepsilon(n)g^{-1} = \varepsilon(\varphi(\pi(g))(n)).$$

Let μ a be a Γ-module as in the previous section, except that this time we write it multiplicatively. Consider an extension of μ by Γ as a Γ-module:

$$1 \longrightarrow \mu \xrightarrow{\varepsilon} E \xrightarrow{\pi} \Gamma \longrightarrow 1. \tag{1.5}$$

The group $\hat{\mathrm{H}}^2(\Gamma,\mu)$ describes the possible extensions (1.5), modulo the equivalence relation described in 1.8. In fact, if we have such an extension, choose a system of coset representatives $\sigma : \Gamma \to E$ *i.e.* a map such that $\pi\sigma = \mathrm{id}_\Gamma$. Then we have

$$\sigma(g)\sigma(g') = \varphi(g,g')\sigma(gg').$$

This function is a 2-cocycle $\varphi : \Gamma \times \Gamma \to \mu$. If we change the map σ, we multiply φ by a 2-coboundary. Vice versa every class in $\hat{\mathrm{H}}^2(\Gamma,\mu)$ arises from an extension of μ by Γ in this way. See [**1**] section 2 or [**7**] 6.6 for explicit computations.
In the following we will consider μ a cyclic group of order n and we will identify $\mathrm{Aut}(\mu)$ with $(\mathbb{Z}/n\mathbb{Z})^*$. As usual we will write $\delta = -1 + n\mathbb{Z}$ and $\Delta = \langle\delta\rangle$.

1.30. Lemma. *Consider $n = 2^k$ with $k \geq 2$; let $\delta \in \Gamma \subseteq \mathrm{Aut}(\mu)$ where μ is a cyclic group of order n. Consider an extension of μ by Γ as a Γ-module*

$$1 \longrightarrow \mu \xrightarrow{\varepsilon} E \xrightarrow{\pi} \Gamma \longrightarrow 1. \tag{1.6}$$

Then this sequence splits if and only if *the exact sequence*

$$1 \longrightarrow \mu \xrightarrow{\varepsilon} \pi^{-1}(\Delta) \xrightarrow{\pi} \Delta \longrightarrow 1 \tag{1.7}$$

splits.

Proof. We point out that, if $\varphi : \Gamma \times \Gamma \to \mu$ is a 2-cocycle, and $[\varphi] \in \hat{\mathrm{H}}^2(\Gamma,\mu)$ is its cohomology class, then $\mathrm{Res}([\varphi]) = [\varphi_{|\Delta\times\Delta}] \in \hat{\mathrm{H}}^2(\Delta,\mu)$.
Every system of coset representatives $\sigma : \Delta \to \pi^{-1}(\Delta)$ is the restriction to Δ of a system of cosets representatives $\Gamma \to E$. Therefore the class of 2-cocycles corresponding to (1.7) is the restriction of the class of cocycles associated to (1.6).

This means that if $\varphi \in \hat{\mathrm{H}}^2(\Gamma, \mu)$ is the class corresponding to (1.6), then (1.7) corresponds to $\mathrm{Res}(\varphi)$. In 1.28, we proved that $\mathrm{Res} : \hat{\mathrm{H}}^2(\Gamma, \mu) \to \hat{\mathrm{H}}^2(\Gamma, \mu)$ is an isomorphism, this suffices to conclude. □

1.31. Remark. Consider $n = 2^k$ with $k \geq 2$; let μ be a cyclic group of order n. The short exact sequence (1.7) splits if and only if there is $\eta \in \pi^{-1}(\delta)$ such that $\eta^2 = 1$. In fact, having such an element η, we can define

$$\begin{aligned} \sigma : \ \Delta &\longrightarrow \pi^{-1}(\Delta) \ ; \\ \delta &\longmapsto \eta \end{aligned}$$

and this has clearly the property that $\pi\sigma = \mathrm{id}$. Conversely if we have a group homomorphism $\sigma : \Delta \to \pi^{-1}(\Delta)$ such that $\pi\sigma = \mathrm{id}$, then $\sigma(\delta)$ is of order 2.

It is now straightforward to prove the following theorem.

1.32. Theorem. *Consider $n = p^k$ with p prime and $k \geq 2$; let $\Gamma \subseteq \mathrm{Aut}(\mu)$ where μ is a cyclic group of order n. Consider an extension of μ by Γ as a Γ-module*

$$1 \longrightarrow \mu \xrightarrow{\varepsilon} E \xrightarrow{\pi} \Gamma \longrightarrow 1.$$

Then:

1. *when $n = 2^k$ with $k \geq 2$ and $\delta \in \Gamma$ the extension splits if and only if there is $\eta \in \pi^{-1}(\delta)$ such that $\eta^2 = 1$.*
2. *Otherwise it always splits.*

1.33. Corollary. *Consider $n = p^k$ with p prime. Let G be a group, and let μ be a G-module being a cyclic group of order n, on which G acts via φ. Let $N = \ker \varphi$, consider $c : N \to \mu$, a G-homomorphism (G acting by conjugacy on N); and consider the extension defined in 1.13:*

$$1 \longrightarrow \mu \xrightarrow{\iota_c} E_c \xrightarrow{\pi_c} G/N \longrightarrow 1 \ .$$

Then:

1. *when $n = 2^k$ with $k \geq 2$ and $\delta \in \varphi(G)$ the extension splits if and only if for all $g \in G$ such that $\varphi(g) = \delta$, we have $c(g^2) = 1$.*
2. *Otherwise it always splits.*

Proof. As $G/N \cong \varphi(G)$, say via κ,

$$1 \longrightarrow \mu \xrightarrow{\iota_c} E_c \xrightarrow{\pi_c} G/N \longrightarrow 1$$

splits if and only if

$$1 \longrightarrow \mu \xrightarrow{\iota_c} E_c \xrightarrow{\kappa\circ\pi_c} \varphi(G) \longrightarrow 1$$

splits. This means that, for our purposes, we can consider $G/N = \varphi(G) \subseteq \mathrm{Aut}(\mu)$ and use 1.32.
In the first case, by 1.32, the extension splits if and only if $\eta \in \pi_c^{-1}(\delta)$ of order 2. Now $c : N \to \mu$ is an embedding that is also a G-homomorphism. Therefore we can consider (1.1) restricted to Δ:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & \pi^{-1}(\Delta) & \xrightarrow{\pi} & \Delta & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle \psi} & & \| & & \\ 1 & \longrightarrow & \mu & \xrightarrow{\iota_c} & \pi_c^{-1}(\Delta) & \xrightarrow{\pi_c} & \Delta & \longrightarrow & 1. \end{array}$$

Surely, if there is $g \in G$ such that $\pi(g) = \delta$ and $c(g^2) = 1$ then we can set $\eta = \psi(g)$ and we have:

$$\eta^2 = \psi(g^2) = \iota_c(c(g^2)) = \iota_c(1) = 1.$$

Conversely if there is η as wanted, by 1.13, we have a cocycle $\tilde{c} : G \to \mu$ extending c. Moreover, by definition of π_c, we ought to have $g \in G$ such that $\pi_c(\psi(g)) = \pi(g) = \delta$. Clearly, $g^2 \in \ker \pi = N$ but we also have that

$$c(g^2) = \tilde{c}(g^2) = {}^g\tilde{c}(g)\tilde{c}(g) = \tilde{c}(g)^{-1}\tilde{c}(g) = 1$$

because $\pi(g) = \delta$. Now, for all $h \in G$ such that $\varphi(h) = \delta$ we have $h = gn$ with $n \in N$. Therefore:

$$c(h^2) = c(gngn) = {}^{gn}\tilde{c}(gn)\tilde{c}(gn) = {}^g\tilde{c}(gn)\tilde{c}(gn) = \tilde{c}(gn)^{-1}\tilde{c}(gn) = 1.$$

The second point is trivial from 1.32. □

5. Transgression

For the reader acquainted with inflation-restriction sequences of cohomology groups, it may be worth while noticing that, what we have done up to now has a strong relation with these sequences.
In fact, consider a group G, a G-module μ on which G acts via φ and $N = \ker \varphi$. Then the inflation-restriction long exact sequence is

$$1 \longrightarrow \mathrm{H}^1(G/N, \mu) \xrightarrow{\mathrm{Inf}} \mathrm{H}^1(G, \mu) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(N, \mu)^{G/N} \xrightarrow{\mathrm{Tra}} \mathrm{H}^2(G/N, \mu) \xrightarrow{\mathrm{Inf}} \mathrm{H}^2(G, \mu) \longrightarrow \cdots$$

where Inf and Res are the usual inflation and restriction morphisms. The arrow labeled Tra is the transgression homomorphism, which is defined in 3.7 of [**4**] for the profinite case (the finite case is easily got from the profinite one). We briefly give the definition here too.

1.34. Definition. Consider a group G and a normal subgroup $N \trianglelefteq G$. Let $\bar{a} \in \mathrm{H}^1(N, \mu)^{G/N}$ where a is a cocycle in $\mathrm{Z}^1(N, \mu)$. Let $\sigma : G/N \to G$ be a system of coset representatives. Since $\bar{a}$ is G/N invariant, for each $\gamma \in G/N$ there is $b(\sigma(\gamma))$ such that

$$\sigma(\gamma)a(\sigma(\gamma)^{-1}h\sigma(\gamma))a(h)^{-1} = {}^hb(\sigma(\gamma))\sigma(\gamma)^{-1}.$$

We can define a lift b of a to G in the following manner. Consider an arbitrary $g = h\sigma(\gamma) \in G$ (for suitable and unique $h \in N$ and $\gamma \in G/N$, we define

$$b(g) = a(h)\,{}^hb(\sigma(\gamma)).$$

The *transgression* homomorphism sends $\bar{a}$ to $\bar{\varphi} \in \mathrm{H}^2(G/N, \mu^N)$, where $\varphi : G/N \times G/N \to \mu$ is defined to be:

$$\varphi(\gamma_1, \gamma_2) = b(\sigma(\gamma_1)) \cdot {}^{\sigma(\gamma_1)}b(\sigma(\gamma_2)) \cdot b(\sigma(\gamma_1)\sigma(\gamma_2))^{-1}.$$

Using that definition, it can be seen that 1.13 is actually an interpretation of the transgression homomorphism.

1.35. Proposition. *In the same notations of 1.13 , if $c : N \to \mu$ is a G-homomorphism, and $\bar{c}$ is its cohomology class, then the extension E_c of 1.13 corresponds to* $\mathrm{Tra}(\bar{c})^{-1}$.

PROOF. On the one hand the extension E_c corresponds to the class of

$$\varphi_E(\gamma_1, \gamma_2) = \psi(\sigma(\gamma_1)\sigma(\gamma_2)\sigma(\gamma_1\gamma_2)^{-1}) = c(\sigma(\gamma_1)\sigma(\gamma_2)\sigma(\gamma_1\gamma_2)^{-1}).$$

On the other hand, the subgroup N is the kernel of the action. This implies that we can choose $b(\sigma(\gamma)) = 1$ for all $\gamma \in G/N$. This way we have $\mathrm{Tra}(\bar{c})$ is the class of

$$\varphi(\gamma_1, \gamma_2) = c(\sigma(\gamma_1)\sigma(\gamma_2)\sigma(\gamma_1\gamma_2)^{-1})^{-1}.$$

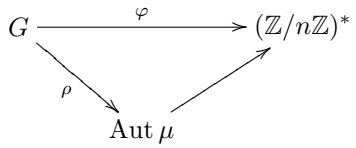
□

CHAPTER 2

Galois extensions

1. A cohomological point of view on the problem

Consider a field K and $n \in \mathbb{Z}_{>0}$. Let $L \supseteq K$ be a finite Galois extension of K such that the subgroup $\mu \subseteq L^*$ of all n-th roots of 1 has order n. Let $G = \mathrm{Gal}(L/K)$, we have an action $\rho : G \to \mathrm{Aut}(\mu)$ of G on μ and $\mathrm{Aut}\,\mu \cong (\mathbb{Z}/n\mathbb{Z})^*$. Composing ρ with this last isomorphism we get:



In other words for $\zeta \in \mu$ the action is ${}^{\sigma}\zeta = \sigma(\zeta) = \zeta^{\varphi(\sigma)}$. Taking into account this fact, we can identify $\mathrm{Aut}(\mu)$ with $(\mathbb{Z}/n\mathbb{Z})^*$ and say that G acts on μ via φ.

2.1. Proposition. *Consider a field K and $n \in \mathbb{Z}_{>0}$. Let $L \supseteq K$ be a finite Galois extension of K such that the subgroup $\mu \subseteq L^*$ of all n-th roots of 1 has order n. Let $G = \mathrm{Gal}(L/K)$ acting on μ via φ as explained above.*
Then we have the following equivalences:

1. *The extension L is the splitting field of a polynomial of the form $x^n - a$ with $a \in K$* if and only if *there is a cocycle $c \in \mathrm{Z}^1(G, \mu)$ such that*
$$(\ker \varphi) \cap (\ker c) = \{1\}.$$
2. *The extension L is the splitting field of a* collection *of polynomials $\{x^n - a_i\}_{i \in I}$ with $a_i \in K$* if and only if
$$\mathrm{C}(G, \mu) = \{1\},$$
where $\mathrm{C}(G, \mu)$ is the group defined in 1.14

We need the following fact.

2.2. Lemma. *There is an isomorphism $\eta : (L^*/K^*)[n] \xrightarrow{\sim} \mathrm{Z}^1(G, \mu)$ defined by $\eta(\alpha K^*) : \sigma \mapsto \frac{\sigma\alpha}{\alpha}$. Moreover, $\mathrm{Gal}(L/K(\alpha)) = \ker \eta(\alpha K^*)$, for all $\alpha \in L^*$ such that $\alpha^n \in K$.*

Proof. Clearly, since $\alpha^n \in K^*$ then we have that $\frac{\sigma(\alpha)}{\alpha} \in \mu$, while if $\alpha' K^* = \alpha K^*$ hence $\alpha' = k\alpha$ with $k \in K^*$ so
$$\frac{\sigma(\alpha')}{\alpha'} = \frac{k\sigma(\alpha)}{k\alpha}.$$
The formula $\eta(\alpha K^*) : \sigma \mapsto \frac{\sigma\alpha}{\alpha}$ defines a cocycle. In fact, since G is a group of automorphisms, for $\sigma, \sigma' \in G$ we have
$$\frac{\sigma\sigma'(\alpha)}{\alpha} = \frac{\sigma\sigma'(\alpha) \cdot \sigma(\alpha)}{\sigma(\alpha) \cdot \alpha} = \eta(\alpha K^*)(\sigma) \cdot \sigma(\eta(\alpha K^*)(\sigma'));$$
and it is easy to see that η is a group homomorphism. Furthermore η is injective, because if $\eta(\alpha K^*) \equiv 1$ then for all $\sigma \in G$, it ought to hold $\sigma(\alpha) = \alpha$ which is

equivalent to say that $\alpha \in K^*$. Finally η is also surjective, in fact by Hilbert's Satz 90 we have

$$\mathrm{B}^1(G, L^*) = \mathrm{Z}^1(G, L^*) \supseteq \mathrm{Z}^1(G, \mu);$$

therefore every cocycle $c \in \mathrm{Z}^1(G, \mu)$ is indeed a coboundary in $\mathrm{B}^1(G, L^*)$. Thus, we have $c : \sigma \mapsto \frac{\sigma\alpha}{\alpha}$ for $\alpha \in L^*$ and $\sigma(\alpha)^n = \alpha^n$ which means that $\alpha^n \in K^*$.
The last remark is immediately seen writing down explicitly $\ker \eta(\alpha K^*)$ for every $\alpha \in E^*$ such that $\alpha^n \in K$. □

2.3. Proof of 2.1. We notice that:

$$N = \{\sigma \in G | \forall\, m \in \mu \;\; \sigma(m) = m\} = \mathrm{Gal}(L/K(\mu)).$$

As proved in 2.2, the existence of $c \in \mathrm{Z}^1(G, \mu)$ with $(\ker \varphi) \cap (\ker c) = \{1\}$ is equivalent to the existence of $\alpha \in L^*$ with $\alpha^n \in K^*$ such that $\ker \varphi \cap \ker \eta(\alpha K^*) = \{1\}$. Since $\mathrm{Gal}(L/K(\alpha)) = \ker \eta(\alpha K^*)$, we have easily that $(\ker \varphi) \cap (\ker c) = \{1\}$ if and only if $\mathrm{Gal}(L/K(\mu, \alpha)) = \{1\}$.

For the second case, we notice that L is the splitting field of a *collection* of polynomials $\{x^n - a_i\}_{i \in I}$ with $a_i \in K$, if and only if L is the splitting field of $\{x^n - \alpha^n\}_{\alpha \in \{\alpha \in E^* | \alpha^n \in K\}}$ over K. Now, we have that:

$$\mathrm{C}(G, \mu) = \mathrm{Gal}(L/K(\mu, \{\alpha \in E^* | \alpha^n \in K\}));$$

and $\mathrm{Gal}(L/K(\mu, \{\alpha \in E^* | \alpha^n \in K\})) = \{1\}$ if and only if L is the splitting field over K of $\{x^n - \alpha^n\}_{\alpha \in \{\alpha \in E^* | \alpha^n \in K\}}$.

2. Proof of the main theorem

Let K be a field and $n = p^k$ for p a prime number and $k \in \mathbb{Z}_{>0}$. Consider $L \supseteq K$ a finite Galois extension of K such that the subgroup $\mu \subseteq L^*$ of all n-th roots of 1 has order n. Let $\varphi : G \to (\mathbb{Z}/n\mathbb{Z})^*$ be the action of G on μ (as usual we have identified $\mathrm{Aut}(\mu)$ with $(\mathbb{Z}/n\mathbb{Z})^*$). We define $N = \ker \varphi = \mathrm{Gal}(L/K(\mu))$. We have $G/N \cong \varphi(G) \subseteq \mathrm{Aut}(\mu)$, therefore all the theory of the previous chapter can be applied. Moreover, when $p = 2$ and δ is the *inversion* in $\mathrm{Aut}(\mu)$, under our identification, we have $\delta = -1 + n\mathbb{Z} \in \mathrm{Aut}(\mu)$. Therefore, as done in the previous chapter, we write $\Delta = \langle \delta \rangle$.

2.4. Theorem. *Consider a field K and $n = p^k$ for p a prime number and $k \in \mathbb{Z}_{>0}$. Let $L \supseteq K$ be a finite Galois extension of K such that the subgroup $\mu \subseteq L^*$ of all n-th roots of 1 has order n. Let $G = \mathrm{Gal}(L/K)$ be acting on μ via $\varphi : G \to (\mathbb{Z}/n\mathbb{Z})^*$. Define $N = \ker \varphi$. Then:*

1. *The Galois extension L is the splitting field of a polynomial of the form $x^n - a$ with $a \in K$* if and only if
   - i. *N is cyclic and its order divides the order of μ;*
   - ii. *for all $g \in G$ and $h \in N$, we have $ghg^{-1} = h^i$ with $(i \bmod n) = \varphi(g)$;*
   - iii. *in case $n = 2^k$ with $k \geq 2$ and $\delta \in \varphi(G)$, we have that for all $g \in G$ such that $\varphi(g) = \delta$, it holds $g^2 = 1$.*
2. *The Galois extension L is the splitting field of a* collection *of polynomials*

$$\{x^n - a_i\}_{i \in I}$$

   with $a_i \in K$ if and only if
   - i. *N is abelian and its exponent divides the order of μ;*
   - ii. *for all $g \in G$ and $h \in N$, we have $ghg^{-1} = h^i$ with $(i \bmod n) = \varphi(g)$;*
   - iii. *in case $n = 2^k$ with $k \geq 2$ and $\delta \in \varphi(G)$, we have that for all $g \in G$ such that $\varphi(g) = \delta$, it holds $g^2 = 1$.*

PROOF. We notice that *i* and *ii* are equivalent to say that there is an embedding $c : N \to \mu$ that is also a G-homomorphism. Therefore, 1.16 together with 2.1 tell us that L is the splitting field of a polynomial of the form $x^n - a$ with $a \in K$ *if and only if* *i* and *ii* hold, and the short exact sequence

$$1 \longrightarrow \mu \xrightarrow{\iota_c} E_c \xrightarrow{\pi_c} G/N \longrightarrow 1\ , \tag{2.1}$$

defined by c as in 1.13, splits.
When p is odd or $k < 2$ or $\delta \notin \varphi(G)$, the sequence (2.1) splits because of 1.33. Otherwise, by 1.33 and the injectivity of c, we have that (2.1) splits if and only *iii* holds.

The second case is very similar. We notice that since L is a finite extension, N needs to be finite. Therefore, by the Elementary Divisor Theorem we have that *i* and *ii* are equivalent to having an injective G-homomorphism $c : N \to (\mu)^r$ for some $r \in \mathbb{Z}_{>0}$. This is equivalent to having a collection of G-homomorphisms $\{c_i : N \to \mu\}_{i\in I}$ such that

$$\bigcap_{i\in I} \ker c_i = \{1\}.$$

Once again we have that L is the splitting field of a collection of polynomials

$$\{x^n - a_i\}_{i\in I}$$

if and only if *i* and *ii* hold, and each short exact sequence, defined by c_i as in 1.13, splits. However, this is true in all cases but when $n = 2^k$ with $k \geq 2$ and $\delta \in \varphi(G)$. In this case, all short exact sequence split, if and only if for all $g \in G$ such that $\varphi(g) = \delta$ we have $c_i(g^2) = 1$, for all $i \in I$. This means that $g^2 = 1$ because the intersection of all kernels is trivial. □

2.5. REMARK. Notice that we have proved the theorem showing that that the three conditions are equivalent to $\mathrm{C}(G, \mu) = \{1\}$.

Theorem 2.4 gives us an important corollary. We fix n, a power of a prime number as above. Suppose we are given a field K and a finite Galois extension E of K such that the subgroup $\mu \subseteq E^*$ of n-th roots of unity has order n. We want to know which is the largest extension of K generated by n-th radicals of K, contained in E. The theorem we have proved gives us an important description of the Galois group of such an extension.

2.6. COROLLARY. *Consider a field K and $n = p^k$ for p a prime number and $k \in \mathbb{Z}_{>0}$. Let $E \supseteq K$ be a finite Galois extension of K such that the subgroup $\mu_n \subseteq E^*$ of all n-th roots of 1 has order n. Let $G = \mathrm{Gal}(E/K)$, and let $\varphi : G \to (\mathbb{Z}/n\mathbb{Z})^*$ be the action of G on μ_n. We define two sets:*

$$S_1 = \{ghg^{-1}h^{-i} | g \in G,\ h \in \ker\varphi,\ (i \mod n) = \varphi(g)\}$$
$$S_2 = \{g^2 \in G | \varphi(g) = \delta\}$$

Let L_n be the largest intermediate field between K and E generated by n-th radicals, i.e.

$$L_n = K(\alpha \in E^* | \alpha^n \in K).$$

Then:

$$\mathrm{Gal}(E/L_n) = \mathrm{C}(G, \mu_n) = \langle S_1 \rangle \cdot \langle S_2 \rangle.$$

PROOF. Let $C_n = \mathrm{C}(G, \mu_n)$. The fact that $\mathrm{Gal}(E/L) = \mathrm{C}(G, \mu_n)$ is a consequence of 2.2. Let $N = \ker\varphi$. We prove that $[N, N] \subseteq C_n$, $N^n \subseteq C_n$. If we consider $g \in N$ then $\varphi(g) = \bar{1}$ so $[h, h'] = hh'h^{-1}h'^{-1} \in S_1$ for all $h, h' \in N$, this implies that the group generated by all commutators is in the group generated by

S_1, and therefore $[N,N] \subseteq C_n$. Moreover we can consider $h \in N$ and $g = 1$, then $\varphi(g) = \bar{1}$, and $n+1 \equiv 1 \mod n$. Therefore we can choose $i = n+1$ and we get

$$ghg^{-1}h^{-i} = h^{1-i} = h^{-n} \in S_1;$$

hence $N^n \subseteq C_n$.
We see that C_n is a normal subgroup of G. Clearly S_2 is stable under conjugacy by elements of G. While $\langle S_1 \rangle$ is normal, in fact for every $g, g' \in G$ and $h \in N$ and $i \equiv \varphi(g) \mod n$, $j \equiv \varphi(g') \mod n$:

$$(g'ghg^{-1}g'^{-1}gh^{-i}g'^{-1})(g'h^ig'^{-1}(h^i)^j) = g'gh(g'g)^{-1}h^{ij}$$

and $ij \equiv \varphi(gg') \mod n$.
The other conditions of 2.4 are satisfied by definition, and the minimality of H_m is also trivial from 2.4.

□

3. A proposition in Neukirch's book

We promised to correct a theorem in [**3**]. Let $k \in \mathbb{Z}_{>0}$ and p be a prime number, consider K a field. We shall write μ_{p^k} for the group of p^k-th roots of unity in an algebraic closure $\bar{K}$.
The *wrong* statement is the following. Let p be a prime, $k \in \mathbb{Z}_{>0}$, and let K be any field with $\operatorname{char} K \neq p$. Let $G = \operatorname{Gal}(K(\mu_{p^k})/K)$. Then the group

$$\hat{\mathrm{H}}^i(G, \mu_{p^k}) = \{1\} \text{ for all } i \in \mathbb{Z},$$

except when $p = 2$, $k \geq 2$, $\operatorname{char}(K) = 0$ and $K \cap \mathbb{Q}(\mu_{2^k})$ is real. In this exceptional case $\hat{\mathrm{H}}^i(G, \mu_{2^k})$ has order 2 for all $i \in \mathbb{Z}$.

Now, consider K of $\operatorname{char} K = q \neq 0$. We denote with $\mathbb{F}_q$ the finite field with q elements. Using the fundamental theorem of Galois theory, it can be seen that the restriction induces an isomorphism

$$\operatorname{Gal}(K(\mu_{2^k})/K) \cong \operatorname{Gal}(\mathbb{F}_q(\mu_{2^k})/K \cap \mathbb{F}_q).$$

Therefore $\operatorname{Gal}(K(\mu_{2^k})/K) \leq \operatorname{Gal}(\mathbb{F}_q(\mu_{2^k})/\mathbb{F}_q) = \langle q \rangle$ where q is the Frobenius automorphism: $q : a \mapsto a^q$ for all $a \in \mathbb{F}_q(\mu_{2^k})$. Hence in the case of $p = 2$ and *positive* characteristic, the two conditions $q \equiv -1 \mod 2^k$ and $\mu_{2^k} \nsubseteq K$ are equivalent to say that $\operatorname{Gal}(K(\mu_{2^k}/K) \subseteq \operatorname{Aut}(\mu)$ is generated by $-1 : \zeta \mapsto \zeta^{-1}$ for all $\zeta \in \mu$. Statement here above implies that cohomology ought to be trivial, but a simple computation based on 1.23 tells us that $\hat{\mathrm{H}}^i(G, \mu_{p^k})$ has order 2. Here it is a correct version of the aforestated proposition.

2.7. Proposition. *Let p be a prime, $k \in \mathbb{Z}_{>0}$, and let K be any field with* $\operatorname{char} K \neq p$. *Let $G = \operatorname{Gal}(K(\mu_{p^k})/K)$. Then the group*

$$\hat{\mathrm{H}}^i(G, \mu_{p^k}) = \{1\} \textit{ for all } i \in \mathbb{Z},$$

except when $p = 2$, $k \geq 2$, and

- *either* $\operatorname{char}(K) = 0$ *and $K \cap \mathbb{Q}(\mu_{2^k})$ is real;*
- *or* $\operatorname{char}(K) \equiv -1 \mod 2^k$ *and $\mu_{2^k} \nsubseteq K$.*

In these exceptional cases $\hat{\mathrm{H}}^i(G, \mu_{p^k})$ has order 2 for all $i \in \mathbb{Z}$.

4. Non prime-power radicals

What we have done up to now referred only to the case of prime-powers radicals. However 2.6 allows us to make a step into the case of general n.
As usual, we have our base field K, and a finite Galois extension E with the property that the n-th roots of 1 contained in E are n, where this time $n \in \mathbb{Z}_{>1}$. We factor n into pairwise-coprime prime powers, let P be the set of prime divisors of n; then we write $n = \prod_{p\in P} p^{e_p}$. It is clear that $\alpha \in E$ is an n-th radical *if and only if* $\alpha = \prod_{p\in S\subseteq Q} \alpha_p$, with α_p being a p^{e_p}-th radical of K for all $p \in S$. This means that the largest intermediate field generated by n-th radicals is the join of all largest intermediate fields generated by p^{e_p}-th radicals. This immediately gives us the following.

2.8. Theorem. *Let $n \in \mathbb{Z}_{>1}$. Consider a field K and finite Galois extension $E \supseteq K$ such that the subgroup $\mu_n \subseteq L^*$ of all n-th roots of 1 has order n . Let M be defined as above. For each $m \in M$ consider μ_m the group of m-th roots of unity in E. Then, the largest intermediate field L generated by n-th radicals of K, has Galois group:*

$$\mathrm{Gal}(E/L) = \mathrm{C}(G, \mu) = \bigcap_{m\in M} \mathrm{C}(G, \mu_m)\,.$$

5. Infinite Galois extension

What we have seen up to now concerns only *finite* Galois extensions; we shall now drop the finiteness hypothesis.

2.9. Definition. Let G, N be topological groups. A *continuous left action* of G on N is a group homomorphism $\varphi : G \to \mathrm{Aut}(N)$, such that the map $G \times N \to N$ defined by

$$(g, n) \mapsto \varphi(g)(n)$$

is continuous.
In this situation, we also say that G *acts continuously* on N, and for all $g \in G$ and $n \in N$, we write

$$^g n = \varphi(g)(n).$$

2.10. Remark. If N is Hausdorff, the kernel of a continuous action is a *closed* subgroup because we have

$$\ker\varphi = \bigcap_{n\in N} \{g \in G |\, ^g n = n\}.$$

That is, $\ker\varphi$ is an intersection of closed subgroups, and therefore closed.

2.11. Definition. Let G be a topological group. A *continuous* G-module μ is a topologigal abelian group μ toghether with a continuous action of G on μ.

2.12. Definition. Let G and μ be two profinite groups with G acting on μ. We define $\mathrm{Z}^1_{\mathrm{C}}(G, \mu)$ to be the set of all continuous cocycles $G \to \mu$. As for the finite case, when mu is abelian $\mathrm{Z}^1_{\mathrm{C}}(G, \mu)$ is a group with the pointwise multiplication.

2.13. Definition. Let G be a profinite group and let μ be a continuous G-module. We define:

$$\mathrm{C}_{\mathrm{C}}(G, \mu) = \bigcap_{q\in \mathrm{Z}^1_{\mathrm{C}}(G,\mu)} \ker q$$

If G is a profinite group and μ is a continuous G-module then $\mu \rtimes G$ endowed with the product topology is a profinite group too. In the following, it is intended that all finite groups are equipped with the discrete topology. We can prove an analogue of 1.13.

2.14. Lemma. *Let G be a profinite group and let N be a closed normal subgroup of G. Consider a finite G-module μ . Let $c : N \to \mu^N$ be a G-homomorphism (G acting continuously by conjugacy on N). Then:*

$$H_c = \{(c(x), x^{-1}) | x \in N\}$$

is a closed normal subgroup of $\mu^N \rtimes G$.

Proof. The map:

$$\begin{aligned} f_c : \ N &\longrightarrow \mu^N \rtimes G \\ x &\longmapsto (c(x)^{-1}, x) \end{aligned}$$

is a continuous homomorphism, so H_c is a closed subgroup because it is image of a compact group N through f_c which is continuous. The proof of the fact H_c is normal descends from 1.12. □

2.15. Proposition. *Let G be a profinite group and let μ be a finite G-module on which G acts continuously via φ. Consider $N = \ker \varphi$, and let $c : N \to \mu$ be a continuous G-homomorphism (G acting continuosly by conjugacy on N). Consider $H_c = \{(c(x), x^{-1}) | x \in N\}$, and define*

$$E_c = \frac{\mu \rtimes G}{H_c}.$$

Then we have:

1. *There are continuous group homomorphisms: $\iota_c : \mu \to E_c$ and $\pi_c : E_c \to G/N$ defined by*

   $$\iota_c : m \mapsto (m, 1)H_c \qquad\qquad \pi_c : [(m, g)] \mapsto gN$$

   and $\psi : G \to E_c$ defined by

   $$\psi : x \mapsto [(1, x)] = (1, x)H_c$$

   such that in the diagram

   $$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \xrightarrow{\pi} & G/N & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle \psi} & & \| & & \\ 1 & \longrightarrow & \mu & \xrightarrow{\iota_c} & E_c & \xrightarrow{\pi_c} & G/N & \longrightarrow & 1 \end{array} \tag{2.2}$$

   all squares are commutative and the bottom row is a short exact sequence.
2. *The bottom row splits if and only if c extends to a continuous cocycle*

   $$\tilde{c} : G \longrightarrow \mu.$$

Proof. The bottom row is a short exact sequence by 1.13. All groups appearing in the bottom row are finite, because μ and G/N are finite by hypothesis. Therefore π_c and ι_c are continuous too. The proof that ψ is continuous depends on the fact that ψ factors through an embedding and a projection modulo the normal subgroup H_c, which is closed, as 2.14 proves.
The rest is proved similarly to 1.13 using continuous maps. □

Thanks to this proposition we can prove the following.

2.16. Lemma. *Let G be a profinite group and let μ be a finite G-module on which G acts continuously via φ. Define $N = \ker \varphi$ and consider G acting by conjugacy on it. For $c \in \mathrm{Hom}_G(N, \mu)$ continuous consider E_c as described in 2.15. Then we*

have that for $q \in \mathrm{Z}^1_{\mathrm{C}}(G,\mu)$ *the restriction* $q_{|N}$ *is a continuous* G*-homomorphism, and*

$$\mathrm{C}_{\mathrm{C}}(G,\mu) = \bigcap_{\substack{c \in \mathrm{Hom}_G(N,\mu) \\ \text{continuous} \\ E_c \text{ splits}}} \ker c.$$

As done before we can now switch to field theory. Consider a field K and $n \in \mathbb{Z}_{>1}$. We shall consider a Galois extension $L \supseteq K$ such that the subgroup $\mu \subseteq L^*$ of n-th roots of unity has order n. In this setting, we shall write $G = \mathrm{Gal}(L/K)$; thus we will have a continuous action of G on μ that we shall call φ. As before we have to find out the correspondence between n-th radicals and cocycles $G \to N$. This is done with the following.

2.17. Lemma. *Let* K *be a field and* $n \in \mathbb{Z}_{>1}$. *Consider* L *a Galois extension of* K *such that* $\mathrm{char}\, K \nmid n$. *Then, there is an isomorphism* $\eta : (L^*/K^*)[n] \xrightarrow{\sim} \mathrm{Z}^1_{\mathrm{C}}(G,\mu)$ *defined by* $\eta(\alpha K^*) : \sigma \mapsto \frac{\sigma\alpha}{\alpha}$. *Moreover,* $\mathrm{Gal}(L/K(\alpha)) = \ker \eta(\alpha K^*)$ *for* $\alpha \in E^*$ *such that* $\alpha^N \in K$.

Proof. The proof is the same as 2.2 except that we use the version of Hilbert's 90 for infinite Galois extensions (Theorem 3.18 in [**4**]). □

Now it is immediate to see the following.

2.18. Proposition. *Consider a field* K *and* $n \in \mathbb{Z}_{>0}$. *Let* $L \supseteq K$ *be a Galois extension of* K *such that the subgroup* $\mu \subseteq L^*$ *of all* n*-th roots of* 1 *has order* n. *Let* $G = \mathrm{Gal}(L/K)$ *acting continuously on* μ *via* φ. *Then, the extension* L *is the splitting field of a* collection *of polynomials* $\{x^n - a_i\}_{i\in I}$ *with* $a_i \in K$ if and only if

$$\mathrm{C}_{\mathrm{C}}(G,\mu) = \{1\}.$$

Now we restrict to the case of $n = p^k$ for p prime and $k \in \mathbb{Z}_{>0}$. We shall consider a Galois extension $L \supseteq K$ such that the subgroup $\mu \subseteq L^*$ of n-th roots of unity has order n. In this setting, we shall write $N = \mathrm{Gal}(L/K(\mu)) = \ker \varphi$. We identify $\mathrm{Aut}(\mu)$ and $(\mathbb{Z}/n\mathbb{Z})^*$. Thus $G/N \cong \varphi(G) \subseteq \mathrm{Aut}(\mu)$ and hence 2.15 can be applied. As before, we define $\delta = -1 + n\mathbb{Z} \in \mathrm{Aut}(\mu)$. Furthermore the groups $\hat{\mathrm{H}}^i(G/N,\mu)$ have already been calculated so the conditions for E_c are the same seen in 1.32.

2.19. Theorem. *Consider a field* K *and* $n = p^k$ *for* p *a prime number and* $k \in \mathbb{Z}_{>0}$. *Let* $L \supseteq K$ *be a Galois extension of* K *such that the subgroup* $\mu \subseteq L^*$ *of all* n*-th roots of* 1 *has order* n. *Let* $G = \mathrm{Gal}(L/K)$ *be acting continuously on* μ *via* $\varphi : G \to (\mathbb{Z}/n\mathbb{Z})^*$. *Define* $N = \ker\varphi$. *Then, the Galois extension* L *is the splitting field of a* collection *of polynomials*

$$\{x^n - a_i\}_{i\in I}$$

with $a_i \in K$ if and only if

i. N *is abelian and its exponent divides the order of* μ,
ii. for all $g \in G$ *and* $h \in N$, *we have* $ghg^{-1} = h^i$ *with* $(i \bmod n) = \varphi(g)$;
iii. in case $n = 2^k$ *with* $k \geq 2$ *and* $\delta \in \varphi(G)$, *we have an element* $\sigma \in G$ *such that* $\varphi(\sigma) = \delta$ *and* $\sigma^2 = 1$.

Proof. Again we try to prove that $\mathrm{C}_{\mathrm{C}}(G,\mu) = \{1\}$ if and only if the three conditions hold. The fact that $\mathrm{C}_{\mathrm{C}}(G,\mu) = \{1\}$ implies *i*, *ii* and *iii* is because $[N,N] \cup N^n \subseteq \mathrm{C}_{\mathrm{C}}(G,\mu)$ and because of 2.16.
Conversely the three conditions imply that for each $x \in N$ there is a continuous G-homomorphism $c : N \to \mu$ such that E_c of 2.15 splits and $c(x) \neq \bar{1}$. In fact, we

are assuming that N is profinite abelian and of exponent dividing n, this implies that

$$\bigcap_{\substack{U \text{ open normal} \\ \text{subgroup}}} U = \{1\}.$$

This implies that for every $x \in N$ there is U open normal subgroup such that $x \notin U$. Hence we have N/U finite, abelian and of exponent dividing n and for $\bar{h} \in N/U$, $g \in G$ and for $(i \bmod n) = \varphi(g)$ we have

$$g\bar{h}g^{-1} = \bar{h}^i.$$

Therefore there is a G-homomorphism $\bar{c} : N/U \to \mu$ such that $\bar{c}(xU) \neq \bar{1}$. Consider the projection $\pi : N \to N/U$, we can define c as follows:

$$\begin{array}{ccc} N & \xrightarrow{c} & \mu \\ & \searrow^{\pi} & \uparrow{\scriptstyle \bar{c}} \\ & & N/U \end{array} .$$

The function just defined is a G-homomorphism because $\bar{c}$ is a G-homomorphism, it is continuous because π is continuous and E_c splits because of *iii*. Moreover $c(x) = \bar{c}(xU) \neq \bar{1}$. □

And as before we get the following corollary.

2.20. Corollary. *Consider a field K and $n = p^k$ for p a prime number and $k \in \mathbb{Z}_{>0}$. Let $E \supseteq K$ be a Galois extension of K such that the subgroup $\mu_n \subseteq E^*$ of all n-th roots of 1 has order n. Let $G = \mathrm{Gal}(E/K)$, and $\varphi : G \to (\mathbb{Z}/n\mathbb{Z})^*$ the action of G on μ_n. We define two sets:*

$$S_1 = \{ghg^{-1}h^{-i} | g \in G,\ h \in \ker\varphi,\ (i \bmod n) = \varphi(g)\},$$
$$S_2 = \{g^2 \in G | \varphi(g) = \delta\}.$$

Let L_n be the largest intermediate field between K and E generated by n-th radicals of K, i.e.

$$L_n = K(\alpha \in E^* | \alpha^n \in K).$$

Then:

$$\mathrm{Gal}(E/L_n) = \mathrm{C}_{\mathrm{C}}(G, \mu_n) = \mathrm{cl}_G(\langle S_1 \rangle \cdot \langle S_2 \rangle),$$

the closure of $\langle S_1 \rangle \cdot \langle S_2 \rangle$.

Bibliography

[1] M. F. Atiyah and C. T. Wall. Cohomology of groups. In J. W. S. Cassels and A. Fröhlich, editors, *Algebraic Number Theory*. Academic Press, 1967.

[2] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*. Springer-Verlag, Berlin Heidelberg New York, 2nd edition, 1990.

[3] Alexander Schmidt Jürgen Neukirch and Kay Wingberg. *Cohomology of number fields*. Springer-Verlag, Berlin Heidelberg New York, 2000.

[4] Helmut Koch. *Galois theory of p-extensions*. Springer-Verlag, Berlin Heidelberg New York, 2002.

[5] Jean Pierre Serre. *Galois cohomology*. Springer-Verlag, Berlin Heidelberg New York, 2002.

[6] Sep Thijssen. Computing torsion in field extensions. Master's thesis, Radboud University Nijmegen, 2010.

[7] Charles A. Weibel. *An introduction to homological algebra*. Cambridge University Press, Cambridge, 1994.