Group Cohomology and Algebraic Number Theory

—

3rd Year Research Internship
Ecole Polytechnique

Raphaël Kalfon

February 8, 2023

0.1 Acknowledgements

My dearest thanks go to **David Harari**, professor at the Paris-Sud University, without whom the writing of this document would not have been possible. Mr.Harari took me through the most technical intellectual meanders of this theory with remarkable clarity and kindness. He never refused to share his time with me, and always did so with enthusiasm. Working with him was a pleasure.

I would also like to particularly thank **Diego Izquierdo** for putting us in touch, as well as for his initial guidance and support through the mysteries of homological algebra in preparation of my work with David.

My final thanks go to the **Ecole Polytechnique**'s work and internships department, the SOIE, for giving me the opportunity of doing such interesting work in this third year of study.

0.2 Content

This document compiles notes written between March and July 2022. The subjects treated range across various points of algebra and number theory, with in view the prospect of understanding local class field theory through the scope of Galois Cohomology. The topics covered are as follows :

- The first chapter covers the main points of **homological algebra** used across this paper, from the most basic definitions to the theory of derived functors, δ-functors, and spectral sequences.
- The second, shorter chapter consists in a few reminders about profinite groups.
- The third chapter devises an **introduction to group cohomology**, and the main tools used to study it. We start with the case of **finite groups**, and introduce the explicit description, induction methods, change of groups, restriction and corestriction. In a second part, we introduce **modified cohomology** and the essential new results it offers on the subject. In a third part, we introduce the **cohomology of profinite groups**, which is essential to study the cohomology of Galois modules. We finish this chapter by an introduction to the theory of the **cohomological dimension** of a group.
- The fourth chapter marks a break with the purely algebraic first chapters, and turns to matters closer to number theory, with a complete introduction to Galois Theory.
- The fifth chapter says a little bit about local fields and their structure.
- The sixth chapter establishes a bridge between the second and the third chapter. It is an introduction to **Galois cohomology**.

The second and fourth chapter very closely follows David Harari's approach in his book **Galois Cohomology and Class Field Theory**, which was my main source on the matter. Similarly, the third chapter is almost entirely derived from Neukirch's treatment of the matter, in the second chapter, with perhaps a little more focus on concrete examples and a correction to exercises.

0.3 How to Read

This document is designed as a first course on the subjects upon which it touches, and can be read linearly. Most proofs are complete : only the longest, most technical ones, that I do not deem enlightening for an introductory course are excluded.

Here's my color-code : in **green boxes**, you will find definitions. In **blue boxes**, propositions. In **red boxes**, theorems. The distinction between the former two statements is subjective : propositions generally have relatively simple proofs, and their conclusions aren't so far reaching. Theorems often have longer proofs, though not necessarily : they are awarded with this title in regard with how far-reaching and structural their consequences are. Finally, in **yellow boxes**, you will find exercises. Exercises are very important to me: they are at the same time entertaining and critical for learning about anything in mathematics. They are all given with a solution. You should try all of them, and not look to the solution without having been stuck for at least twenty minutes : it is only when stuck that the deepest learning is achieved. The exercises' difficulty is denoted by asterisks : *.

- * : the exercise is a silly remark that should seem fairly evident.
- ** : the exercise might not be easy for a first read, but should be evident after having been seen once or twice.
- *** : the exercise requires a bit of thinking / intuition, and might be difficult in a first approach.
- **** : the exercise holds a substantial difficulty. These exercises are not intended to be solved in an introductory reading. However, they are excellent training as research problems.

0.4 Prerequisites

In order to make the reading of this document most pleasent, our advice regarding the prior knowledge to have acquired is as so:

- The basic language of category theory (functors, natural transformation, natural isomorphisms, adjunctions, limits...) is necessary, though not further that at a basic level. The first chapter of Riehl's **Category Theory**, as well as the definition and basic properties of limits and adjunction is sufficient. Some basic knowledge of abelian categories is also desirable, more for its vocabulary than for its techniques.
- A solid familiarity with the first four chapters of Atiyah and MacDonald's excellent book **Commutative Algebra** will be assumed : the vocabulary of rings, ideals, modules will be used without restriction.
- A previous exposure to any theory of (co)homology is desirable, though not absolutely necessary. Weibel's first chapter of his book on **Homological Algebra** is a good secondary source to follow on the matter. The first chapter gives a detailed review on these subjects anyway.
- In terms of number theory, knowledge of Galois theory (finite and infinite) will be assumed. The Galois theory used in this book doesn't go further than Morandi's treatment in **Galois Theory**, which is an excellent reference on the matter. For other algebraic number theoretic matters, knowledge of the first chapter of Neukirch's excellent **Algebraic Number Theory** will be assumed.
- Knowledge of profinite groups, of their topology and of their main properties (generalized cardinals, quotients, etc) is assumed.

0.5 Apologies

I sincerely apologize for any error, incompleteness, or obscurity in my proofs, statements and notations. I first wrote this document as notes to myself as I was learning those subjects, which I believe has advantages and disadvantages for an external reader. The main advantage is that the point of view adopted is not clouded by heaps of much deeper knowledge that could result in a hasty treatment of certain points easy to understand with hindsight but not in a first approach. I have tried to be as pedagogical as possible. The obvious disadvantage is that the subjects might be treated with a lack of hindsight, and of course, with possibly major errors. I thus apologize for the headaches they might cause you, though I believe that when learning mathematics, some headaches are ultimately very beneficial.

Chapter 1

Homological Algebra

In all of this chapter, R is a commutative ring with 1. Most of the content can be found in less detailed terms in the book [5]. For category theoretic prior language, one may turn to [3].

1.1 Exact Sequences and Chain Complexes

In order to make this text more readable for the inexperienced reader, we restrict our use of the language of abelian categories, although they are doubtlessly more general and flexible thatn the one of R-modules.

1.1.1 Exact Sequences

This is about the most fundamental object of homological algebra.

Definition : Exact Sequence

Let $(A_i, f_i)_{i\in\mathbb{Z}}$ be a sequence of R-modules and morphisms, with $f_i : A_i \to A_{i+1}$. The sequence is **exact** if for all i, $\ker f_i = \text{Im } f_{i-1}$.

An exact sequence is often represented as a diagram with the following form:

$$\ldots \xrightarrow{f_{i-2}} A_{i-1} \xrightarrow{f_{i-1}} A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} \ldots$$

Isomorphisms and morphisms give rise to exact sequences where almost all terms are zero, and are written simply in the following way:

$$0 \longrightarrow A \xrightarrow{f_{i-1}} B \longrightarrow 0$$

$$0 \longrightarrow \ker f \xrightarrow{i} A \xrightarrow{f} B \xrightarrow{p} \text{coker} f \longrightarrow 0$$

The first sequence being exact is equivalent to f being an isomorphism. The second sequence where of course, i is an inclusion and p is a projection, holds and is exact for any morphism f.

Other examples are given by the zero sequence, or the following sequence :

$$\ldots \xrightarrow{i} A \xrightarrow{1_A} A \xrightarrow{p} 0 \xrightarrow{i} A \xrightarrow{1_A} A \xrightarrow{p} 0 \xrightarrow{i} A \xrightarrow{1_A} A \xrightarrow{p} \ldots$$

Checking those assumptions is a good introductory exercise. Another good exercise is to prove the elementary proposition :

Proposition : Zeroes, Injectivity, Surjectivity

If $(A_i, f_i)_{i\in\mathbb{Z}}$ is an exact sequence, and $A_{i+1} = 0$, then f_{i-1} is surjective and f_{i+1} is injective. So in a subsequence of the type $0 \to A \to B \to 0$, the arrow between A and B is an isomorphism.

Proof : Formal, immediately follows from the definition.

We call **short exact sequences** exact sequences where exactly 3 terms are non-zero. They are written as :

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

...which is just another way of writing that f is injective, g is surjective and that $\text{Im } g = \ker f$ (which is stronger than just $g \circ f = 0$). When A, B and C are R-modules, it is the same thing than to say that $C \cong B/A$ (viewing A as a submodule of B thanks to the injective arrow f), thanks to the first isomorphism theorem (which also holds in any abelian category, in the form that the co-image of f is isomorphic to the image of f).

Exercise : Exact Sequence of Finite Modules **

Let $A_0, ..., A_n$ be a finite sequence of modules, and suppose there is an exact sequence :

$$0 \to A_0 \to A_1 ... A_{n-1} \to A_n \to 0$$

Prove that $\frac{\prod_{0\leq i\leq n/2} |A_{2i}|}{\prod_{1\leq i\leq (n+1)/2} |A_{2i-1}|} = 1$.

Proof : an easy induction from the equality for any morphism $A \xrightarrow{f} B$, $|\textbf{\textit{Im}}\ f| = |A|/|\textbf{\textit{Ker}}\ f|$.

1.1.2 Split Exact Sequences

Definition : Split Exact Sequences

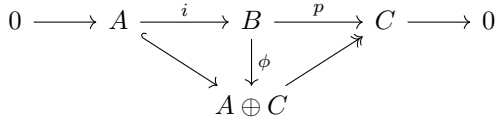
A short exact sequence $0 \to A \underset{i}{\to} B \underset{p}{\to} C \to 0$ is said to be **split** if either one of the three equivalent properties are verified :

- $\exists s : C \to B$, $p \circ s = 1_C$
- $\exists t : B \to A$, $t \circ i = 1_A$
- $\exists \phi : B \cong A \oplus C$, where $\phi \circ i$ and $p \circ \phi^{-1}$ are the canonical morphisms from $A \oplus C$ to A and C.

Proof : 3 $\implies$ 1 and 2 is natural by composing ϕ or ϕ^{-1} with the canonical maps $A \oplus C \to A$ and $C \to A \oplus C$. To prove that 1 $\implies$ 3 define $b \mapsto (i^{-1}(b - s \circ p(b)), p(b))$, the first term being well defined by exactness. Immediate to see it is a morphism. To see it is surjective, consider $i(a) + p \circ s(c)$. To see it is injective, use exactness and explicit form.

To prove that 2 $\implies$ 3 define $b \mapsto (t(b), p(b))$. It is clearly a morphism. Surjectivity comes from considering $i(a) + u - i \circ t(u)$ where u is a pre-image of an element $c \in C$. Injectivity comes easily by using exactness.

The last of those properties, the most important, can be summarized in the following diagram :



If there's a name for such an object, it means that some sequences aren't split. For example, take the following sequence of $\mathbb{Z}$-modules :

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

... where the arrows are the canonical inclusion and quotient arrows. We do not have $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ for obvious order reasons.

1.1.3 Chain Complexes

Definition : Chain and Cochain complexes

A **chain complex** $C_\bullet$ of R-modules (or of objects in any abelian category !) is a sequence of R-modules $(A_i, \partial_i)_{i\in\mathbb{Z}}$ with $\partial_i : A_i \to A_{i-1}$, and $\partial_i \circ \partial_{i+1} = 0$. The operators ∂ are called the **differential operators**.

A **cochain complex** $C^\bullet$ is defined in the same way, but with $\partial^i : A^i \to A^{i+1}$ and $\partial^{i+1} \circ \partial^i = 0$.

Cochain and chain complexes really aren't that different. Any chain complex can be turned into a cochain complex (and conversely) by switching all indexes i to $-i$. To differentiate them, cochain complexes most of the time have supscripts (∂^i) while chain complexes have subscripts (∂_i). All exact sequences are obviously chain (and cochain complexes, depending on the indexation), but the converse is not true. One has for example the chain complex :

$$... \longrightarrow 0 \longrightarrow M \longrightarrow 0 \longrightarrow M \longrightarrow 0 \longrightarrow M \longrightarrow 0 \longrightarrow M \longrightarrow ...$$

... for any R-module M, which is not exact as soon as M is not the zero module.

Chain and cochain complexes come with their morphisms. The definition will only be given for chain complexes, but one will very easily extrapolate this definition to cochain complexes.

Definition : Morphisms of Chain Complexes

Let $C_\bullet$ and $D_\bullet$ be two chain complexes. A **morphism of chain complexes** f between $C_\bullet$ and $D_\bullet$ is a sequence of morphism $(f_i)_{i\in\mathbb{Z}}$, $f_i : C_i \to D_i$, such that $f_i \circ \partial_{C\,i} = \partial_{D\,i+1} \circ f_{i+1}$.

More explicitly, morphisms can be represented in the context of the diagrams representing the complexes :

$$\begin{array}{ccccccccc}
... & \longrightarrow & C_{i+1} & \xrightarrow{\partial_{C\,i+1}} & C_i & \xrightarrow{\partial_{C\,i}} & C_{i-1} & \xrightarrow{\partial_{C\,i-1}} & ... \\
 & & \downarrow{\scriptstyle f_{i+1}} & & \downarrow{\scriptstyle f_i} & & \downarrow{\scriptstyle f_{i-1}} & & \\
... & \longrightarrow & D_{i+1} & \xrightarrow{\partial_{D\,i+1}} & D_i & \xrightarrow{\partial_{D\,i}} & D_{i-1} & \xrightarrow{\partial_{D\,i-1}} & ...
\end{array}$$

The commutativity condition between differentials and components of the morphism is more simply rephrased (and should be understood) by saying that the f_i make all the squares commute. This definition works just as well for cochain complexes.

The next proposition gives an example of why abelian categories are useful.

Proposition : Chain Complexes form an Abelian Category

In the category $R - \mathbf{Mod}$ of R modules, chain (and cochain) complexes with their morphisms form an abelian category.

Proof : This is a formal proof, where everythig is obviously defined and verified.

Here's another lemma, which can be useful from times to times. Its proof is a good introduction to what we call diagram chasing.

Exercise : The Five Lemma ***

Let $M_1 \to M_2 \to M_3 \to M_4 \to M_5$ and $M'_1 \to M'_2 \to M'_3 \to M'_4 \to M'_5$ be two exact sequences of R-modules. In the diagram below, suppose m and p are isomorphisms, l is a monomorphism and q is an epimorphism. Prove that n is an isomorphism (more generally, what you should remember is that if the lines are exact and the four arrows on the sides are isos, then the middle arrow is also an iso).

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_5 \\ \downarrow{\scriptstyle l} & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle q} \\ M'_1 & \xrightarrow{g_1} & M'_2 & \xrightarrow{g_2} & M'_3 & \xrightarrow{g_3} & M'_4 & \xrightarrow{g_4} & M'_5 \end{array}$$

Solution : a bit of a sketch, but roughly : $n(x) = 0 \implies g_3 n(x) = 0 \implies p f_3(x) = 0 \implies f_3(x) = 0$. *Pull back to* y *such that* $f_2(y) = x$, $n f_2(y) = 0 \implies g_2 m(y) = 0$. *Pull back* $m(y)$ *by* z, $g_1(z) = m(y)$. *Pull back to* M_1 *because* l *is an epi, so* $g_1 l(u) = m(y)$ *so* $m(f_1(u)) = m(y)$ *so* $y = f_1(u)$ *and by exactness* $f_2(y) = x = 0$. *Surjectivity is the same sort of nonsense.*

This sort of proof is routine in homological algebra. The goal of homological algebra is somehow to pack up this kind of proof in some kind of theoretical framework, so that they can be directly reinvested when similar situations are stumbled upon in various areas of mathematics (and believe me, it happens).

1.2 Homology and Cohomology

When we have a chain complex, a natural question is, how far is this sequence from being exact ? The interpretation of such a question comes from algebraic topology: to a certain class of nice topological spaces one may associate a chain complex (called the simplicial or singular chain complex). How far the sequence is from being exact actually measures the "holes" present in the topological space, in each dimension. The measure of the distance to exactness is done through homology (or cohomology with cochain complexes).

Definition : Homology and Cohomology groups

Let $C_\bullet$ be a chain complex. The n^{th} **homology object** of $C_\bullet$, denoted $H_n(C)$ for $n \in \mathbb{Z}$, is defined as the object $\ker \partial_i / \text{Im } \partial_{i+1}$.

Let $C^\bullet$ be a cochain complex. The n^{th} **cohomology object** of $C^\bullet$, denoted $H^n(C)$ for $n \in \mathbb{Z}$, is defined as the object $\ker \partial_{i+1} / \text{Im } \partial_i$.

Before moving on to anything else, one must do a few calculations. You are invited to go back to every single example that we have treated so far, and compute the corresponding homology groups. Homology and Cohomology behave well with respect to morphisms. One can easily check that the commutativity relations of chain complex morphisms induce that a partial morphism f_i takes $\ker \partial_{C,i}$ to $\ker \partial_{D,i}$ and $\text{Im } \partial_{C,i+1}$ to $\text{Im } \partial_{D,i+1}$. So whenever you have a morphism $C_\bullet$ to $D_\bullet$, you get a morphism $H_n(f) : H_n(C) \to H_n(D)$. One can easily check that these quotients behave well with respect to composition, so that :

Proposition : Homology and Cohomology are functors

The map $C_\bullet \mapsto H_n(C)$ and $f \mapsto H_n(f)$ assemble into an additive functor from the category of chain complexes over R-modules to R-modules.

Proof : formal.

In many cases, in particular with the applications of chain complexes and homology, one will see that the objects in the chain complex often aren't that important: it is the homology modules which contain all the information. One might come up with the following definition.

Definition : Quasi-isomorphism between chain complexes

Let $C_\bullet$, $D_\bullet$ be chain complexes. A quasi-isomorphism between $C_\bullet$ and $D_\bullet$ is a morphism of chain complexes $C_\bullet \to D_\bullet$ such that for all $n \in \mathbb{Z}$, $H_n(f) : H_n(C) \to H_n(D)$ is an isomorphism.

For example, one will easily check, that the zero map, in this case, defines a quasi-isomorphism.

$$\begin{array}{ccccccccccccc}
\ldots & \longrightarrow & 0 & \longrightarrow & A & \xrightarrow{1_A} & A & \longrightarrow & 0 & \longrightarrow & A & \xrightarrow{1_A} & A & \longrightarrow & \ldots \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\ldots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \ldots
\end{array}$$

1.3 Chain Homotopies

We now introduce a technique that allows us to easily formulate when two morphisms between chain complexes induce the same morphism in homology.

Definition : Chain Homotopies

Let $C_\bullet$ and $D_\bullet$ be two chain complexes. Let f and g be two morphisms between $C_\bullet$ and $D_\bullet$. f and g are said to be homotopic if there exists a morphism (not necessarily of chain complexes) s of degree 1 between $C_\bullet$ and $D_\bullet$ such that $f_n - g_n = \partial_{D,n+1} s_n + s_{n-1} \partial_{C,n}$.

This definition is quite raw, and deserves a bit of explanations. Firstly, a morphism of degree 1 between $C_\bullet$ and $D_\bullet$ is the data of $s_n : C_n \to D_{n+1}$. They can be represented as so, but be careful as the following diagram is **not necessarily commutative**.

$$\begin{array}{ccccccccc}
\ldots & \longrightarrow & C_{n+1} & \longrightarrow & C_n & \longrightarrow & C_{n-1} & \longrightarrow & \ldots \\
 & & \downarrow{\scriptstyle s_{n+1}} & & \downarrow{\scriptstyle s_n} & & \downarrow{\scriptstyle s_{n-1}} & & \\
\ldots & \longrightarrow & D_{n+2} & \longrightarrow & D_{n+1} & \longrightarrow & D_n & \longrightarrow & \ldots
\end{array}$$

More generally, as you may guess, a morphism of degree n between $C_\bullet$ and $D_\bullet$, with $n \in \mathbb{Z}$ is a morphism from the complex $(C_k)_{k\in\mathbb{N}}$ to $(D_{k+n})_{k\in\mathbb{N}}$. In order not to be confused with the way in which morphisms are positioned with respect to one another, it might be useful to remember the following **non commutative** diagram:

$$\begin{array}{ccccccccc}
\ldots & \longrightarrow & C_{n+1} & \longrightarrow & C_n & \xrightarrow{\partial_{C,n}} & C_{n-1} & \longrightarrow & \ldots \\
 & & {\scriptstyle g_{n+1}}\downarrow\downarrow{\scriptstyle f_{n+1}} & \swarrow^{s_n} & {\scriptstyle g_n}\downarrow\downarrow{\scriptstyle f_n} & \swarrow^{s_{n-1}} & {\scriptstyle g_{n-1}}\downarrow\downarrow{\scriptstyle f_{n-1}} & & \\
\ldots & \longrightarrow & D_{n+1} & \xrightarrow{\partial_{D,n+1}} & D_n & \longrightarrow & D_{n-1} & \longrightarrow & \ldots
\end{array}$$

... and remembering that adding the two loops $C_n \to D_{n+1} \to D_n$ and $C_n \to C_{n-1} \to D_n$ gives you $f_n - g_n$. We then have the following proposition, which is not too hard to prove.

Proposition : Homotopic Maps induce the same map in Homology

If f and g are homotopic, then $H_n(f) - H_n(g) = 0$ for all $n \in \mathbb{N}$.

Proof : If f is homotopic to 0, then for all $x \in \ker \partial_{C,n}$ the term $s_{n-1}\partial_{C,n}$ dies while the other lies in the image of $\partial_{D,n+1}$ so gets killed. Then use additivity of Homology functor.

1.4 The Fundamental Lemma of Homological Algebra

This is arguably the most important theorem in homological algebra.

Theorem : The Fundamental Lemma Of Homological Algebra

Let C_1, C_2, C_3 be chain / cochain complexes. Suppose there exists an exact sequence $0 \to C_1 \to C_2 \to C_3 \to 0$ (which is simply an exact sequence in the category of chain / cochain complexes). Then, there exists a long exact sequence :

$$... \to H_{n+1}(C_3) \to H_n(C_1) \to H_n(C_2) \to H_n(C_3) \to H_{n-1}(C_1) \to ...$$

...or, in the case of cohomology:

$$... \to H^{n-1}(C_3) \to H^n(C_1) \to H^n(C_2) \to H^n(C_3) \to H^{n+1}(C_1) \to ...$$

In addition, the construction of this long exact sequence is natural, meaning that a morphism of exact sequences yields a morphism between the corresponding long exact sequences.

To make the last part more explicit, say that if there is a morphism of exact sequences, which is a commutative diagram with exact lines :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_1 & \longrightarrow & C_2 & \longrightarrow & C_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \\ 0 & \longrightarrow & D_1 & \longrightarrow & D_2 & \longrightarrow & D_3 & \longrightarrow & 0 \end{array}$$

... then there is a commutative diagram :

$$\begin{array}{ccccccccccc} ... & \longrightarrow & H_{n+1}(C_3) & \longrightarrow & H_n(C_1) & \longrightarrow & H_n(C_2) & \longrightarrow & H_n(C_3) & \longrightarrow & H_{n-1}(C_1) & \longrightarrow & ... \\ & & \downarrow{\scriptstyle H_{n+1}(f_3)} & & \downarrow{\scriptstyle H_n(f_1)} & & \downarrow{\scriptstyle H_n(f_2)} & & \downarrow{\scriptstyle H_n(f_3)} & & \downarrow{\scriptstyle H_{n-1}(f_1)} & & \\ ... & \longrightarrow & H_{n+1}(D_3) & \longrightarrow & H_n(D_1) & \longrightarrow & H_n(D_2) & \longrightarrow & H_n(D_3) & \longrightarrow & H_{n-1}(C_1) & \longrightarrow & ... \end{array}$$

While the existence of maps $H_n(C_1) \to H_n(C_2) \to H_n(C_3)$ is just a consequence of functoriality, there are two very important part to this theorem : the existence of a morphism $\delta_n : H_n(C_3) \to H_{n-1}(C_1)$, and the commutativity of the squares :

$$\begin{array}{ccccccc} ... & \longrightarrow & H_n(C_3) & \longrightarrow & H_{n-1}(C_1) & \longrightarrow & ... \\ & & \downarrow{\scriptstyle H_n(f_3)} & & \downarrow{\scriptstyle H_{n-1}(f_1)} & & \\ ... & \longrightarrow & H_n(D_3) & \longrightarrow & H_{n-1}(D_1) & \longrightarrow & ... \end{array}$$

Proof : This is a typical diagram chasing proof. You may skip it for a superficial read, but we recommend that you delve deep into it at least once. Let's construct the morphism δ_n. Start with the diagram (with exact lines) :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_{n+1} & \xrightarrow{f_{n+1}} & B_{n+1} & \xrightarrow{g_{n+1}} & C_{n+1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \partial_{n+1}} & & \downarrow{\scriptstyle \partial_{n+1}} & & \downarrow{\scriptstyle \partial_{n+1}} & & \\
0 & \longrightarrow & A_n & \xrightarrow{f_n} & B_n & \xrightarrow{g_n} & Cn & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \partial_n} & & \downarrow{\scriptstyle \partial_n} & & \downarrow{\scriptstyle \partial_n} & & \\
0 & \longrightarrow & A_{n-1} & \xrightarrow{f_{n-1}} & B_{n-1} & \xrightarrow{g_{n-1}} & C_{n-1} & \longrightarrow & 0
\end{array}$$

You want to construct an element in $\ker \partial_n \subset A_n$ *from an element in* $\ker \partial_{n+1} \subset C_{n+1}$. *Start with an element in* $x \in C$, $x \in \ker \partial_{n+1}$. *By exactness of the first line pull it back to an element* $y \in B_{n+1}$. *Then push it down with* ∂_{n+1}. *By commutativity* $g_n \partial_{n+1}(y) = 0$, *so you can pull back* $\partial_{n+1}(y)$ *to a unique element of* A_n *by exactness, and voilà : you have an element of* A_n. *It remains to be checked that this element is in* $\ker \partial_n$ *and that this construction is unambiguous in homology and linear (we have made a choice: : y, a pre-image of* $x \in c_n$*).*

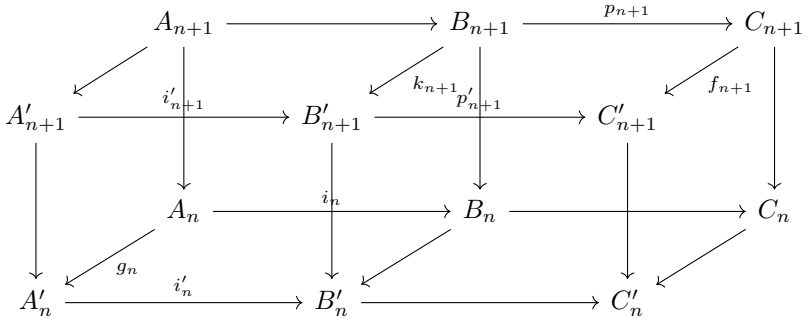
Checking that the element we constructed is in $\ker \partial_n$ *is easy thanks to commutativity of down left square and injectivity of* f_n.

Now we have to check that this construction is unambiguous in homology. There are two things : firstly that the choice of y does not matter, meaning that changing a pre-image y to another y' *only changes the output by an element of Im* $\partial_{n+1} \in A_n$. *This is true becaus if* $y - y' \in \ker g_{n+1}$, *then it is* $f_{n+1}(\Delta)$ *for* $\Delta \in A_{n+1}$. *So pushing it down to* B_n *and taking a pre-image by* f_n *is the same as taking* $\partial_{n+1}(\Delta)$ *by injectivity of* f_n *and commutativity of the upper left square. But* $\partial_{n+1}(\Delta)$ *is a boundary, so the output makes no difference in homology.*

The second check to be made is that an element of Im $\partial_{n+2} \in C_{n+1}$ *is sent to a boundary in* A_n. *This requires adding an upper line with complexes in degree* $n+2$ *to our diagram, and noticing that if* $x = \partial_{n+2}(u)$, *one can take a pre-image* v *of* u *by* g_{n+2}, *and then chose* $\partial_{n+2}(v)$ *as a pre-image for* x. *The following push-down to* B_n *will thus kill it, and* x *will be sent to* 0.

Now that we have proven that this construction is well defined in homology, it is not hard to see that it is also linear, by just seeing that every step of the construction is linear.

Naturality remains to be proven. Disclaimer : you are not conceptually missing anything if you stop reading the proof now, however it is a good exercise of diagram chasing, and involves the pretty fully commutative diagram :



To make it more understandable, I did not include the boundaries, did not include the zeroes (but the lines are all exact !), and only wrote the names of the morphisms we will use.

We want to prove that those two constructions commute in homology : starting with $x \in C_{n+1}$, *taking a pre-image y by* p_{n+1}, *then taking* $\partial_{n+1}(y)$, *taking a pre-image by* i_n *noted u and then applying* g_n... *is the same as firstly taking* $f_{n+1}(x)$, *then taking a pre-image* y' *by* p'_{n+1}, *taking* $\partial'_{n+1}(y')$, *and then taking a pre-image by* i'_n *called* u'. *One now has to show that* $u' - g_n(u) = \partial'_{n+1}$ *of something.*

In order to do this, first note that by commutativity of some squares $i'_n(g_n(u) - u') = \partial'_{n+1}(k_{n+1}(y) - y')$. *Then by commutativity of some other squares,* $p'_{n+1}(k_{n+1}(y) - y') = 0$ *so* $k_{n+1}(y) - y' = i'_{n+1}(\Delta)$. *Now we have by commutativity of another square* $\partial'_{n+1}(k_{n+1}(y) - y') = \partial'_{n+1}(i'_{n+1}(\Delta)) = i'_n(\partial_{n+1}(\Delta))$. *Then by injectivity of* i'_n *we get that* $g_n(u) - u'$ *is indeed a boundary.*

1.5 Exact Functors

Definition : Left, Right Exact Functors

Let F be a **covariant** functor from R-**Mod** $\to R$-**Mod**. We say F is **left exact** if for every short exact sequence $0 \to A \to B \to C \to 0$, the sequence $0 \to F(A) \to F(B) \to F(C)$ is exact. If F is **contravariant** instead, F is left exact if the sequence $0 \to F(C) \to F(B) \to F(A)$ is exact.

We say F is **right exact** if for every short exact sequence $0 \to A \to B \to C \to 0$, the sequence $F(A) \to F(B) \to F(C) \to 0$ is exact. If F is **contravariant** instead, F is right exact if the sequence $F(C) \to F(B) \to F(A) \to 0$ is exact.

We say F is **exact** if it is both right exact and left exact.

To remember the definitions, remember that where the 0 is conserved in the spectral sequence is always the same as the direction indicated in the denomination of the functor. An intuitive way to remember covariant right exact functors is that they preserve surjections. Similarly, a left exact functor functor preserves injections.

Exercise : Left and Right Exact Functors, Injections and Surjections **

Prove that covariant left / right exact functors preserve injections / surjections.

Solution : we do it for the left exact case. f injective is equivalent to the sequence $0 \to A \xrightarrow{f} B \to$ coker f being exact. Now apply the functor F and conclude.

Trivially, the zero functor is exact (but isn't that interesting). There are other trivial examples, such as the one that sends and R-module A to $\oplus_{i\in I} A$ and duplicates morphisms componentwise. Let's give the two non-trivial examples we will focus on.

1.5.1 The $\_ \otimes B$ functor

Let $B \in R - \mathbf{Mod}$. It is not hard to check that for any module $A \in R - \mathbf{Mod}$, the map $A \mapsto A \otimes B$ and the map $f \in \mathbf{Hom}_{R-\mathbf{Mod}}(C, D) \mapsto f \otimes 1_B \in \mathbf{Hom}_{R-\mathbf{Mod}}(C \otimes B, D \otimes B)$ defines a covariant endofunctor in $R - \mathbf{Mod}$.

Proposition : $\_ \otimes B$ is right exact

The functor $\_ \otimes B$ is right-exact, but not necessarily left exact.

Suppose $0 \to A \underset{i}{\to} A' \underset{p}{\to} A'' \to 0$ is exact. Clearly, since p is surjective, $p \otimes 1_B$ defines a surjection $A' \otimes B \to A'' \otimes B$. It is also clear that Im $(1_B \otimes i) \subset \ker(1_B \otimes p)$. The only non trivial thing to prove is the equality.

In order to prove it, let $\hat{p} : A' \otimes B/Im\ (1_B \otimes i), \overline{a' \otimes b} \mapsto p(a') \otimes b$. This is a well defined morphism, to which we can construct an inverse. Consider the map $A'' \times B \to A' \otimes B/Im\ (1_B \otimes i), (a'', b) \mapsto \overline{a' \otimes b}$, with a' such that $p(a') = a''$. Thanks to the quotient, the choice of a' does not matter, which makes this a well defined bilinear map. It is then easy to check that this factors into a map $A'' \otimes B \to A' \otimes B/Im\ (1_B \otimes i)$ that is an inverse for $\hat{p}$.

For the non left-exactness, consider the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ and apply a tensor product by $\mathbb{Z}/2\mathbb{Z}$. Since $\mathbb{Q} \otimes \mathbb{Z}/2\mathbb{Z} = 0$ and $\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$, the first arrows of the resulting sequence are $0 \to \mathbb{Z}/2\mathbb{Z} \to 0$, which is not the beginning of an exact sequence.

Exercise : Flat Modules ***

An R-module B is called flat if the functor $\_ \otimes B$ is exact. Prove that a free module is flat. Prove that if R is a PID, being flat and being without torsion is the same. *You may accept the fact that the direct limit functor is an exact functor in the category of inductive system of R-modules.*

Solution : A free module B is a direct sum of a given number of copies of R. So by commutativity of the tensor product with direct sums, tensorization with B maps an object to the same number of copies of itself, and duplicates morphisms. It is easy to check that this functor is exact.

It is clear that being flat implies not having torsion (because else $\mathbb{Z} \to \mathbb{Z}$ by multiplication by n would be rendered non injective by tensorisation). Now if a finitely generated module does not have torsion on a PID, then it is free. So it works for finitely generated modules. Then for an arbitrary torsion-free module, note that it is the direct limit of its finitely generated modules. Conclude by commutativity of tensor product with direct limits, and by exactness of the direct limit functor.

1.5.2 The Hom$(B, _)$ and Hom$(_, B)$ functors

Recall that if B is an R-module, we can define two additive functors associated to B:

There is the **covariant Hom functor**, **Hom**$(B, \_)$ defined by :

$$A \to \mathbf{Hom}(B, A)$$
$$\forall f \in \mathbf{Hom}(A, C), f \mapsto f^* : \mathbf{Hom}(B, A) \to \mathbf{Hom}(B, C)$$

...with $f^* : g \mapsto fg$.

Dually, we have the **contravariant Hom functor**, **Hom**$(\_, B)$ defined by :

$$A \to \mathbf{Hom}(A, B)$$
$$\forall f \in \mathbf{Hom}(A, C), f \mapsto f_* : \mathbf{Hom}(C, B) \to \mathbf{Hom}(A, B)$$

...with $f_* : g \mapsto gf$.

Proposition : Hom functors are left exact

The functors **Hom**$(\_, B)$ and **Hom**$(B, \_)$ respectively define left, contravariant and covariant exact functors. However, they are not necessarily right exact.

*Proof : Left exactness is easy and comes from the fact that if f is injective, then post-composition by f is still injective on morphism. If f is surjective, pre-composition by f is still injective on morphisms. However there are no reasons for right exactness to be preserved : apply **Hom**$(\mathbb{Z}/2\mathbb{Z}, \_)$ and **Hom**$(\_, \mathbb{Z})$ to the exact sequence $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ to obtain counter-examples.*

1.5.3 Properties of Exact Functors

The name "exact" for exact functors will be further justified in this section. We will see that exact functors actually preserve lots of information in the category of modules over a ring R.

Proposition : Exact Functors Preserve Mono and Epi Morphisms

If $f : A \to B$ is a mono or an epimorphism, $F(f) : F(A) \to F(B)$ is too.

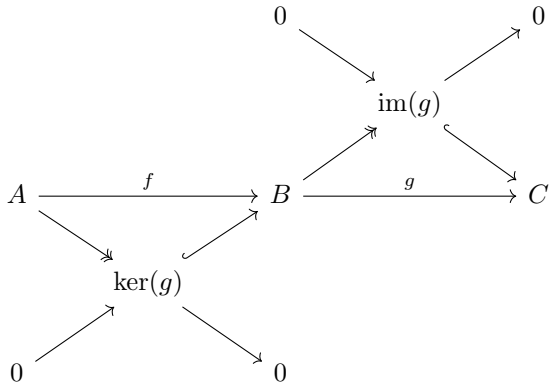
We remind that in the category of modules, monomorphisms are the same thing as injective morphisms and dually for epis and surjective morphisms. So monomorphism is the same thing as $\ker f = 0$ *and epimorphism is the same as* $Im\ f = B$*. Let* F *be an exact functor. If* $f : A \to B$ *is a monomorphism, then* $0 \to A \xrightarrow{f} B \to cokerf \to 0$ *is a short exact sequence, and so is its image, so* $F(f)$ *is still injective. The proof for surjectivity is identical by considering the short exact sequence* $0 \to \ker f \to A \xrightarrow{f} B \to 0$*. Note that the arguments in this proof can be more precisely used to show that right exact functors preserve epimorphisms and left exact functors preserve monomorphisms.*

And now, a property that legitimizes the name we gave to our functors:

Proposition : Exact Functors Preserve Long Exact Sequences

Let F be an exact functor (covariant or contravariant). If $C^\bullet$ is an exact complex, then $F(C)^\bullet$ is also an exact complex.

An exact sequence $A \xrightarrow{f} B \xrightarrow{g} C$ *yields a diagram with exact diagonals:*



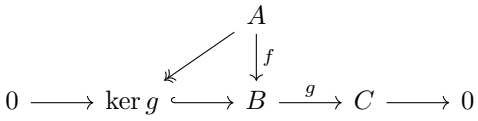
Apply F *to everything. Now* $Im\ (F(f)) = Im\ (F(A) \to F(\ker g) \to F(B)) = Im\ (F(\ker g) \to F(B))$ *since* F *preserves epis. This in turn is* $\ker(F(B) \to F(Im\ (g))$ *since* F *is exact. Now* $\ker(F(B) \to F(Im\ (g))) = \ker(F(B) \to F(Im\ (g)) \to F(C))$ *because* F *preserves monos. This final expression is* $\ker(F(g))$ *by commutativity. So* F *preserves very short exact sequences of the form* $A \to B \to C$*, so preserves long exact sequences.*

This property will be useful for a later proof.

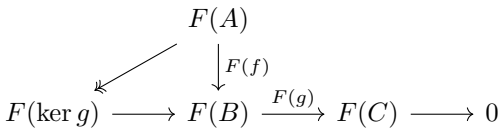
Proposition : Minimization of Axioms For Exact Functors

A covariant functor F is right exact if and only if for any exact sequence $A \to B \to C \to 0$, the sequence $F(A) \to F(B) \to F(C) \to 0$ is exact. The similar property also holds in the contravariant and left exact case.

If F *verifies this property it is clearly right exact. If* F *is right exact, an exact sequence* $A \to B \to C \to 0$ *yields a diagram (with an exact line) :*



Applying F *yields :*



... where the line is still exact. Now one can prove that Im $F(f) = \ker F(g)$ *in a similar way as in the proof above thanks to the fact that* F *preserves epis.*

1.6 Projective, Injective Modules and Resolutions

To introduce derived functors (in R-**Mod**), we have to introduce the notion of projective and injective module.

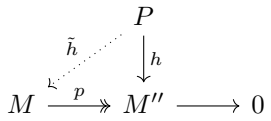
1.6.1 Projective Modules

Definition : Projective Module

A **projective module** (or a projective object in R-**Mod**) is an R-Module P that follows one of the equivalent properties below :

- The functor $\mathbf{Hom}(P, \_)$ is right exact.
- Every exact sequence $0 \to M' \to M \to P \to 0$ is split.
- There exists a free module L and a module K such that $L = K \oplus P$

In those three equivalent definitions, the first one is the most important. It's the one that is the most easily generalized to any abelian category. It can be reformulated with the following diagram :



For any morphism $P \to M''$, if you have a surjection from $M \to M''$ then P factors through this surjection. An enlightening example of projective module is the following:

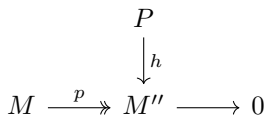
Proposition : Free Modules are Projective

Free Modules are Projective Modules.

Proof : if P *is free, a morphism* h *from* P *to* M *is determined by the image of a base. Take* $\tilde{h}$ *that sends elements of the base of* P *to inverse images by* p *of their image by* P*.*

With this fact we can prove the equivalence.

Proof of the equivalence : (1) $\implies$ (2) *by applying the* $\mathbf{Hom}(P, \_)$ *functor to such an exact sequence. Now use surjectivity of the map* $\mathbf{Hom}(P, M') \to \mathbf{Hom}(P, P)$ *to split the sequence.* (2) $\implies$ (3)*, use the fact that free modules are projective, construct the free module on the elmements of* P *(called* L*), use the exact sequence associated to the surjection* $L \to P$ *and split it to get the answer.* (3) $\implies$ (1) *is fairly easy, by considering that if we have a diagram:*



... with p surjective, it can be extended in :

$$\begin{array}{ccccc} & & K \oplus P & & \\ & & \downarrow{\scriptstyle p'} & & \\ & & P & & \\ & & \downarrow{\scriptstyle h} & & \\ M & \xrightarrow{p} & M'' & \longrightarrow & 0 \end{array}$$

.. with $K \oplus P$ free. $K \oplus P$ is projective, so one can construct a factorization of $u : h \circ p' \to M$ such that $p \circ u = h \circ p'$. Composing the inclusion $P \hookrightarrow K \oplus P$ with u yields the factorization.

So, projective modules are not too hard to find in the category of modules. They also have quite a few stability properties :

Proposition : Stability Of Projective Modules

- A direct factor of a projective module is projective.
- A direct sum of projective modules is projective.

Proof : Easy through the characterization with free modules.

Be careful : there are non free projective modules. For example, $\mathbb{Z}/6\mathbb{Z}$ is projective over itself because it is free, however $\mathbb{Z}/2\mathbb{Z}$ is not free as a $\mathbb{Z}/6\mathbb{Z}$-module. But it is projective since it is a direct factor in the $\mathbb{Z}/6\mathbb{Z}$.

Exercise : Projective Modules on a Principal Ideal Commutative Ring **

Let R be a commutative principal ideal ring. What are the projective modules in R-Mod ?

Solution : a projective module is a factor, so a sub-module of a free module. But in R-Mod, all sub-modules of a free module are free. So projective modules are exactly free modules.

We now present another types of modules. Don't worry: their importance will come later.

1.6.2 Injective Modules

Injective modules, as one might have guessed, are the dual notion of projective modules.

Definition : Injective Module

An **injective module** (or an injective object in R-**Mod**) is an R-Module I that follows one of the equivalent properties below :

- The functor $\mathbf{Hom}(\_, I)$ is right exact.
- Every exact sequence $0 \to I \to M \to M'' \to 0$ is split.
- For any module L that contains M, then there exists a module K such that $L = K \oplus M$ (so basically, M is always a direct factor everywhere).

Once again, the most important part of this definition is the first definition. It is summed up in the following diagram, which also translates verbatim to any abelian category.

$$\begin{array}{ccccc} 0 & \longrightarrow & X & \xrightarrow{i} & Y \\ & & \downarrow{\scriptstyle h} & \swarrow{\scriptstyle \tilde{h}} & \\ & & I & & \end{array}$$

If a module X injects itself in a module Y, then any arrow from X to I extends to an arrow from Y to I.

Proof of the equivalence : (1) $\implies$ (2) *and* (2) $\implies$ (3) *are easy and proved similarly as in the projective case.* (3) $\implies$ (1) *is harder. Given a diagram :*

$$\begin{array}{ccccc} 0 & \longrightarrow & X & \xrightarrow{i} & Y \\ & & \downarrow{\scriptstyle h} & & \\ & & I & & \end{array}$$

... one can build the pullback of Y and I along X, denoted $Y \times_X I$, which is the module $Y \oplus I$ quotiented by the module generated by the $(i(x), h(x))$ for $x \in X$. The map $k : z \mapsto [(0, z)]$ from $I \to Y \times_X I$ is injective because i is injective. Thus by (3) *we have $Y \times_X I = A \oplus I$ with k being the splitting map. The composition $-p_I \circ j$, where j is the map $y \mapsto [(y, 0)]$ and p_I is the map $(a, i) \mapsto i$ in the following diagram :*

$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \xhookrightarrow{i} & Y & \xrightarrow{j} & Y \times_X I \\ & & \downarrow{\scriptstyle h} & & & & \downarrow{\scriptstyle \simeq} \\ & & I & \xleftarrow[p_I]{} & & & A \oplus I \end{array}$$

... gives the factorization: indeed, x is sent to $i(x)$, then to $[(i(x), 0)] = [(0, -h(x))] = k(-h(x))$, which is thus sent to $(0, -h(x))$. Through $-p_I$, this is sent to $h(x)$.

Injective Modules are less easy to find than projective modules, that contain all free modules. For examples, $\mathbb{Z}$ is not injective as a $\mathbb{Z}$-module (consider the exact sequence $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$). However, we have this easy criterion to find them out.

Proposition : Baer's Criterion

An R-module I is injective if and only if for all left ideals $J \subset R$, a morphism $J \to I$ extends to a morphism $R \to I$ along the inclusion $J \hookrightarrow R$.

Proof : Nothing to prove if I is injective. Now if Baer's criterion is verified, we have a mono $i : M \hookrightarrow N$ and a map $h : M \to I$ that we wish to extend to a map $N \to I$. Consider the poset of extensions of $h : \tilde{M} \to I$. By Zorn's lemma, it has a maximal element that we call $(\tilde{h}, M')$. If $M' \neq N$, then there is $x \in N$ not in M'. We will extend $\tilde{h}$ to a morphism $M' + (x) \to I$.

To do this, consider the ideal of R, $J = \{r \in R, rx \in M'\}$. The map $J \to I$, $r \mapsto f(rx)$ can be extended into a morphism $f : R \mapsto I$. Define $\tilde{\tilde{h}} : M' + (x) \to I$, $m' + ax \mapsto \tilde{h}(m') + f(a)$. It clearly extends $\tilde{h}$, and we can check it is well defined.

This criterion allows us to find out a non obvious example of an injective module.

Proposition : The fraction field is injective

If A is a commutative integral domain, the fraction field of A is an injective A-module.

Proof : We use Baer's criterion. Note that if $J = 0$ there's nothing to do. For a morphism $f : J \to A$, chose an arbitrary non zero element in $j \in J$, and define for all $a \in A$, $f(a) = \frac{a}{j} f(j)$. You can check firstly that this is linear, then that it extends f and finally that it is canonical and does not even depend on the choice of j.

Here's another non trivial but important nonetheless example : $\mathbb{Q}/\mathbb{Z}$ is injective as a $\mathbb{Z}$-module. You should try and prove this with Baer's criterion. If you don't succeed, the proof is contained in the following exercise.

Exercise : Injective Modules on a Principal Ideal Commutative Ring ***

Let R be a commutative principal ideal ring. What are the injective modules in R-Mod ?

Solution : M is injective if and only if any morphism $(j) \to M$ extends to a morphism $R \to M$. This must be true for the morphisms defined by $f_{a,m} : aj \mapsto am$ for $m \in M$ (this is well defined because A is a free R module, and R is principal, so $(j) \simeq R$). So the image of 1 by an extension of $f_{a,m}$ to R gives an element α such that $j\alpha = a$. Hence M must be divisible: for all a and all $j \in R$, there exists α such that $j\alpha = a$. Proving that all divisible R-modules are injective is not hard: to extend a morphism whose domain is (j), send 1 on one of the quotients of $f(j)$ by j. Note that the extension is not unique if M is not uniquely divisible.

1.6.3 Resolutions

Resolutions are a notion that is fairly easy to define. They are the last step to reach derived functors.

Definition : Injective and Projective Resolutions

Let M be an R-module. A **projective resolution** of M is an exact sequence :

$$...P_2 \to P_1 \to P_0 \to M \to 0$$

...where all the P_i are projective.

An **injective resolution** of M is an exact sequence :

$$0 \to M \to I_0 \to I_1 \to I_2...$$

...where all the I_i are injective.

There are easy examples. If M is free, a projective resolution of M is trivial to obtain :

$$0 \to M \to M \to 0$$

For any ring R, if 0 is not a zero divisor, $R/(u)$ as an R-module has the following projective resolution:

$$0 \to R \to R \to R/(u) \to 0$$

... where the first non trivial arrow is multiplication by u.

Injective resolutions are less easy to find out. Here's one for $\mathbb{Z}$ ($\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are injective by Baer's criterion):

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

A natural question is whether or not all modules have injective and projective resolutions. In the category of R-modules, the answer is yes.

Proposition : The Category Of R-Modules has Enough Projectives

For all R-module M, there exists a natural exact sequence of the form

$$0 \to K \to P \to M \to 0$$

...where P is projective. This implies that every module has a projective resolution.

Proof : the proof of this result is fairly easy and very elegant. The existence of the exact sequence comes from the fact that every module is a quotient of a projective module: take the free R-module on the elements of M, which naturally surjects on M by associating each element to its value in M and extending it by linearity.

For the existence of a projective resolution, we will build it by induction. Consider a first exact sequence :

$$0 \to K_0 \to P_0 \to M \to 0$$

Let P_1 be a projective module that surjects onto K_0. We thus have a second exact sequence :

$$0 \to K_1 \to P_1 \to K_0 \to 0$$

So we can form the following commutative diagram :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_0 & \xrightarrow{i_0} & P_0 & \xrightarrow{p_0} & M & \longrightarrow & 0 \\ & & & \nwarrow^{p_1} & \uparrow{\scriptstyle i_0 p_1} & & & & \\ 0 & \longrightarrow & K_1 & \xrightarrow{i_1} & P_1 & \xrightarrow{p_1} & K_0 & \longrightarrow & 0 \end{array}$$

Since i_0 is bijective onto $\ker p_0$ and p_1 is surjective, we clearly have Im $i_0 p_1 = \ker p_0$. We now have a longer exact sequence :

$$0 \to K_1 \to P_1 \to P_0 \to M \to 0$$

The reader should fairly easily be able to repeat those steps and construct a projective resolution of M in this way.

Proposition : The Category Of R-Modules has Enough Injectives

For all R-module M, there exists a natural exact sequence of the form

$$0 \to M \to I \to Q \to 0$$

...where I is injective. This implies that every module has an injective resolution.

Proof : The hard part of the proof is that every module can be embedded into an injective module: after this, the construction of the resolution is exactly the dual one of the projective case.

Proving it takes a while. A first result is that the category of abelian groups has enough injectives : any abelian group is a quotient of a sufficient number of copies of $\mathbb{Z}$, so any abelian groups injects itself into the same number of copies of $\mathbb{Q}$ (if $M \subset M' \subset M''$, then $M'/M \subset M''/M$). Now, since $\mathbb{Q}$ is divisible, and since a sum and quotient of divisible groups stays divisible, then we have just embedded our abelian group in a divisible group, and thus it has been embedded into an injective module.

We can now deduce the theorem for all R-modules. For this, we prove the following lemma: if L, R are a pair of additive, (left and right) adjoint functors $R : \mathcal{B} \to \mathcal{A}$, $L : \mathcal{A} \to \mathcal{B}$, such as the left adjoint L is faithful and is exact, then if $\mathcal{B}$ has enough injectives, then so does $\mathcal{A}$. This is a short exercise : to construct an injective module in which to throw M, proceed as so. There is a monomorphism $i : L(M) \xrightarrow{i} I$. Its adjoint is a morphism $\tilde{i} : M \xrightarrow{i} R(I)$. Now it is fairly easy to show that $R(I)$ is still injective, and that $\tilde{i}$ is still a monomorphism : consider the image of the rigth exact sequence under L and use the property that $L(\tilde{i})$ composed with an adjunction unit is a monomorphism.

Now we just need to find a pair of adjoint functors between R-modules and abelian groups, such that the one from R-modules to abelian groups is the left adjoint, is exact and faithful. The forgetful functor U is so, and its right adjoint is the coextension of scalars: send an abelian group A to $\boldsymbol{Hom}_{Ab}(U(R), A)$ equipped with the action $rf = f(\cdot r)$. It is a good exercise (although tedious) to check that this is an adjunction.

Projective and injective resolutions have a nice property, that will be very dear to us later.

Proposition : Comparison Lemma

Let M and M' be two R-modules. A morphism between $M \to M'$ gives rise to a morphism between their injective / projective resolutions, which is unique up to homotopy.

What we mean by this formulation is summed up in the following diagram: if there is a morphism f, one can construct the dotted arrows that complete f into a morphism between the resolutions.

$$\begin{array}{ccccccccccc} \ldots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\ & & \vdots & & \vdots & & \vdots & & \downarrow f & & \\ \ldots & \longrightarrow & P'_2 & \longrightarrow & P'_1 & \longrightarrow & P'_0 & \longrightarrow & M' & \longrightarrow & 0 \end{array}$$

Proof : Construction comes from projectivity of the modules P_i. After f_i is constructed, construct f_{i+1} by applying projectivity to the diagram :

$$\begin{array}{ccccc} P_{i+1} & \xrightarrow{\epsilon_{i+1}} & \ker \epsilon_i & \xrightarrow{\epsilon_i} & 0 \\ \downarrow f_{i+1} & & \downarrow f_i & & \\ P'_{i+1} & \xrightarrow{\epsilon'_{i+1}} & \ker \epsilon'_i & \xrightarrow{\epsilon'_i} & 0 \end{array}$$

Now if take two extensions of f. We will construct the homotopy. The first member $M \to P'_0$ is the zero map. Now $f_1 - g_1$ have their image in $\ker \epsilon'_0$. So one can construct a map from P_0 to P'_1 by projectivity that satisfy the axioms of homotopy. Now if one bit of the homotopy has been formed, form the next one by considering $f_{i+1} - g_{i+1} - s_i \epsilon_{i+1}$ which will have image in the right kernel. Use projectivity.

Exercise : Isomorphisms between Projective Resolutions *

Prove that if f (in the above diagram) is an isomorphism, then all of the f_i have quasi-inverses : morphisms g_i such that $g_i \circ f_i$ and $f_i \circ g_i$ are homotopic to the identity.

This result will be crucial for the rest, as derived functors are directly constructed from the homology / cohomology modules of those resolutions. Another crucial result, which is difficult to prove but which will be paramount in the rest of the paper :

Proposition : Horseshoe Lemma

Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of R-modules. There exist projective (or injective) resolutions $P_{M'}, P_M, P_{M''}$ of the three modules, such the sequence of complexes $0 \to P_{M'} \to P_M \to P_{M''} \to 0$ is exact and that in degree ≥ 1, $P_M = P'_M \oplus P''_M$ and the exact sequences $0 \to P_{M'i} \to P_{M'i} \oplus P_{M''i} \to P_{M''i} \to 0$ are split. Moreover, the choice of those resolutions is natural, meaning that a morphism between exact sequences naturally gives rise to a morphism between the corresponding exact sequence of resolutions.

More explicitly, given a short exact sequence :

$$0 \to M' \to M \to M'' \to 0$$

... we have projective (or injective) resolutions that fit in this commutative diagram :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
... & \longrightarrow & P_1' & \longrightarrow & P_0' & \longrightarrow & M' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
... & \longrightarrow & P_1' \oplus P_1'' & \longrightarrow & P_0' \oplus P_0'' & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
... & \longrightarrow & P_1'' & \longrightarrow & P_0'' & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

... and a morphism of exact sequences gives rise to a morphism between the two diagrams.

Proof : This is long, fairly complicated, and not extremely relevant to the theory that comes afterwards. We will omit it. Quite a bit of work to prove that the sequence is indeed exact at the end.

1.7 δ-Functors and Derived Functors

In this section, some theorems will be a little tricky to prove. One may skip some of the proofs, and come back to them later with more maturity about δ-functors and derived functors.

1.7.1 δ-Functors

Definition : δ-functors

A δ-functor is a sequence of functors $(T_n)_{n\in\mathbb{N}}$ along with the data, for each exact sequences $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$, of natural morphisms $\delta_n : T_{n-1}(M'') \to T_n(M')$ for all n, such that the following long sequence is exact :

$$... \xrightarrow{T_{n-1}(g)} T_{n-1}(M'') \xrightarrow{\delta_{n-1}} T_n(M') \xrightarrow{T_n(f)} T_n(M) \xrightarrow{T_n(g)} T_n(M'') \xrightarrow{\delta_{n+1}} T_{n+1}(M') \xrightarrow{T_{n+1}(f)} ...$$

"Naturality" means as always that for a morphism of exact sequences :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0
\end{array}$$

... all of the following squares are commutative :

$$\begin{array}{ccccc}
... & \longrightarrow & T_{n+1}(M'') & \xrightarrow{\delta_{n+1}} & T_n(M') & \longrightarrow & ... \\
 & & \downarrow & & \downarrow & & \\
... & \longrightarrow & T_{n+1}(N'') & \xrightarrow{\delta'_{n+1}} & T_n(N') & \longrightarrow & ...
\end{array}$$

Definition : Homological and Cohomological δ-functors

A **homological δ-functor** is a delta functor of which all the terms for $i \geq 0$ are 0.

A **cohomological δ-functor** is a delta functor of which all the terms for $i \leq 0$ are 0.

To understand well where this strange definition comes from, you should tell yourself that this (co)homological δ-functor mumbo-jumbo simply formalizes the idea of "sequence of functors that behave like homology groups and cohomology groups". The basis for the definition is the fundamental lemma of homological algebra, the difference being that δ-functors may act on objects of any abelian category, while the H_n or H^n functors behave solely on chain or cochain complexes.

We usually index a homological δ-functor with decreasing positive integers instead of negative integers.

Exercise : An Example of a Homological δ-Functor ***

Let $a \in R$. Define for any module M, $T_n(M) = 0$ for all $n \in \mathbb{Z} \setminus \{0, 1\}$, $T_1(M) = \{m \in M, a \cdot m = 0\}$, $T_0(M) = M/a \cdot M$. Action on maps is respectively given by restriction and induced maps. Prove that this a homological δ-functor in the category or R-modules.

Solution : use very much the fact that $M'' \simeq M/M'$ in an exact sequence $0 \to M' \to M \to M'' \to 0$. Define a morphism $T_1(M'') \to T_0(M')$ by taking $[x]$ to any representative of x, multiplying it by a and projecting the result in M/M'. Checking exactness is a bit of a pain but eventually works out.

Exercise : δ-Functors and Composition *

Let (F_n) be a cohomological δ-functor from R-**Mod**, and G be an exact endofunctor of R-**Mod**. Prove that $(F_n \circ G)$ is still a δ-functor.

Solution : easy.

Definition : Morphism of δ-functors

A **morphism of homological δ-functor** is a sequence of natural transformations $t_n : T_n \to U_n$ such that make the morphisms induced on long exact sequences commute.

What is meant by this definition is that for an exact sequence $0 \to M' \to M \to M'' \to 0$, for all $n \in \mathbb{N}$ the following squares must be commutative :

$$\begin{array}{ccccccc} \ldots & \longrightarrow & T_{n+1}(M'') & \xrightarrow{\delta_{n+1}} & T_n(M') & \longrightarrow & \ldots \\ & & \downarrow{\scriptstyle t_{n+1}(M'')} & & \downarrow{\scriptstyle t_n(M')} & & \\ \ldots & \longrightarrow & U_{n+1}(M'') & \xrightarrow{\delta'_{n+1}} & U_n(M') & \longrightarrow & \ldots \end{array}$$

Definition : Universal (co)homological δ-functors

A **homological δ-functor** $(T_n)_{n\in\mathbb{N}}$ is said to be **universal** if for any other δ-functor $(U_n)_{n\in\mathbb{N}}$ and any natural transformation $t_0 : U_0 \to T_0$ there exists a unique morphism of δ-functors $(t_n)_{n\in\mathbb{N}}$ with t_0 in first position.

For a **cohomological** δ-functors, the definition is the same, but with transformations replace $t^0 : T^0 \to U^0$.

Universal δ-functors are extremely powerful objects. They generate morphisms between objects without any effort. Now, one has to find a way to check easily if a homological or cohomologiical δ-functor is universal or not. Fortunately, we have this beautiful theorem :

Theorem : Criterion for Universality

Let $(T_n)_{n\in\mathbb{N}}$ be homological δ-functor. If $(T_n)_{n\in\mathbb{N}}$ is **erasable**, meaning that for each object M there exists an epimorphism $P \xrightarrow{\epsilon} M$ such that $T_n(\epsilon) = 0$ for all $n \in \mathbb{N} \setminus \{0\}$, then $(T_n)_{n\in\mathbb{N}}$ is universal.

The cohomological equivalent of erasibility is the existence of a monomorphism $M \xrightarrow{\epsilon} I$ such that $T_n(\epsilon) = 0$. The consequences on universality are the same.

Proof : not included in this version, but the proof is about the same as in the following exercise.

Exercise : An Alternative Universality Criterion for More General δ-functors ****

Let $(F_n)_{n\in\mathbb{Z}}$ and $(G_n)_{n\in\mathbb{Z}}$ be δ-functors between two abelian categories $\mathcal{C} \to \mathcal{D}$. Prove the following theorem :

- If $\mathcal{C}$ has enough injectives and projectives, and if $(F_n)_{n\in\mathbb{Z}}$ vanishes on the injectives, and $(G_n)_{n\in\mathbb{Z}}$ vanishes on the projectives then any natural transformation $t_0 : F_0 \to G_0$ extends to a natural transformation of δ-functors $(t_n)_{n\in\mathbb{Z}}$ in a unique way.

This is a very long exercise that may take you quite a while to solve. Try doing it rigorously, even though it might be long and tedious : believe me that you'll come out of it stronger.

Solution : this is going to take a while, so be prepared. We will firstly use the fact that F vanishes on the injectives to construct the t_i for $i \geq 1$: the construction of the t_i for $i \leq -1$ is just the dual construction, using that G vanishes on the projectives.

***Definition and unicity of the** t_i **for** $i \geq 0$: To define the t_i, inject any object A into an injective object I :*

$$0 \to A \hookrightarrow I \to I/A \to 0$$

Then this induces two long exact sequence by δ-functoriality, in which we can add t_0 at the beginning :

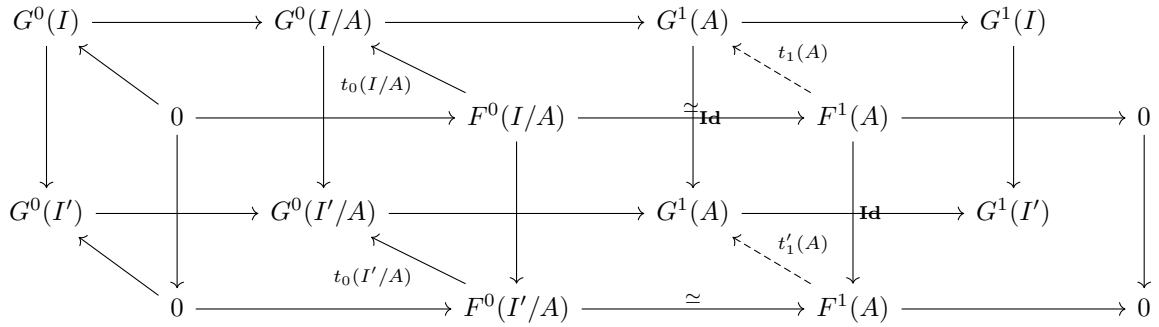
$$\begin{array}{ccccccccc}
F^0(A) & \longrightarrow & 0 & \longrightarrow & F^0(I/A) & \xrightarrow{\delta} & F^1(A) & \longrightarrow & 0 \\
\downarrow{\scriptstyle t_0(A)} & & \downarrow & & \downarrow{\scriptstyle t_0(I/A)} & & \vdots{\scriptstyle t_1(A)} & & \downarrow \\
G^0(A) & \longrightarrow & G^0(I) & \longrightarrow & G^0(I/A) & \xrightarrow{\delta'} & G^1(A) & \longrightarrow & G^1(I)
\end{array}$$

In order to make this whole thing commute, we must define $t_1(A)$ as $\delta' t^0(I/A)\delta^{-1}$. Notice that this certifies that if our construction works out (if the t_i are well defined and they indeed define natural transformations) then they are necessarily unique, since they must verify the above property which is only contained in the information of t_0, F and G. By induction, define similarly the t_i for $i \geq 2$.

***The** t_i **for** $i \geq 0$ **are well defined** : We must verify that this definition of t_i does not depend on the injective object in which we injected A. Notice that if I and I' are two such objects, the injectivity of I allows us to define a morphism of exact sequences :*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \hookrightarrow & I & \twoheadrightarrow & I/A & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathbf{Id}} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle \tilde{u}} & & \\
0 & \longrightarrow & A & \hookrightarrow & I' & \twoheadrightarrow & I'/A & \longrightarrow & 0
\end{array}$$

Then, using the δ-functoriality of the functors and t_0, we obtain a commutative "slab" (which may take a while to process, but try to be convinced that the morphism $t_1(A)$ and $t'_1(A)$ are exactly constructed so that the slab commutes !) :

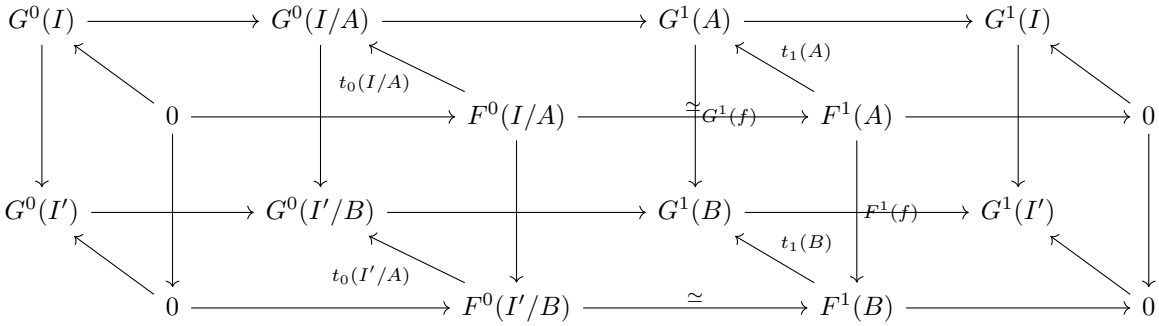


By looking at one of the faces of the central cube, we get that the definition of the t_1 does not depend on the chosen injective object I. By induction, the same follows for the t_i with $i \geq 2$.

***The t_i define a natural transformation** : take a morphism $A \xrightarrow{f} B$ in $\mathcal{C}$. Taking an injective object and applying injectivity yields a commutative diagram :*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \hookrightarrow & I & \twoheadrightarrow & I/A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle \tilde{u}} & & \\ 0 & \longrightarrow & B & \hookrightarrow & I' & \twoheadrightarrow & I'/B & \longrightarrow & 0 \end{array}$$

The definition of the t_i yields a commutative slab as above :



...and the same face as above yields naturality. Continue by induction.

1.7.2 Derived Functors

We remind the reader that all of the functors in this article are considered to be additive. For a left exact covariant functor F, we will introduce a sequence of universal δ-functors $(R^iF)_{i\in\mathbb{N}}$, called the **right derived functors of** F. As in the definition of δ-functors, for any short exact sequence :

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

... we have a long exact sequence :

$$0 \to R^0F(A) \to R^0F(B) \to R^0F(C) \to R^1F(A) \to R^1F(B) \to R^1F(C) \to R^2F(A)...$$

Dually, for a covariant right exact functor F, we will introduce a sequence of functors $(L_iF)_{i\in\mathbb{N}}$, called the **right derived functors of** F, such that we have a long exact sequence :

$$...L_2F(C) \to L_1F(A) \to L_1F(B) \to L_1F(C) \to L_0F(A) \to L_0F(B) \to L_0F(C) \to 0$$

Those functors were introduced in Algebraic Topology. They appear when trying to compute the homology of products of topological spaces.

The construction of derived functors is in several steps. This part is important, and will be reviewed in debth through the computations of the Tor and Ext functors. We will first do it for **covariant** left exact and right exact functors, and then move on to contravariant functors.

For the **left derived functors** of a **covariant right exact** functor F, for any module M, first consider a projective resolution of M :

$$... \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

... then take out the M (which makes the sequence no longer exact !).

$$... \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow 0$$

... then apply F (which doesn't make the sequence anymore exact than it was).

$$... \longrightarrow F(P_2) \longrightarrow F(P_1) \longrightarrow F(P_0) \longrightarrow 0$$

Since the sequence isn't necessarily exact anymore, you can compute its homology groups, which will give you a measure of how far the functor is from being exact. This is what derived functors are about.

Definition : Covariant Left Derived Functors, Action on Objects

The n^{th} Left Derived functor of a covariant right exact functor F, denoted L_nF, is obtained on a module M by taking the homology group at $F(P_n)$ (so the kernel of the morphism going from $F(P_n) \to F(P_{n-1})$ quotiented by the image of the morphism $F(P_{n+1}) \to F(P_n)$).

Verification : is this well defined ? If there are two projective resolutions, good use of the comparison lemma with identity provides morphisms between the resolutions with composition homotopical to the identity. Since F is an additive functor, it preserves homotopies towards identity. So the groups are the same in the end.

For a morphism $M \to M'$, one proceeds as before by considering projective resolutions. Use of comparison lemmas gives rise to morphisms between the two resolutions as so:

$$\begin{array}{ccccccccccc} ... & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f} & & \\ ... & \longrightarrow & P_2' & \longrightarrow & P_1' & \longrightarrow & P_0' & \longrightarrow & M' & \longrightarrow & 0 \end{array}$$

Then, apply F after having taken out M.

$$\begin{array}{ccccccccc} ... & \longrightarrow & F(P_2) & \longrightarrow & F(P_1) & \longrightarrow & F(P_0) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle F(f_2)} & & \downarrow{\scriptstyle F(f_1)} & & \downarrow{\scriptstyle F(f_0)} & & \\ ... & \longrightarrow & F(P_2') & \longrightarrow & F(P_1') & \longrightarrow & F(P_0') & \longrightarrow & 0 \end{array}$$

Now we have morphisms between complexes, we have morphisms between the corresponding homology modules.

Definition : Left Derived Functors, Action on Morphisms

For a morphism $f : M \to M'$, $L_nF(f)$, is defined as the morphism induced by f_n on the homology group at $F(P_n)$.

Verification : Those morphisms are well defined for the same reasons. Homotopy works after functors.

For covariant right exact functors, the construction is the dual one, but we will mention it anyway. To construct **right derived functors** of a **covariant left exact** functor F, for any module M, one first has to consider an **injective** resolution of M :

$$0 \longrightarrow M \longrightarrow I_0 \longrightarrow I_1 \longrightarrow I_2 \longrightarrow ...$$

... then take out the M (which makes the sequence no longer exact !).

$$0 \longrightarrow I_0 \longrightarrow I_1 \longrightarrow I_2 \longrightarrow ...$$

... then apply F (which doesn't make the sequence anymore exact than it was).

$$0 \longrightarrow F(I_0) \longrightarrow F(I_1) \longrightarrow F(I_2) \longrightarrow ...$$

Since the sequence isn't exact anymore, you can compute its cohomology groups.

Definition : Right Derived Functors of a Covariant Right Exact Functor

The n^{th} Right Derived functor of a right exact covariant functor F, denoted R^nF, is obtained on a module M by taking the cohomology group at $F(I_n)$ (so the kernel of the morphism going from $F(I_n) \to F(I_{n+1})$ quotiented by the image of the morphism $F(I_{n-1}) \to F(I_n)$).

The action of R^nF on morphisms is defined just as it is for left derived functors.

Now we are there, we can mention the contravariant case:

Definition : Derived functors of Contravariant Functors

If F is a contravariant right exact functor, one may define its left derived functors by taking injective resolutions of objects and computing the cohomology modules and morphism of their image by F.

If F is a contravariant left exact functor, one may define its right derived functors by taking projective resolutions of objects and computing the homology modules / morphisms of their image by F.

To remember how this goes, remember two things:

1. The derived functors go the other way than the exactness.
2. Left derived functors are always based on homology and right derived functors are always based on cohomology.

So if you have a covariant functor, to get homology you need a projective resolution and to get cohomology you need an injective resolution. For a contravariant functor, to get homology you need an injective resolution and to get cohomology you need a projective resolution.

This must seem deadly abstract at the moment: it's the problem with homological algebra. We advise the reader not to study this topic independently from its applications, which are very widespread through mathematics. There will be examples of properties and calculations in the rest of this paper, which we hope, will make it less abstract.

1.7.3 Properties of Derived Functors

Derived Functors have properties that are helpful for computations.

Proposition : The First Derived Functor

Let M be an R-module, and F be a right exact functor. We have a canonical isomorphism :

$$L_0F(M) \cong F(M)$$

Dually, if F is left exact, we have a canonical isomorphism :

$$R^0F(M) \cong F(M)$$

This is a good exercise to start with. Try and prove it yourself before moving on.

Proof : We will prove it for left derived functors (the proof is identical in the dual case). Consider a projective resolution of M : $... \to P_2 \to P_1 \to P_0 \to M$. Since F is right exact, use the fact that the sequence $F(P_1) \to F(P_0) \to F(M) \to 0$ is still exact.

Proposition : Commutativity of Left Derived Functors and Direct Sums

Let M be an R-module, and F be a covariant right exact functor. We have $L_iF(A \oplus B) \cong L_iF(A) \oplus L_iF(B)$. This property also holds for the right derived functors of a contravariant left exact functor.

Proof : this is proven through the fact that a direct sum of projective objects is still projective, a direct sum of projective resolutions is still a projective resolution, and the homology of a direct sum is the direct sum of the homologies.

We remind the reader that this proves that derived functors are additive.

Finally, here's the property we expected :

Theorem : Derived Functors are Universal δ-functors

Left / Right Derived Functors in the Category of R-modules are **universal** homological / cohomological δ-functors.

Proof : To show it is a homological / cohomological δ functor, for a given exact sequence apply the functor to the horseshoe lemma resolution. You can then use the fundamental theorem of homological algebra to construct the long exact sequence, since split lines stay exact by additivity of your original functor. To obtain universality, we just have to show that modules are erasable in homology and cohomology. This is a consequence of the fact that injective and projective modules have trivial homology groups (under any left exact or right exact functor - since their resolutions are just one isomorphism) and that every module can be injected into an injective modules and is a quotient of a projective module.

1.7.4 The Ext and Tor Functors

Ext and Tor functors will be the two examples of derived functors we will focus on. This section might as well be seen as an exercise to make sure that the definitions are well understood.

The Tor Functors

Definition : The Tor functors

Let B be an R-module. The Tor functors associated to B, denoted $\mathbf{Tor}_n^R(\_, B)$ for $n \in \mathbb{N}$ are defined as the left-derived functors of the functor $\_ \otimes B$.

Our goal is now going to compute $\mathbf{Tor}_n^{\mathbb{Z}}(G, H)$ for G and H any finitely generated abelian groups. This will be rendered fairly easy by the fact that, since a property of derived modules is that they commute with direct sums (which is true because it is for homology and cohomology modules), we only need to compute when G and H are $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for a certain n.

For the Tor functor, the following calculations will be very useful :

Proposition : Basic Calculations for the Tor Functor

Let R be a commutative ring, and M be an R-module.

- $\mathbf{Tor}_n^R(M, R) = 0$ if $n > 0$, and M if $n = 0$.
- $\mathbf{Tor}_n^R(R, M) = 0$ if $n > 0$, and M if $n = 0$.
- If u is not a zero divisor, then $\mathbf{Tor}_n^R(R/(u), M) = M/uM$ if $n = 0$, $M[u]$ if $n = 1$, and $= 0$ if $n > 0$.

Proof : follows from $M \otimes_R R \cong M$, and through the following projective resolutions of R, and $R/(u)$. We denote $M[u] = \{x \in M, ux = 0\}$.

$$0 \longrightarrow R \longrightarrow R \longrightarrow 0$$

$$0 \longrightarrow R \xrightarrow{\times u} R \longrightarrow R/(u) \longrightarrow 0$$

We leave it to the reader to compute $\mathbf{Tor}_{\mathbb{Z}}^n(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ from here.

The Ext Functors

Definition : The Ext functors

Let B be an R-module. The **Ext** functors associated to B, denoted $\mathbf{Ext}_R^n(\_, B)$ for $n \in \mathbb{N}$ are defined as the right-derived functors of the contravariant functor $\mathbf{Hom}(\_, B)$, or as the right-derived functors of the covariant functor $\mathbf{Hom}(B, \_)$.

Proof of the isomorphism : not included in this version.

The calculations are similar than those of **Tor**, since in both cases we can use projective resolutions. Because the direct sums commute with the right derived functors of a contravariant functor, they are also enough to compute $\mathbf{Ext}_R^n(G, H)$ for all finitely generated abelian groups.

Proposition : Basic Calculations for the Tor Functor

Let R be a commutative ring, and M be an R-module.

- $\mathbf{Ext}^n_R(M,R) = 0$ if $n > 0$, and M if $n = 0$.
- $\mathbf{Ext}^n_R(R,M) = 0$ if $n > 0$, and M if $n = 0$.
- If u is not a zero divisor, then $\mathbf{Ext}^n_R(R/(u),M) = M[u]$ if $n = 0$, M/uM if $n = 1$, and $= 0$ if $n > 0$.

Proof : not included in this version, but similar to ***Tor****.*

We leave it to the reader to compute $\mathbf{Ext}^{\mathbb{Z}}_n(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ from here.

1.8 Spectral Sequences

We now reach one of the most scary parts of homological algebra : spectral sequences. The goal of this part is to make them a little less scary.

Definition : Spectral Sequence (in the first quadrant)

Let $\mathcal{C}$ be an abelian category. A cohomological spectral sequence (in the first quadrant) in $\mathcal{C}$ is the data of...

- An integer $a \in \mathbb{N}$ and objects E_r^{pq}, indexed by $p \in \mathbb{N}, q \in \mathbb{N}, r \geq a$ that are all 0 if $p < 0$ or $q < 0$. Objects with r lower index are said to be "on page r".
- Morphisms $d_r^{pq} : E_r^{pq} \to E_r^{p+r,q-(r-1)}$ such that $d_r^{p+r,q-(r-1)} \circ d_r^{pq} = 0$.
- Isomorphisms between E_{r+1}^{pq} and the cohomology object at pq on page r, namely :

$$E_{r+1}^{pq} \simeq \mathbf{Ker} d_r^{pq} / \mathbf{Im} d_r^{p-r,q+(r-1)}$$

A homological spectral sequence has the dual definition.

Spectral Sequences are a famously scary concept for students in homological algebra. Thankfully, I got a marvellous explanation from Ravi Vakil's document ([4]) which I more or less copied with slight adjustments. To get a better picture (the one you should have in mind), here's what typical pages 0, 1, and 2 look like.

Page 0 is just lines of complexes.

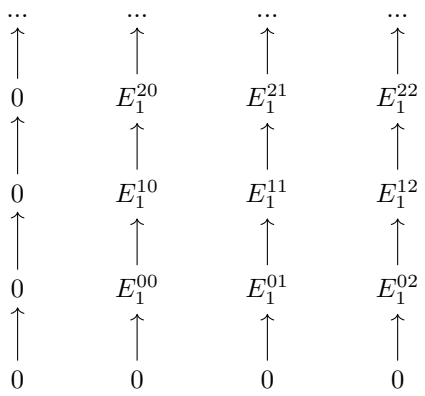
$$0 \longrightarrow E_0^{20} \longrightarrow E_0^{21} \longrightarrow E_0^{22} \longrightarrow ...$$

$$0 \longrightarrow E_0^{10} \longrightarrow E_0^{11} \longrightarrow E_0^{12} \longrightarrow ...$$

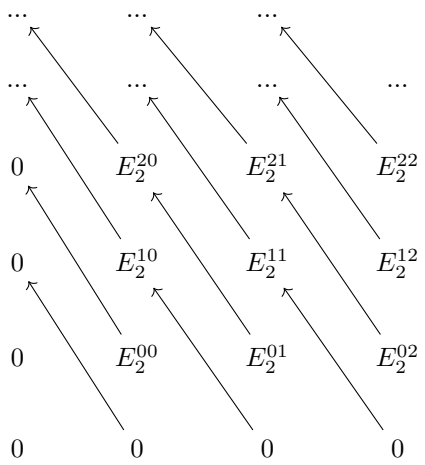
$$0 \longrightarrow E_0^{00} \longrightarrow E_0^{01} \longrightarrow E_0^{02} \longrightarrow ...$$

$$0 \longrightarrow 0 \longrightarrow 0 \longrightarrow 0 \longrightarrow ...$$

It is a good exercise to figure out the following diagrams by yourself before further reading. Here's page 1 :



So page 1 just consists in columns of complexes. Page 2 is where it gets interesting (note that we only drew the arrow of which we had room to draw : start and head point. There are a lot more).



A good thing to keep in mind in order to remember how spectral sequences work, is that in this representation the slope of the arrows at page r is $\frac{r}{r-1}$. Also note that the action of d_r on the sum $p+q$ is adding $r-1$.

So, the idea of spectral sequences is to start with a quadrant with lines of cochain complexes. Then, computing the cohomology of those complexes give you the second page, now with column of complexes. Computing the cohomology on the columns give you the third page, with diagonals of complexes. Computing the cohomology gives you a third page... etc. Here are two easy, but very important facts you should prove before moving on.

Exercise : Stable Values of a Spectral Sequence **

Prove that for all $p, q \in \mathbb{N}$ and $r \geq a$, there exists an r_0 such that $\forall r \geq r_0$, $E_r^{pq} \simeq E_{r_0}^{pq}$. This value is called the **stable value** of E at pq and is denoted E_∞^{pq}.

Solution : if you take r such that $r > \max(p, q+1)$, you obtain a complex $0 \xrightarrow{d_{p-r,q+(r-1)}} E_r^{pq} \xrightarrow{d_{p,q}} 0$, which by the isomorphism condition implies that $E_{r+1}^{pq} \simeq E_r^{pq}$.

Exercise : Stable Values Are Sub-Quotients **

1. Prove that E_∞^{pq} is a subgroup of a quotient (or equivalently, a quotient of a subgroup) of E_a^{pq}.
2. Deduce that in the catgory of R-modules, if E_a^{pq} is zero / torsion / any property stable by sub-object and by quotient, E_∞^{pq} is.

It is immediate that E_{r+1}^{pq} is a subquotient of E_r^{pq}. And a subquotient of a subquotient is a subquotient (essentially because a subgroup of a subgroup and a quotient of a quotient is a subgroup or a quotient). The second question is trivial.

Here's what we're going to do next : introduce the notions of convergence of a spectral sequence (without expecting you to understand it !), and then go in detail through a specific case of convergence.

1.8.1 Convergence of a Spectral Sequence

Definition : Convergence of a Spectral Sequence

Let E_a^{pq} be a cohomological sequence in the first quadrant, starting at $a \in \mathbb{N}$. Let $(H_i)_{i\geq 0}$ be a sequence of objects in $\mathcal{C}$. We say that E_r^{pq} converges towards $H^\bullet$ if for all n, there is a filtration :

$$F_{n+1} = 0 \hookrightarrow F_n \hookrightarrow F_{n-1} \hookrightarrow F_{n-2} \hookrightarrow ... \hookrightarrow F_1 \hookrightarrow F_0 = H^n$$

... with $F_i/F_{i+1} \simeq E_\infty^{i,n-i}$.

In this situation we write $E_a^{pq} \implies H^{p+q}$.

To memorize where the quotients are, this filtration is usually written :

$$E_\infty^{n,0} \overset{E_\infty^{n-1,1}}{\hookrightarrow} F_{n-1} \overset{E_\infty^{n-2,2}}{\hookrightarrow} ... \overset{E_\infty^{1,n-1}}{\hookrightarrow} F_1 \overset{E_\infty^{0,n}}{\hookrightarrow} H_n$$

The idea of this definition is that when all the terms of a first quadrant spectral sequence have converged on a diagonal where the sum $p+q$ is constant, this gives you information on the object H^{p+q}.

Here are short exercises to make this a little less nonsensical. All spectral sequences are in the first quadrant and start at an arbitrary a (it does not matter).

Exercise : Convergence In Degree 0 *

Suppose $E_a^{pq} \implies H^{p+q}$. Give a link between H^0 and the spectral sequence.

Solution : The filtration then takes the form $0 \overset{E_\infty^{0,0}}{\hookrightarrow} H^0$ which is equivalent to $H^0 \simeq E_\infty^{0,0}$.

Exercise : Convergence when a lot of terms are zero *

1. Suppose that all the terms E_∞^{pq} are 0 when $p+q=n$. Prove that $H^n = 0$.
2. Prove the reciprocal : if $H^n = 0$, then all the terms E_∞^{pq} are 0 when $p+q=n$.
3. Suppose only one of the terms of the same diagonal, $E_\infty^{p_0,n-p_0}$ is non zero. Prove that $H^n = E_\infty^{p_0,n-p_0}$.

Solution : the first one is a very easy induction that proves that all the F_i are then 0. The reciprocal is just as easy : all the F_i must be zero and by induction all the E_∞^{pq} are. The second one gives all terms of the filtrations 0 before p_0 and constant afterwards.

Exercise : Information on the Dimension **

The considered category is now a category of vector spaces over a field. Suppose all of the all the terms E_∞^{pq} are of finite dimension. Prove that $\dim H^n = \sum_{p=0}^{n} \dim E_\infty^{n-p,p}$.

Solution : this is an easy calculation, immediate from the filtration.

I can almost hear it : what the $\zeta\eta\%\sum^i \varepsilon\mathfrak{N}$ is this definition ? Well, this definition reflects a situation that really happens. We will move on to applications, that we hope, will convince you that spectral sequences are actually really nice.

1.8.2 Spectral Sequences Associated to a Double Complex, Applications

Definition : Double Complex

A (cohomological) double complex in an abelian category $\mathcal{C}$ is the data of objects $(A^{pq})_{p,q\in\mathbb{Z}}$ along with differentials $d_\wedge^{pq} : A_{pq} \to A_{p+1,q}$, $d_>^{pq} : A_{pq} \to A_{p,q+1}$ (shortened to $d_\wedge$ and $d_>$) such that $d_>^2 = 0$, $d_\wedge^2 = 0$ and $d_> d_\wedge + d_\wedge d_> = 0$.

Note that any commutative grid such that the composition of two consecutive morphisms on the same line is 0 can be turned into a double complex by changing $d_\wedge^{pq}$ to $(-1)^p d_\wedge^{pq}$. Usually, it doesn't change the properties of the morphisms that homological algebra looks at, namely images and kernels.

Definition : The Total Complex Associated to a Double Complex

Let $(A^{pq})_{p,q\in\mathbb{Z}}$ be a double complex. The **total complex** associated to $(A^{pq})_{p,q\in\mathbb{Z}}$ is the complex where the objects are $T_n = \oplus_{i\in\mathbb{Z}} A^{n-i,i}$ and the differentials are $d_\wedge + d_>$ (sending the right objects into the right summands).

Here's a simple observation that will be very relevant in what follows : given a double complex $(A^{pq})_{p,q\in\mathbb{Z}}$, the total complexes associated to $(A^{pq})_{p,q\in\mathbb{Z}}$ and $(A^{qp})_{p,q\in\mathbb{Z}}$ are the same.

Here's a theorem that we will not prove, but that will be the basis to the rest of this section.

Theorem : The Spectral Sequence Associated to a Double Complex

Let $(A^{pq})_{p,q\in\mathbb{Z}}$ be a double complex. There exists a spectral sequence E_r^{pq} starting at 0 where $E_0^{pq} = A^{pq}$, with horizontal differentials taken from the complex A^{pq}. Moreover, page 1 is the cohomology groups with the morphisms induced by the vertical differential.

Finally, the spectral sequence converges to the cohomology of the total complex associated to A :

$$E_r^{pq} \implies T(A)^{p+q}$$

This is where the fun starts. For example, following Ravi Vakil's work, we will prove famous homological algebra theorem (usually tediously proved through diagram chasing) by simply plugging them into the previous spectral sequence. Here's the idea : suppose you have a commutative diagram of the following form...

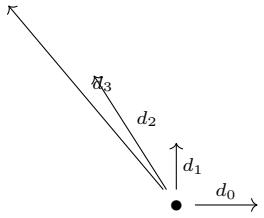
$$\begin{array}{ccccc} A & \longrightarrow & E & \longrightarrow & F \\ \uparrow & & \uparrow & & \uparrow \\ B & \longrightarrow & D & \longrightarrow & H \\ \uparrow & & \uparrow & & \\ C & \longrightarrow & G & & \end{array}$$

... where the composition of two consecutive arrows (in the same direction) are zero and the squares commute. Without loss of generality, you can extend this diagram into an entire commutative grid by adding zeroes everywhere, and change certain morphisms to their opposites, in order to turn the commutative diagram into a double complex (anticommutative diagram).

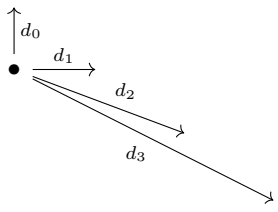
$$\begin{array}{ccccccc} 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ A & \longrightarrow & E & \longrightarrow & F & \longrightarrow & 0 \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ B & \longrightarrow & D & \longrightarrow & H & \longrightarrow & 0 \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ C & \longrightarrow & G & \longrightarrow & 0 & \longrightarrow & 0 \end{array}$$

Now here's where the mathematics happen : there are **two ways** in which you can plug this diagram into a spectral sequence. Either by considering the double complex $(A^{pq})_{p,q\in\mathbb{Z}}$, or $(A^{qp})_{p,q\in\mathbb{Z}}$. This will yield two different sources of information on a single object : the total complex associated to both of those double complexes. And usually, one way gives you a lot of easily available information on the cohomology groups of the total complex, which in turn give you information on the second spectral sequence.

You should remember those two pictures : one orientation goes like this...



... and the second one has mirror order :



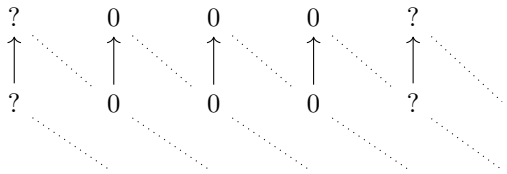
Let's prove the five lemma with this method. It is a classic statement saying that if the following diagram has exact lines, that all four vertical morphisms on the sides are isomorphisms then the middle one is an isomorphism too.

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_5 \\ \uparrow{\scriptstyle l} & & \uparrow{\scriptstyle m} & & \uparrow{\scriptstyle n} & & \uparrow{\scriptstyle p} & & \uparrow{\scriptstyle q} \\ M'_1 & \xrightarrow{g_1} & M'_2 & \xrightarrow{g_2} & M'_3 & \xrightarrow{g_3} & M'_4 & \xrightarrow{g_4} & M'_5 \end{array}$$

Firstly, entering this diagram into the spectral sequence with the first orientation yields at page 1, by exactness of the lines :

$$\begin{array}{ccccc} ? & 0 & 0 & 0 & ? \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ ? & 0 & 0 & 0 & ? \end{array}$$

It is easy to see that all the terms of this spectral sequence have converged. By looking at diagonals of constant $p+q$, this proves that **the total complex has homology zero in degree** 2 **and** 3 **at least**.



Now this has been established, let's look at the spectral sequence the other way around. In page 1, we obtain :

$$0 \longrightarrow 0 \longrightarrow ? \longrightarrow 0 \longrightarrow 0$$

$$0 \longrightarrow 0 \longrightarrow ? \longrightarrow 0 \longrightarrow 0$$

Because the objects on the upper left and on the lower right are 0, the objects in the middle have converged. Since they are alone on their diagonal, they represent the homology group in degree 2 and 3. And since this homology was zero, those should be zero too, which amounts to the fact that the middle morphism is an isomorphism. Careful reading of this proof will give you a more subtle statement : the morphism on the left need only be an epimorphism (which is equivalent to having 0 cohomology on the codomain) and the morphism on the right need only be a monomorphism (which is equivalent to having 0 cohomology on the domain).

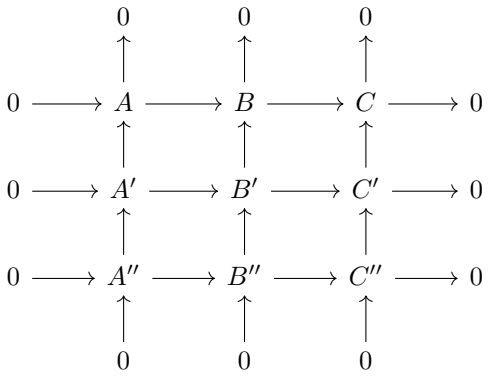
If you have understood well spectral sequences and have done those proofs once through diagram chasing, those proofs should be greatly satisfactory.

Here are other proofs that closely follow this method.

Exercise : The Nine Lemma *

On the commmutative (or anticommutative) diagram underneath, where the columns are exact, prove the three following facts :

1. If the top two rows are exact, prove the bottom one is a complex and that it is exact too.
2. Same question but replacing the top two rows with the two bottom rows.
3. If the top and the bottom rows are exact, and the middle row vanishes, prove the middle row is exact.

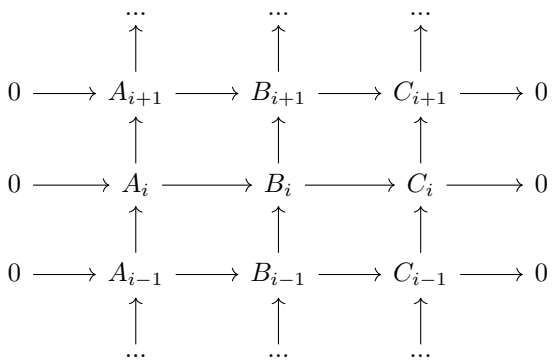


Solution : Taking cohomology starting vertically gives you zero cohomology of the total complex. Taking cohomology horizontally gives you on page 1 *three unknown items that are alone on their diagonal, and thus must yield zero in cohomology. So they must all be zero, and thus the middle sequence must be exact.*

Even a part of the fundamental theorem of homological algebra may easily be deduced from here (although we haven't got the most important part, namely naturality).

Exercise : The Fundamental Theorem Of Cohomological Algebra **

Using spectral sequences, prove the existence of a connecting morphism in the fundamental theorem of cohomological algebra. Start from the diagram underneath.



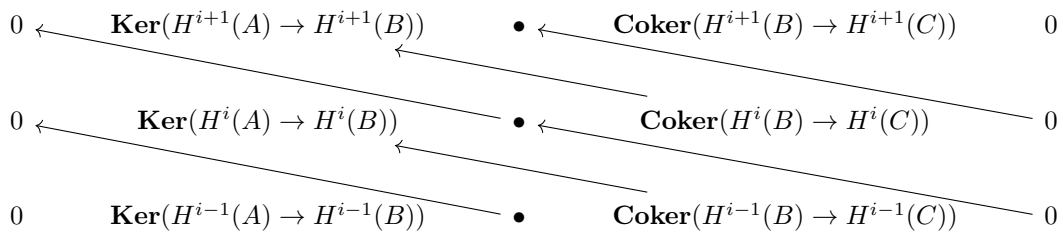
Solution : starting horizontally yields zero everywhere, so the total complex has zero cohomology in all degrees. Then, taking the spectral sequence the other way yields in cohomology the following diagram in page 1*.*

$$0 \longrightarrow H^{i+1}(A) \longrightarrow H^{i+1}(B) \longrightarrow H^{i+1}(C) \longrightarrow 0$$

$$0 \longrightarrow H^{i}(A) \longrightarrow H^{i}(B) \longrightarrow H^{i}(C) \longrightarrow 0$$

$$0 \longrightarrow H^{i-1}(A) \longrightarrow H^{i-1}(B) \longrightarrow H^{i-1}(C) \longrightarrow 0$$

Now, on page 2*, we get a diagram of the form :*



It is clear that all the dots on the middle column have converged, and the filtration implies that they must be zero. Now all the others are bound to converge at the next spot, so the arrows linking kernels and cokernels must be isomorphisms. The linking homomorphism is obtained by composing projection of $H^i(C) \to \textbf{\textit{Coker}}(H^i(B) \to H^i(C))$, isomorphism with the kernel and injection of the kernel in $H^{i+1}(A)$. Exactness of the long sequence is because of the domain and codomain of the connecting morphism, as well as the fact that the dots on the middle column are zero.

One last exercise to convince you that spectral sequences are spectacular computational tools.

Exercise : Exactness of the Mapping Cone **

Let $A^\bullet$ and $B^\bullet$ be two cohomological complexes, and $\mu : A^\bullet \to B^\bullet$. Define the mapping cone of μ as the following complex : $C_i = A_i \oplus B_{i-1}$ and $d : C_i \to C_{i+1}$, $(a, b) \mapsto (-d_A(a), \mu(a) + d_B(b))$. We wish to prove that μ induces an isomorphism in cohomlogy if and only if the mapping cone is exact.

1. Prove it through diagram chasing.
2. Prove it through spectral sequences (hint : prove there exists a long exact sequence

$$... \to H^{i-1}(C) \to H^i(A) \to H^i(B) \to H^i(C) \to H^{i+1}(A) \to ...$$

...and conclude).

Solution : there's nothing complicated in the diagram chase, it's just annoying. The second proof is much more elegant, and uses the filtration and the fact that all the terms have already converged at page 2. This exact sequence has zero maps. Note that we do get the right maps in the mapping cone, since in order to use spectral sequences you have to make your diagrams anticommutative first, hence the minus sign.

This may take a while, but should eventually make you feel much better about spectral sequences.

Here's a last exercise, which can be quite useful sometimes.

Exercise : The Low Degree Exact Sequence ***

Let E_r^{pq} be a spectral sequence in the right quadrant starting at an arbitrary degree a. Suppose it converges to the sequence $(H^n)_{n\in\mathbb{N}}$. Prove that there is an exact sequence :

$$0 \to E_2^{1,0} \to H^1 \to E_2^{0,1} \to E_2^{2,0} \to H^2$$

Solution : the filtration at $n = 1$ is written as an exact sequence $0 \to E_\infty^{1,0} \to H^1 \to E_\infty^{0,1} \to 0$. Writing the spectral sequence shows that $E_2^{1,0} = E_\infty^{1,0}$ and that $E_\infty^{0,1} = \textbf{\textit{Ker}}(E_2^{0,1} \to E_2^{2,0})$. So you may compose the projection on $E_\infty^{0,1}$ with the inclusion in $E_2^{0,1}$, followed by the map $E_2^{0,1} \to E_2^{2,0}$. Now we need a map $E_2^{2,0} \to H^2$. In order to do this, see that we have an inclusion $E_\infty^{2,0} \hookrightarrow H^2$ through the filtration. Now just see that $E_\infty^{2,0} = E_3^{2,0} = \textbf{\textit{Coker}}(E_2^{0,1} \to E_2^{2,0})$. So the composition of the projection and the inclusion gives the right map, and it is easy to see the sequence is then exact.

1.8.3 Grothendieck's Spectral Sequence of Composed Functors

The Grothendieck spectral sequence of composed functors is a theorem that will be very helpful in studying Galois Cohomology. It may sound complicated, but is no more difficult to use than spectral sequences in the former case. We will not prove it.

Theorem : Grothendieck's Composed Functors Spectral Sequence

Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be three abelian categories, and $F : \mathcal{A} \to \mathcal{B}$, $G : \mathcal{B} \to \mathcal{C}$ two covariant left exact functors. Suppose that F sends injectives in $\mathcal{A}$ to G-acyclical objects in $\mathcal{B}$ (objects M such that $R^iG(M) = 0$ for $i > 0$, such as injective objects). Then there is a spectral sequence starting at page 2 with the following convergence :

$$E_2^{pq} = (R^pG)((R^qF)(A)) \implies R^{p+q}(GF)(A)$$

This theorem is very useful when studying the cohomology of a functor that can be described as the composite of two other functors. Here is an example : let $H \subset G$ be a group inclusion with H normal in G, and let A be a G-module. The right exact functor of fixed points under G ($A \mapsto A^G$) can be expressed as the composite of two functors of the same kind : $A \mapsto A^H \mapsto (A^H)^{G/H} = A^G$.

This will yield interesting finiteness or annihilation theorems in the case of group cohomology, the idea (that you can check) being that if the R^iF and the R^jG are zero after ranks i_0 and j_0, then the $R^m(FG)$ is zero after rank $i_0 + j_0$.

It also yields another practical tool, that can often make some proofs rigorous.

Exercise : Exact and Derived Functor **

Let $F : \mathcal{A} \to \mathcal{B}$ be an exact functor that preserves injectives, and $T : \mathcal{B} \to \mathcal{C}$ be a right exact or left exact functor. Express the derived functor of $T \circ F$ in terms of those of T. Find a similar fact if the order of T and F is inverted.

Solution : the exact sequence has one only non zero line, where $q = 0$. So this yields isomorphisms between $R^p(TF)(A)$ and $R^p(T)(FA)$. Inverting F and T works as well since F is acyclical, and we obtain $R^q(FT)(A)$ and $F(R^q(T)(A))$.

Chapter 2

Some Profinite Groups

These notes come from the reading of the excellent notes by Luis Ribes [2].

2.1 Defining Profinite Groups

2.1.1 Definition

A profinite group is a group constructed as a limit of finite groups in the sense that I will make precise in the following definition. We remind the reader that a directed set is an ordered set $(I, \leq)$ such that for any two elements a, b, there exists c such that $c \geq a$ and $c \geq b$.

Definition : Profinite Groups

A **projective system of finite groups** is a triple (I, G, f) where I is a directed set, G is a collection of finite groups G_i indexed by i, and f is a family of group morphisms $f_{i,j} : G_j \to G_i$ for all $j \geq i$ subject to the relationship $f_{i,j} \circ f_{j,k} = f_{i,k}$ for $i \leq j \leq k$.

The **projective limit** of the triple (I, G, f) is the subgroup $\varprojlim G_i$ of $\prod_{i \in I} G_i$ defined by the property, for all $x \in \varprojlim G_i$ and $i \leq j$, $f_{i,j}(x_j) = x_i$.

A profinite group comes with natural projections on each one of the components of the limit, inherited from the product.

The best way to think about profinite groups is as a limit (in the categorical sense) of the diagram spanned by the commutative system. It is the group standing above all the other ones, that verifies the universal property we expect :

Proposition : Universal Property of Profinite Groups

Suppose we have a group G and morphisms $t_i : G \to G_i$ such that $f_{j,i} \circ t_i = t_j$ for $j \leq i$. Then there is a unique morphism $t : G \to \varprojlim G_i$ verifying $p_i \circ t = t_i$.

Proof : With such a setup, define $t : G \to \varprojlim G_i$, which maps g to the element $(t_i(g))_{i \in I}$. It is immediate that it is in $\varprojlim G_i$ by property of the t_i. The property of t is immediate, and the p_i uniquely determine t.

2.1.2 The Profinite Topology

Profinite groups are endowed with a completely natural topology : the topology inherited from the product, where all the G_i are considered to be finite groups with the discrete topology. We call it the **profinite topology** on $\varprojlim G_i$, which then verifies :

Proposition : Properties Of the Profinite Topology

Let $G = \varprojlim G_i$ be a profinite group with its profinite topology. The following properties hold :

- G is a topological group.
- G is Hausdorff.
- G is compact.
- G is totally discontinuous.
- G has a basis of neighborhoods of e consisting of open normal subgroups.

Proof : Since $\varprojlim G_i$ is a subgroup of $\prod G_i$, it is enough to verify that $\prod G_i$ is a topological group. To prove this, remember that the product topology has the property that a map to $\prod X_i$ is continuous if and only if its composition with all projections are continuous. It is now clear that the map : $\prod G_i \times \prod G_i \to G_j$, $x, y \mapsto x_j y_j$ is continuous (the inverse image of $x_j y_j$ contains around each of its points (a, b) the open set $(a_j \times \prod_{i \neq j}) G_i \times (b_j \times \prod_{i \neq j} G_i)$. Inversion is the same proof.

Hausdorfness comes from the fact that products and subsets of Hausdorff are Hausdorff.

Compactness comes from Tychonoff : $\prod G_i$ is compact, and $\varprojlim G_i$ can be seen as the intersection of the closed sets $F_{i,j}$, $j \geq i$, equal to $\Phi_{i,j}^{-1}(\{e\})$ where $\Phi_{i,j}$ is the composite of the projection $\prod_{i \in I} G_i \mapsto G_j \times G_i$, and $G_j \times G_i \to G_i$, $(x, y) \mapsto p_{i,j}(x)^{-1} y$, which is continuous by discreteness.

For total discontinuity, let A be connected in $\varprojlim G_i$. If A contains more than two points a and b, their projections on a certain coordinate will have different values. However, projections must be continuous and send connected components to connected components : so their image can't be more than a point.

Obtaining a basis of open neighborhoods of e made up of normal subgroups is tireless, taking the subgroups of $\prod G_i$ where all components are G_i except for a finite number of them, and intersecting them with $\varprojlim G_i$. They are clearly open, normal, since being normal in the top group implies being normal in the lower group, and by definition of the product topology they are a basis of neighborhoods of e.

We have the following, much harder to prove theorem :

Theorem : Topological Characterization of Profinite Groups

A group G can be described as a profinite group if and only if it satisfies the following properties :

- G is compact and totally discontinuous.
- G is compact, and G has a fundamental system of neighborhoods of e made up of open, normal subgroups.

Proof : not included in this version.

2.1.3 Examples

Here are examples of profinite groups. Which will also be the moment for you to do a few exercises.

Exercise : Profinite Completion of a Group ***

Let G be an arbitrary group, and denote $\mathcal{N}$ the set of all normal subgroups normal of G with finite index, partially ordered by inclusion.

1. Devise a projective system of finite groups where the finite groups are the quotient groups G/N where $N \in \mathcal{N}$, and $G/N \geq G/M \iff N \subset M$. The limit of this system is called the profinite completion of G, and is denoted $\hat{G}$.
2. Devise a natural map $G \to \hat{G}$.
3. Prove that this map has dense image.
4. Prove that this map is injective if and only if G is residually finite, i.e $\cap N = 1$.

Solution : in question 1*, the only thing to verify is that this defines indeed a directed set. To see this, notice that normal subgroups of finite index are closed under intersection, since* $G \to G/N \times G/M$ *is surjective and has kernel* $N \cap M$*. The natural map* $G \to \hat{G}$ *is clearly the projection in all degrees. For the dense image, consider an open set* U *which is not equal to the whole group for a finite number of components* G/N_i*. Then the component of* U *in* $G/\cap N_i$ *contains an element which projects in all of those* G/N_i *in* U *(look at the definition of a profinite group). So the image is dense. Now the property of injectivity* $\iff$ *residually finite is essentially self-proving : if it is not residually finite then it cannot be injective, and if it is residually finite the image is* e *if and only if the input is* e*.*

Exercise : Profinite and pro-p completion of $\mathbb{Z}$ ***

We now study a special case of the former situation. Let $\mathbb{Z}_p$ denote the p-adic integers, the profinite limit of the groups $\mathbb{Z}/p^n\mathbb{Z}$ for $n \in \mathbb{N}$ and projections $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ given by reduction. On the other hand, let $\hat{Z}$ denote the profinite completion of $\mathbb{Z}$. Prove that $\hat{\mathbb{Z}} \simeq \prod_{p \text{ prime}} \mathbb{Z}_p$.

Solution : devise a map from the product of $\mathbb{Z}_p$ *to* $\hat{\mathbb{Z}}$ *by sending* $(x_{p,n})$ *to each* $\mathbb{Z}/n\mathbb{Z}$ *by decomposing* $\mathbb{Z}/n\mathbb{Z} \simeq \prod \mathbb{Z}/p_i^{n^i}\mathbb{Z}$*, and then taking the obvious reduction mapping. It is obvious that this makes the right diagrams commute. Then devise a map from* $\hat{\mathbb{Z}} \to \prod_{p\ prime} \mathbb{Z}_p$ *by sending each element to its image modulo* p^i *for all* p *and all* i*. It is an easy check to see that these maps are inverses.*

2.2 Basic Properties of Profinite Groups

Here are firstly some properties about profinite groups and their subgroups.

Proposition : Some Lemmas about Profinite Groups

- An open subgroup of a profinite group is closed.
- A closed subgroup of a profinite group is the intersection of all the open subgroups that contain it.
- A closed subgroup of a profinite group is a profinite group, and has a description $H \simeq \varprojlim_i H/H \cap U_i$ where the U_i are open normal subgroups of G.
- A quotient of profinite group by a closed subgroup is compact and totally discontinuous (hence profinite if the quotienter is normal). It is described $G/H \simeq \varprojlim_i (G/U_i)/(H/(H \cap U_i))$ where the U_i are open normal subgroups of G.
- A product of profinite groups is a profinite group.

Proofs : the first one is obtained by decomposing along classes. It is a general fact of topological groups.

The second one is obtained in the following way : suppose x is not in H, and let's prove that there is an open subgroup containing H that does not contain x. Do so use compacity to cover H in a finite number of open cosets t_iU_i that do not meet x. Then consider the group $H \cap U_i$: it is indeed open and does not meet x.

For the third one, closed and stays compact and totally discontinuous. For the description, there is an obvious arrow $H \to \varprojlim H/H \cap U_i$ by projection. The image of H is clearly dense by taking intersections of the U_i. Now H is compact so the image is closed, so it is the whole group.

The fourth one is by compacity and total discontinuity. The fourth one is by compacity (projection) and total discontinuity, which is obtained in the following way : if yK and xK are disjoint, find an open subgroup U such that yUK and xUK are disjoint (this is possible by the following proof : consider the map $G \times G \times K \times K \to G \times G$, $t, t', k, k' \mapsto xtk, xt'k'$. Then the image of $e \times e \times K \times K'$ is disjoint from the diagonal. So if the image of a compact in the source is disjoint from a compact in the target, it is easy to devise an open neighborhood of a compact of the source which is still disjoint of the target. This neighborhood contains a subset of the form $U \times U \times K \times K'$). Now divide $G = \sqcup x_iUK$ (finitely, with say $x_0 = x$ and $x_1 = y$). The image yields a decomposition in open sets $G/K = [xU] \sqcup V$ where V is open and contains the image of yU. Thus x and y are not in the same connected component.

For the next step of this proof, a way to obtain it is as follows : notice that the arrow $G/H \to \prod(G/U_i)/(H \cap U_i)$ is part of the obvious commutative diagram :

$$\begin{array}{ccc} G & \xrightarrow{\simeq} & \prod G/U_i \\ \downarrow & & \downarrow \\ G/H & \longrightarrow & \prod(G/U_i)/(H/H \cap U_i) \end{array}$$

...which yields surjectivity. Injectivity comes from the fact that if an element is in the group generated by H, U_i for all i, then it is in H since H is the intersection of the open subgroup that contain it.

For the fifth, a product of compacts is compact, a product of totally discontinuous is totally discontinuous.

The nice thing to remember about profinite groups is that they behave exceptionnally well under the usual algebraic operations : subgroups, quotients, and more than anything : products, and thus limits.

Profinite groups also possess a nice properties relative to sections : all of their quotients are actually topological retracts from them.

Proposition : Profinite Groups and Sections

Let G be a profinite group and let $H \subset G$. Then the projection $\pi : G \to G/H$ admits a continuous section $\sigma : G/H \to G$ such that the composition $\pi\sigma : G/H \to G \to G/H = \mathbf{Id}_{G/H}$. Thus we have a homeomorphism (but not a group isomorphism !) $G \simeq G/H \times H$.

Proof : here is the idea of the proof. First, we start by showing that if K is a normal closed subgroup contained in H, such that K has finite index in H, then the projection $G/K \to G/H$ admits a section. Then we do a transfinite induction to go from K to ever smaller subgroups, and use Zorn's lemma to prove that there must exist a section from $G/H \to G/\{e\} \simeq G$.

Now here are the details : to obtain the first lemma, the idea is that you want to find an open subgroup U such that $G/H = \sqcup x_iUH/H$, such that the restricted projections $G/K \to G/H$, $x_iUK/K \to x_iUH/H$ are homeomorphisms. Those maps are clearly surjective and continuous. For injectivity, if $\pi(x_iu_i) = \pi(x_ju_j)$, this means that $x_j^{-1}x_iu_iu_j^{-1} \in H$ so $x_j = x_i$. Now we must have $u_iu_j^{-1} \in H \implies u_i = u_j$ modulo K. To do so, since K has finite index in H, it is open in H and thus there is an open normal subgroup U such that $H \cap U \subset K$. This is all it takes.

Now this is proven, consider the projection $G \to G/H$. Now consider the set of maps $G/H \to G/K$ where K is a closed subgroup contained in H, such that the composition $G/K \to G/H \to G/K$ is the identity. We will prove that this is an inductive set. It is not empty since it contains the identity of $G/H \to G/H$. Now consider a chain $H \supset K_0 \supset K_1 ...$ and the corresponding section. We can then construct the section $G/H \to G/(\cap K_i)$: it is a little check to see that the sections $G/H \to (G/K_i)$ are a map from G/H on the projective system that they form, with projections $G/K_{i+1} \to G/K_i$. Now a subtle point is that the surjections $G/(\cap K_i) \to G/K_i$ induce a continuous map to the projective limit of the G/K_i, which has obviously dense image and which is closed since $G/(\cap K_i)$ is compact. Moreover, it is clearly injective. So we have an isomorphism (topological and algebraic). Now compose isomorphisms above and under. And boom. So we have inductiveness.

2.3 Supernatural Numbers and Sylow p-groups

A supernatural number is a formal expression of the form $\prod p^{v_p}$ where the product ranges over the primes (possibly infinitely many) and the v_p are elements of $\mathbb{N} \cup \{\infty\}$. Supernatural allow us to generalize the notion of cardinal and index for profinite groups.

Definition : Cardinal And Index for Profinite Groups

Let G be a profinite group. Its **cardinal** is defined as the supernatural number which is the lowest common multiple of the groups G/U_i, where U_i ranges over the open subgroups of G. More generally, when H is a closed subgroup of G, its **index** $[G : H]$ is defined as the lowest common multiple of the indices $[G/U_i : H/H \cap U_i]$.

Exercise : Indices in Profinite and Finite Groups ***

Check that this definition coincides with the classical index definition we have in the case where $[G : H]$ is finite (for the old, and the new definition of index).

Solution : Suppose $[G : H]$ is finite in the sense that there is a finite number of cosets gH. Then the description $G/H \simeq \varprojlim (G/U_i)/(H/H \cap U_i)$ verifies $G/H \simeq (G/U_i)/(H/H \cap U_i)$ for some i. Indeed, this morphism is always surjective, and becomes injective for i large enough since finitely many compact sets (here, the classes of H) can always be separated in disjoint open sets for U_i small enough. So the new index is at least that of the new, and can be shown to be smaller by surjectivity of projections.

Conversely, suppose that $[G : H]$ is finite in this new sense. This means that the cardinals $(G/U_i)/(H/H \cap U_i)$ are bounded. Thus they have a largest element K. The arrow of G/H onto this largest element is surjective, and must be injective, since all arrows above K are isomorphisms (surjective in finite sets), and thus an element of G/H has an image in $\prod (G/U_i)/(H/H \cap U_i)$ determined by its image in K.

Thankfully, we have this fact :

Proposition : The Index Formula for Profinite Groups

Let $K \subset H \subset G$ be profinite groups. Then we have an equality (of supernatural numbers) :

$$[G : K] = [G : H][H : K]$$

Proof : Denote K_U, H_U, G_U the projection of K, H, G in G/U. We have the equality $[G_U : K_U] = [G_U : H_U][H_U : K_U]$. All we have to check is that the lcm of $[H_U : K_U]$ taken over open normal subgroups of G is indeed $[H : K]$, but this is true since every open subgroup of H contains a normal subgroup of the form $U' = H \cap U$ where U is open normal in G : this yields a surjective mapping of $H_{U'}/K_{U'} \to H_U/K_U$ for all U open in H. Thus all it takes is to consider the groups obtained by normal subgroups of G, which we do. Now just take the lcm over U of this expression.

2.3.1 Sylow Subgroups of Profinite Groups

Now that we have defined the index of profinite groups and subgroups, we can now define the notion of sylow subgroups in profinite groups.

Definition : Sylow Subgroup of a Profinite Group

Let p be a prime number and $H \subset G$ be an inclusion of profinite groups. H is said to be a **p-Sylow subgroup** of G if the index $[H : 1]$ is a power of p (H is said to be a pro-p-group) and if the index $[G : H]$ is coprime to p.

Exercise : Surjective Maps and Sylow Subgroups ***

Let $f : G \to G'$ be a continuous surjective morphism of profinite groups. Prove that the image of a p-Sylow subgrooup of G is a p-Sylow subgroup of G'.

Solution : clearly the image $f(H)$ is a pro-p-group, since open subgroups of $f(H)$ are images of open subgroups of H which yields surjective maps $H/U \to f(H)/f(U)$. Now see that there is a continuous surjection $G/H \to G'/f(H)$, and thus by the index formula the index of $G'/f(H)$ must be coprime to p.

Sylow subgroups of profinite groups have analogous properties than in the finite case, thanks to the following lemma :

Proposition : Profinite Limits of Non-Empty Sets / Compact Topological Spaces

A profinite limit of non empty compact topological spaces / finite sets is never empty.

Proof : The second case implies the first one. To do notice that a profinite limit of non empty compact topological spaces can be described as a decreasing intersection of compacts in the compact product of the spaces.

We now cite the essential properties of Sylow subgroups of profinite groups, that we advise you to try and prove them by yourself before reading their proofs.

Proposition : Properties of Sylow Subgroup of Profinite Groups

- For all prime number p, G possesses a p-Sylow.
- All p-Sylows of G are conjugates of one another.
- Every pro-p-subgroup of G is contained in a p-Sylow.
- If G is abelian, it is the direct product of its p-Sylows.

Proof : Using the fact that p-Sylow are transferred by surjections, for the first one notice that each G/U_i possesses a p-Sylow, denoted H_i. Now use the lemma to construct a subgroup $G \supset H = \varprojlim H_i$ which is closed because compact, and where $G/H \simeq \varprojlim G_i/H_i$ clearly has index coprime to p.

For the second one, let H and H' be two p-Sylows. In each G/U_i, their images are conjugates by an element c_i. The set of elements c_i such that $c_i H_i c_i^{-1} = H_i'$ is non empty for all i and works down by projective limit, so we may find one that works for everyone.

For the third one, let H be a pro-p-group. Its image H_i in each finite quotient is still pro-p, so is contained in a p-Sylow. Then it's the same argument again.

This is true for finite abelian groups. Now see that in the process of taking the profinite limit, you are actually taking the limit on each p-subgroup individually since projections between p and q groups are 0. Now this comes from the fact that in a category, limits (here products and profinite group) commute : taking the profinite limits and then the product or first the products and then the profinite limit of the whole is the same.

Chapter 3

Group Cohomology

Groups are easy to study when they are finite, but quickly become very complicated. It is the case for example of important groups, such as the Galois group of infinite algebraic extensions. A good way to study them is to study their representations.

Group cohomology is another approach to the matter, which is at the same time a generalization and a particularization of representation theory : it is more general in the way that the object it studies are G-modules, modules on the ring $\mathbb{Z}[G]$ (which is more general than representations), but studies the associated cohomology of a certain functor, which we will dive into.

Our study of group cohomology will be divided in seven sections which I will start by describing.

1. **The Abelian Category of Modules on Finite Groups** is an introduction to what G-modules on finite groups are, and to the main tools that are associated to them, with a focus on induction.
2. **Cohomology of Finite Groups** aims at defining and constructing, as you'd expect, the cohomology of finite groups. An accent is put on the practical tools available to study it : inductions, explicit descriptions, change of groups such as restriction - corestriction, and finally, the Hoschild Serre spectral Sequence.
3. In **Modified Cohomology Groups**, we slightly modify and extend our functor into a longer one, which computes a slightly different kind of cohomology. As an application, we will be able to compute the cohomology of cyclic groups.
4. **Cup-Products and Tate Nakayama** is dedicated to the construction of a tool called the **cup-products**, which is a way of bringing the tensor product to our theory. We use it to state, without proof, the Tate-Nakayama theorem.
5. **Cohomological Triviality** is a nice chapter in which the acquired constructive knowledge of the past chapters is put into practice to study when modules have trivial cohomology, as well as properties of the modules that do.
6. In **Cohomology of Profinite Groups**, we extend our theory of cohomology to profinite groups. We spend a significant amount of time studying the properties that move up from finite groups to profinite groups.
7. **Cohomological Dimension** studies a particular invariant of a group, cohomological dimension, which is related to certain annihilation properties.

Those chapters essentially fit into two categories : chapters 1, 2, 3, 4 and 6 are constructive chapters, where we define objects and find out their properties, while chapters 5 and 7 "put things in practice". For a first "lighter" read, one may skip chapters 3, 4 and 5 without great damage. However, they will be necessary to move on to the applications of Group Cohomology to local class field theory.

The treatment of those matters is very much inspired from David Harari's excellent book on the matter ([1]).

3.1 The Abelian Category of Modules on Finite Groups

In all of this section, G is a finite group.

3.1.1 Definition

Definition : The Abelian Category of Modules on Finite Groups

We call the category of module on a finite group G, or simply the category of G-modules when it is implied that G is a finite group, the category $\mathbf{Mod}_G$ of modules on the ring $\mathbb{Z}[G]$, or equivalently modules with an action of the finite group G by linear automorphisms.

As all categories of modules on a ring, $\mathbf{Mod}_G$ has enough injectives and projectives, which makes it a good place to do homological algebra. Group cohomology consists in doing homological algebra in this category to retrieve information on the group G.

In the three following sections, we describe how to construct some modules on finite groups from others.

3.1.2 G-modules and G/H-modules

Let H be a normal subgroup of G. One has a projection $G \to G/H$. In this section, we study how such projections allow us to construct other modules from existing ones.

Definition : Deflation and Inflation

Let A be a G/H-module. Then one can make A an G module, of base set A and with action $*$ of G defined as $g * a = p(g) \cdot a$. This module called the **inflation** of A from G/H to G. Seeing that G/H-linear maps become G-linear in that context, we have defined a functor $\mathbf{Inf}^G_{G/H} : \mathbf{Mod}_{G/H} \to \mathbf{Mod}_G$.

Let A be a G-module. Then one can construct a G/H-module A^H of base set A^H, of the fixed points under the action of H and with action $*$ of G/H defined as $p(g) * a = g \cdot a$ (which does not depend on the choice of a g). This module called the **deflation** of A from G to G/H. Seeing that restricting linear maps to A^H turns them into G/H-linear maps, we have defined a functor from $\mathbf{Def}^G_{G/H} : \mathbf{Mod}_G \to \mathbf{Mod}_{G/H}$.

The following proposition is fairly easy to derive :

Proposition : Inflation/Deflation Adjunction

The inflation and deflation functors are respectively left and right adjoint functors of one another. In other words, for all G-module A and G/H-module B, there is a natural isomorphism :

$$\mathbf{Hom}_G(\mathbf{Inf}^G_{G/H}(B), A) \simeq \mathbf{Hom}_{G/H}(B, \mathbf{Def}^G_{G/H}(A))$$

Proof : the post-composition of a G/H-morphism between B and A^H with the inclusion of $A^H \subset A$ is exactly a G-morphism between B (as a G-module) and A. Conversely, any G-morphism between B and A has value in A^H because the action of H on $\mathbf{Inf}^G_{G/H}(B)$ is trivial. It is easy to check that those correspondances are inverses of one another. Naturality is an easy (though slightly tedious) check that we leave to the reader.

It is immediate that the functor $\mathbf{Inf}^G_{G/H}$ is exact, since it doesn't change neither sets nor morphisms. This allows us to describe the (co)homological properties of the functor $\mathbf{Def}^G_{G/H}$, which will be of great importance to us in group cohomology.

Proposition : Homological Properties of Deflation

The Deflation functor preserves injective objects. Moreover, it is left-exact but not right exact.

Proof : the fact that it preserves injectives is immediate, since if A is injective in $\boldsymbol{Mod}_G$, then $\boldsymbol{Hom}_{G/H}(\_, \boldsymbol{Def}^G_{G/H}(A)) \simeq \boldsymbol{Hom}_G(\boldsymbol{Inf}^G_{G/H}(\_), A)$, which is exact as a composition of two exact functors.

To obtain left exactness, take an exact sequence $0 \to A \to B \to C$, then apply deflation. It is obvious that the arrow $f : A^H \to B^H$ remains injective, since it is a restriction of an injective arrow. Now if $x \in \boldsymbol{ker}(B^H \to C^H)$, this means that there is an element $y \in A$ such that $f(y) = x$. If we have $y \neq g \cdot y$ for $g \neq e$, then $f(y) = gf(y) = f(gy)$ with $y \neq gy$ which is not possible since f is injective. To give a counter-example for right exactness, take $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2 \to 0$ where everyone has an action by $\mathbb{Z}/2$ which is $x \mapsto -x$ in the two first components and is the identity on the last one.

The heart of group cohomology is actually to study the cohomology associated to this left exact, not right exact functor.

3.1.3 G-modules and H-modules

In this section, let $H \subset G$ be a subgroup, not necessarily normal. There are also ways to go back and forth between H-modules and G-modules.

Definition : Restriction and Induction

Let A be a G-module. One can construct an H-module out of A by restricting the action of G to the action of just H. This module is called the **restriction** of A from G to H. By taking sets and morphisms to themselves, one constructs a forgetful functor $\mathbf{Res}^G_H : \mathbf{Mod}_G \to \mathbf{Mod}_H$.

Let A be an H-module. One can naturally construct an G-module out of A, written $I^H_G(A)$, of base set $\mathbf{Hom}_H(\mathbb{Z}[G], A)$, where $\mathbb{Z}[G]$ is seen as an H-module. The action by G is given by $g \cdot f(x) := f(xg)$. It is called the **induction** of A from H to G. By sending a morphism $f : A \to B$ to the post-composition morphism $f^* : \mathbf{Hom}_H(\mathbb{Z}[G], A) \to \mathbf{Hom}_H(\mathbb{Z}[G], B)$, one constructs a induction functor $\mathbf{Ind}^G_H : \mathbf{Mod}_H \to \mathbf{Mod}_G$.

Dually, but less trivially than in the former case, we obtain an adjunction between the pair of morphisms we just defined.

Proposition : Restriction/Induction Adjunction

The restriction and induction functors are respectively left and right adjoint functors of one another. In other words, for all G-module A and H-module B, there is a natural isomorphism :

$$\mathbf{Hom}_H(\mathbf{Res}^G_H(A), B) \simeq \mathbf{Hom}_G(A, \mathbf{Ind}^G_H(B))$$

Proof : given an H-morphism $f : A \to B$, one can construct a morphism $\tilde{f}$ from $A \to \boldsymbol{Hom}_H(\mathbb{Z}[G], B)$, by sending x to the H-morphism from $\mathbb{Z}[G] \to B$, $\lambda \mapsto [u \mapsto f(u \cdot x)]$. This may be a little tedious to ingest, but I invite you to simply take the time to check that the image of λ is indeed a H-morphism, and that the morphism in itself is truly a G-morphism.

Conversely, given a G-morphism $f : A \to \boldsymbol{Ind}^G_H(B)$, one can construct an H-morphism $A \to B$ by $a \mapsto f(a)(1)$ (remember that $f(a)$ is itself a morphism). Once again, you should take the check as a small exercise.

Naturality is nothing hard, but is an absolute formal headache: you may do it if you want to, but you may also believe that it has been checked by many and always found true.

The **Ind** functor will be also very dear to us in our cohomology theory. This is why we take some time to describe some of its important properties.

Proposition : Homological Properties of Induction

If B is an injective H-module, then $\mathbf{Ind}_H^G(B)$ is an injective G-module. Also, the functor $\mathbf{Ind}_H^G$ is exact.

*Proof : the preservation of injectivity is the same proof as above, since **Res** is clearly exact. Exactness is obtained from the fact that $\mathbb{Z}[G]$ is projective in $\boldsymbol{Mod}_H$ since it is free : for a base, one might take representatives of cosets for the left action of H on G. Thus the corresponding $\boldsymbol{Hom}_H(\mathbb{Z}[G], \_)$ functor is right exact.*

Using the fact that G is finite, we can actually obtain a double adjunction between **Ind** and **Res**.

Proposition : Induction/Restriction Adjunction

The restriction and induction functors are respectively right and left adjoint functors of one another. In other words, for all G-module A and H-module B, there is a natural isomorphism :

$$\mathbf{Hom}_H(B, \mathbf{Res}_H^G(A)) \simeq \mathbf{Hom}_G(\mathbf{Ind}_H^G(B), A)$$

Proof : Given a H-morphism $f : B \to A$, a morphism of $\boldsymbol{Hom}_G(\boldsymbol{Ind}_H^G(B), A)$ is canonically obtained through the mapping $\lambda \mapsto \sum_{g \in G/H} g^{-1} f(\lambda(g))$ - I leave it to you to check that this expression does not depend on representatives of G/H, and is indeed a G-morphism. To go the other way around, given $f \in \boldsymbol{Hom}_G(\boldsymbol{Ind}_H^G(B), A)$, define an H-morphism from A to B that sends to b the evaluation of f at λ_b, the map that is b on the class of H and 0 elsewhere. You can check that this is indeed a G-morphism. You can also check that those two maps are inverses of one another (though it is a bit tricky). Naturality is another headache that you may undertake or not depending on your level of masochism.

Similarly as above, we obtain the following fact :

Proposition : Homological Properties of Restriction

If A is an injective G-module, then $\mathbf{Res}_H^G(A)$ is an injective H-module. If A is a projective G-module, then $\mathbf{Res}_H^G(A)$ is a projective H-module.

Proof : Restriction has a left and right adjoint which is exact. This proves all of our properties.

3.2 Cohomology of Finite Groups

3.2.1 Formal Definition

We can now define the cohomology of a finite group G relatively to a G-module A. Remember that the deflation functor $A \to A^H$ for H a subgroup of G was a left exact functor. Cohomology is the study of the cohomology of the biggest deflation functor.

Definition : Group Cohomology

Let G be a finite group, and let $\mathbf{Mod}_G$ be the associated module category. Let A be a G-module. The **cohomology groups** of G relative to the G-module A are the groups :

$$H^i(G, A) = R^i\mathbf{Def}_1^G(A)$$

...where $R^i\mathbf{Def}_1^G$ is the i-th derived functor of $\mathbf{Def}_1^G$, the functor defined from $\mathbf{Mod}_G \to \mathbf{Mod}_1$ that maps to A the abelian group A^G of fixed points under G. We can similarly define the $H^i(H, A)$, the derived functors of the functor $\mathbf{Def}_{G/H}^G$, which maps $A \to A^H$, the G/H-module (or abelian group, according to the context) of fixed points under H.

Silly Check :

If G is the trivial group, what is its cohomology ?

The composite of $\mathbf{Def}_{G/H}^{G}$ with the forgetful functor with value in $\mathbf{Ab}$ is the same thing as the composite of the forgetful functor from $\mathbf{Mod}_G \to \mathbf{Mod}_H$ with the $\mathbf{Def}_1^H$ functor. Checking the effect of composing functors in cohomology is a rather complicated matter, but when one of the two is exact it is easily achieved through the Grothendieck spectral sequence of composed functors. Here, it is the case.

With this complicated definition, it is too early to compute anything except the routine check we made above. However, the following sections are all aimed at making some computations possible.

3.2.2 Explicit Description of Cohomology Groups

Our first goal will be to prove the following, fairly amazing proposition.

Theorem : Towards the Explicit Description of Cohomology Groups

Let A be a G-module, and let :

$$... \to P_i \to P_{i+1} \to ... \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

... be a projective resolution of $\mathbb{Z}$ in $\mathbf{Mod}_G$ ($\mathbb{Z}$ has trivial action by G). Then the functors that map A to the cohomology groups of the complex :

$$0 \to \mathbf{Hom}_G(P_0, A) \to \mathbf{Hom}_G(P_1, A) \to \mathbf{Hom}_G(P_2, A)...$$

... and that map morphism to the morphisms associated to post-composition $\mathbf{Hom}_G(P_i, A) \to \mathbf{Hom}_G(P_i, B)$ is a cohomological δ-functor.

Additionally, it is isomorphic to the group cohomology functors defined earlier.

Proof : the fact that it is a cohomological δ-functor is a consequence of the fact that the $\boldsymbol{Hom}_G(P_i, \cdot)$ functors are all exact and of the snake lemma.

To obtain the isomorphism with our cohomology functor is the harder part. One first part is to obtain an isomorphism in degree 0. First of all, it is easy to see that the functor $\boldsymbol{Hom}_G(\mathbb{Z}, \cdot)$ is isomorphic to the functor $\boldsymbol{Def}_1^G$, and then that an element of $\boldsymbol{ker}(\boldsymbol{Hom}_G(P_0, A) \to \boldsymbol{Hom}_G(P_1, A))$ can be canonically associated to an element of $\boldsymbol{Hom}_G(\mathbb{Z}, \cdot)$ through the exact sequence : $0 \to \boldsymbol{Im}(P_1 \to P_0) \to P_0 \to \mathbb{Z} \to 0$ and conversely so. It is also not hard to see that this association is natural, and thus we have our natural isomorphism between the first functor and $H^0(\mathbb{Z}, \cdot) = \boldsymbol{Def}_1^G$. By universality, this first isomorphism extends uniquely to morphisms in all degrees. All we have to do then is check that the second functor vanishes on injectives: if it is so, we will prove by induction that we have isomorphisms in all degrees, through the exact sequence $0 \to A \to I \to B \to 0$, where I is injective as a G-module (see next section for more detail on this kind of methods).

Every G-module can be injected into an induced G-module, which is a module of the form $\boldsymbol{Ind}_1^G(X)$ where X is an abelian group. For example, any G-module A is injected in $\boldsymbol{Ind}^G(A)$ through the map $a \mapsto [g \mapsto g \cdot a]$ (one can easily check that this is a G-morphism). If a G-module is injective, it injects as a direct factor : so by additivity of cohomology we just have to check that our second functor dies in degree ≥ 1 on modules of the form $\boldsymbol{Ind}_1^G(X)$. Now, by adjunction, the sequence :

$$0 \to \mathbf{Hom}_G(P_0, \mathbf{Ind}_1^G(X)) \to \mathbf{Hom}_G(P_1, \mathbf{Ind}_1^G(X)) \to \mathbf{Hom}_G(P_2, \mathbf{Ind}_1^G(X))...$$

...is naturally isomorphic to the sequence :

$$0 \to \mathbf{Hom}(\mathbf{Def}_1^G(P_0), X) \to \mathbf{Hom}(\mathbf{Def}_1^G(P_1), X) \to \mathbf{Hom}(\mathbf{Def}_1^G(P_2), X)...$$

Exactness of this complex can be proven as so : the P_i are projective G-modules, so they are a direct factor of a free G-module. A free G-module is also a free abelian group. So the P_i are direct factors of free abelian groups, so they are free abelian groups.

Now in the exact sequence $... \to P_{i+1} \xrightarrow{p_{i+1}} P_i \to ...$ seen in the category of abelian groups, we have for all $i \geq 1$, an exact sequence $0 \to \textbf{\textit{ker}}\ p_i \to P_i \to \textbf{\textit{im}}\ p_i \to 0$, which splits since we are working with free abelian groups. So $P_i = \textbf{\textit{ker}}\ p_i \oplus I_i$ where p_i restricts to an isomorphism : $I_i \simeq \textbf{\textit{im}}\ p_i$. This yields a slanted sequence in degrees ≥ 1, which stays slanted after applying $\textbf{\textit{Hom}}(\_, X)$. It is then easy to verify that the above sequence cohomologically dies in degree greater than 1 : for example, in first degree you get ...

$$0 \to \mathbf{Hom}(\mathbf{Def}_1^G(P_0), X) \to \mathbf{Hom}(\mathbf{ker}\ p_1, X) \oplus \mathbf{Hom}(I_1, X) \to \mathbf{Hom}(\mathbf{ker}\ p_2, X) \oplus \mathbf{Hom}(I_2, X)...$$

A morphism in the kernel of p_1^* is actually a morphism that starts from $\textbf{\textit{ker}}\ p_1 \to X$, which can be written as $f = f \circ p_0^{-1} \circ p_0$ where we loosely write p_0^{-1} as a section to the surjection $p_0 : P_0 \to \textbf{\textit{ker}}\ p_1$, which can be done since we are working with free abelian groups.

That was a very long proof, which I hope was not too hard to follow. It is full of very classical homological algebra techniques. This long proof will now allow us to reach a beautiful description of group cohomology. Notice how great a step we have made here : computing the groups $H^i(G, A)$ can now be done with just a projective resolution of $\mathbb{Z}$! Here's how we can gather one.

Definition : Canonical Projective Resolution of $\mathbb{Z}$

Denote L_i the G-module $\mathbb{Z}[G^{i+1}]$ with action of G given component-wise $(g \cdot (g_0, g_1, ..., g_n) = (gg_0, gg_1, ..., gg_n))$. Let $d_i : L_i \to L_{i-1}$ be the G-morphism given by :

$$d_i(g_0, g_1, ..., g_n) = \sum_{j=0}^{i} (-1)^j (g_0, ..., \hat{g_j}, ...g_n)$$

...where the hats stands for omitting the j-th coordinate. Then :

$$... \xrightarrow{d_{i+1}} L_i \xrightarrow{d_i} L_{i-1} \xrightarrow{d_{i-1}} ... \xrightarrow{d_1} L_0 \xrightarrow{d_0} \mathbb{Z}$$

... is a projective resolution of $\mathbb{Z}$ in the category of G-modules.

Proof : Exactness a classic computation that we will not write up here (see [1], page 24). The L_i are all free as G-modules : a base is given by elements of the form $(1, g_1, ..., g_n)$. Indeed, this family clearly generates L_i, and you may check it is free by considering the linear combination : $\sum_{i=1}^{t} (\sum_{j=0}^{|G|} n_i^j g_j) c_i = \sum_{j=0}^{|G|} g_j \sum_{i=1}^{t} n_i^j c_i$, and then using the fact that the first coordinate is one to eliminate each $\sum_{i=1}^{t} n_i^j c_i$ individually.

Now, given a G-module A, we will be interested in the complex :

$$0 \to \mathbf{Hom}_G(L_0, A) \to \mathbf{Hom}_G(L_1, A) \to \mathbf{Hom}_G(L_2, A)...$$

...given with the d_i precomposition arrows.

The abelian groups $\mathbf{Hom}_G(L_i, A)$ are canonically isomorphic to the abelian groups $\tilde{K}^i(A)$ of functions $G^{i+1} \to A$ verifying $f(gg_0, ..., gg_n) = g \cdot f(g_0, ..., g_n)$. Such a function is entirely determined by values taken on elements of the form $(1, g_1, g_1g_2, ..., g_1g_2...g_n)$ (to go from one to another, factor out g_0 and make the right $g_i^{-1}g_i$ appear), which is a base as shown in the proof above. So this transformations yields a natural isomorphism of abelian groups between $\mathbf{Hom}_G(L_i, A)$ and simply the abelian group on functions from $G^i \to A$, by identifying a linear function $f \in \mathbf{Hom}_G(L_i, A)$ to the induced regular function $(g_1, ..., g_n) \mapsto f(1, g_1, g_1g_2, ..., g_1g_2...g_n)$. It is an amusing computation (which justifies the awkward choice of elements of the form $(1, g_1, g_1g_2, ..., g_1g_2...g_n)$) to check the following property :

Theorem : Explicit Description of Cohomology Groups

The cohomological δ-functor $H^i(G,\cdot)$ is isomorphic to the functor that maps an object A to the cohomology groups of the complex :

$$K^0(A) \to K^1(A) \to K^2(A) \to ...$$

where $K^i(A)$ is the abelian group of functions $f : G^i \to A$, and the differentials are given by :

$$df(g_1,...,g_{i+1}) = g_1 \cdot f(g_2,...,g_{i+1}) + \sum_{j=1}^{i}(-1)^j f(g_1,...,g_jg_{j+1},...,g_{i+1}) + (-1)^{i+1} f(g_1,...,g_i)$$

...and the action of morphisms is obtained by post-composition, in order to obtain a morphism $K^i(A) \to K^i(B)$.

I guess your main question now, is, "how did this simplify ***anything*** ?" Well this description is much more concrete than the former, and will allow us to manipulate cohomology groups much more easily, especially in small degrees. For example, here's a few checks that you can make :

Exercise : Some Checks **

Using the explicit description of cohomology groups, check the following properties :

1. If A is a finite G-module, prove that the $H^i(G,A)$ are finite. Moreover, prove that multiplication by $|A|$ kills $H^i(G,A)$.
2. If G acts trivially on A, then $H^1(G,A) = \mathbf{Hom_{Gp}}(G,A)$ (where **Gp** denotes the category of groups). For example, if $G = \mathbb{Z}/n$ acting trivially, $H^1(G,A)$ is isomorphic to the n-torsion subgroup of A.

Solution : this is fairly simple. The only fact to have in mind is that multiplication by n commutes with additive functors.

We will often come back to this definition, especially when we want to construct morphisms between cohomology groups.

3.2.3 Induction Techniques

Induction techniques are very present more generally homological algebra when, in your category, each one of your objects injects into an acyclic objects. For finite G-modules, it is the case, and we already saw it.

Proposition : Properties of Induced G-modules

- Let X be an abelian group. then for all $i \geq 1$, $H^i(G, \mathbf{Ind}_1^G(X)) = 0$.
- Let A be a G-module. Then we have a canonical injection of $A \hookrightarrow \mathbf{Ind}_1^G(A)$.

Proof : The first point of the proof is contained in the proof of the lemma above. The second point is too, by mapping $a \in A$ to $[g \mapsto g \cdot a]$.

This idea is extremely useful for the following reason : let $0 \to A \to \mathbf{Ind}_1^G(A) \to B \to 0$ be an exact sequence. Then the long cohomology sequence yields :

$$0 \longrightarrow A^G \longrightarrow (\mathbf{Ind}_1^G(A))^G \longrightarrow B^G \twoheadrightarrow H^1(G,A) \longrightarrow 0$$

$$\longrightarrow H^1(G,B) \xrightarrow{\simeq} H^2(G,A) \longrightarrow 0 \longrightarrow H^2(G,B) \longrightarrow ...$$

So, we have a surjective arrow $B \to H^1(G,A)$ and isomorphisms $H^{i-1}(G,B) \to H^i(G,A)$. For example, we can derive from here another proof of the fact that if A is finite, then all the $H^i(G,A)$ for $i \geq 1$ are all finite. Indeed, in our exact sequence above, since G is finite, then $\mathbf{Ind}_1^G(X)$ is finite too (a finite amount of choices for each element of G). So is B. The surjective homomorphism thus proves that $H^1(G,A)$ is finite. So is $H^1(G,B)$, since B is finite too.

Here's another important fact that you can prove through these methods.

Proposition : Inductive Limits and Cohomology Groups

Let (A_j) be an inductive system of G-modules. Then we have isomorphisms :

$$\varinjlim H^i(G,A_j) \simeq H^i(G, \varinjlim A_j)$$

Proof : in degree 0*, it is easy to see that* $\varinjlim (A_j^G) = \varinjlim (A_j)^G$ *(if* x *and* gx *are sent to the same* u *after a while, then this implies* $gu = u$*). Then, given an exact sequence* $0 \to A_j \to \boldsymbol{Ind}_1^G(A_j) \to B_j \to 0$*, inductive limits is exact and so yields* $0 \to \varinjlim A_j \to \varinjlim \boldsymbol{Ind}_1^G(A_j) \to \varinjlim B_j \to 0$*. Now we have a natural isomorphism* $\varinjlim \boldsymbol{Ind}_1^G(A_j) \simeq \boldsymbol{Ind}_1^G(\varinjlim A_j)$ *(see* **Ind** *as a hom functor, see that* $\mathbb{Z}[G]$ *is finitely presented since it is a finitely generated free abelian group, and use https://math.stackexchange.com/questions/226479/direct-limits-and-rm-hom. Or prove it directly). Now take in parallel the long exact sequence associated to* $0 \to \varinjlim A_j \to \boldsymbol{Ind}_1^G(\varinjlim A_j) \to \varinjlim B_j \to 0$ *and the direct limit of the long exact sequences associated to* $0 \to A \to \boldsymbol{Ind}_1^G(A) \to B \to 0$*, find an isomorphism in degree* 1 *and conlude by induction.*

3.2.4 Restriction-Corestriction

Restriction-Corestriction techniques makes use of natural transformations relating the cohomology of G and one of its subgroups' H. It is **very useful**.

Definition : Restriction and Corestriction

The inclusion $A^G \hookrightarrow A^H$ is a natural transformation from the functor $\mathbf{Def}_1^G \to \mathbf{Def}_{G/H}^G$ (both seen with codomains in abelian groups). Thus it induces cohomologically, in all degrees, homomorphisms :

$$H^i(G,A) \to H^i(H,A)$$

This morphism is called the **restriction morphism** from G to H, not to be confused with the restriction functor. It will be denoted **Res**.

The map $A^H \to A^G$, $a \mapsto \sum_{g \in G/H} g \cdot a$ is a natural transformation from the functor $\mathbf{Def}_{G/H}^G \to \mathbf{Def}_1^G$. Thus it induces cohomologically, in all degrees, homomorphisms :

$$H^i(H,A) \to H^i(G,A)$$

This morphism is called the **corestriction morphism** from H to G. It will be denoted **Cores**.

We have an easy, but very important property :

Proposition : The Composition Cores ∘ Res

Let $m = [G : H]$. The composition **Cores** ∘ **Res** is multiplication by m in $H^i(G, \cdot)$.

Proof : It is easy to see it is the case in degree 0*, and so it is everywhere by universality.*

This gives a ton of insight into certain properties of $H^i(G, \cdot)$, that you should attempt as exercises.

Exercise : Consequences of Cores ∘ Res **

Using the former property, prove the following :

1. If G is finite of cardinal m, then the $H^i(G, \cdot)$ are of m-torsion for all $i > 0$.
2. If G is finite and if A is of finite type as a G-module, then the $H^i(G, \cdot)$ are all finite.
3. If A is uniquely divisible as an abelian group, then $H^i(G, \cdot) = 0$ for all $i > 0$.

Solutions : for the first one, apply ***Cores*** ∘ ***Res*** *with* $H = 1$*, noting that* $H^i(1, \cdot)$ *is the zero functor in degree* $i > 0$*. Fr the second one, notice that the* H^i *are of finite type (see description with cochains : the abelian group of functions is of finite type since* G *is finite) and of torsion in degree* > 0*. For the last one, notice that in degree* > 0 *and for all* $n \in \mathbb{N}$*, multiplication by* n *is an isomorphism in* A *so it is an isomorphism in all of the cohomology groups. But they are torsion...*

With little effort, we gained a lot of information on the $H^i(G, A)$. For example, we now know that if A is finite and of order coprime to G, then A is acyclic for G, since the $H^i(G, A)$ is then torsion for two coprime numbers.

3.2.5 The Hoschild-Serre Spectral Sequence

Another easy observation one can make is that $\mathbf{Def}^G_{G/H} \circ \mathbf{Def}_1^{G/H} = \mathbf{Def}_1^G$. We are thus minutes away from the theorem :

Theorem : The Hoschild-Serre Spectral Sequence

Let G be a finite group and H be normal in G. Then for all G-module A, there is a spectral sequence starting on page 2 :

$$H^p(G/H, H^q(H, A)) \implies H^{p+q}(G, A)$$

Proof : This is an immediate application of the Grothendieck composed functors spectral sequence, the only necessary check being that injectives of G***-Mod*** *are sent to acyclic objects of* G/H***-Mod****. It is easily (directly) shown through the definition of an injective module that injectives of* G*-mod are sent to injectives in* G/H*-mod. Another way to prove it is that fixation under* H *has an exact left adjoint, which is the forgetful functor from* G/H***-Mod*** *to* G***-Mod****.*

This will be very useful later on. While the action of G/H on the $H^q(H, A)$ is hardly explicit, we will get interesting annihilation properties if we know for example that the $H^q(H, \cdot)$ or the $H^p(G/H, \cdot)$ vanish after a certain rank.

3.2.6 Exercises

Those are interesting exercises (that will be necessary for what follows), that did not fit into the above text. I recommend that you spend time on them.

Exercise : The Shapiro Isomorphism ***

Prove that there is an isomorphism of δ-functors:

$$H^i(G, \mathbf{Ind}_H^G(A)) \to H^i(H, A)$$

Solution : This is an instance of what I call using the super-horseshoe lemma. Do the following : horseshoe lemma and an exact sequence $0 \to A \to B \to C \to 0$ yields this :

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & I_A & \longrightarrow & I_A \oplus I_C & \longrightarrow & I_C & \longrightarrow & 0 \end{array}$$

Now apply $\boldsymbol{Ind}_H^G$, which is exact, additive and preserves injectives.

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & \mathbf{Ind}_H^G(A) & \longrightarrow & \mathbf{Ind}_H^G(B) & \longrightarrow & \mathbf{Ind}_H^G(C) & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & \mathbf{Ind}_H^G(I_A) & \longrightarrow & \mathbf{Ind}_H^G(I_A) \oplus \mathbf{Ind}_H^G(I_C) & \longrightarrow & \mathbf{Ind}_H^G(I_C) & \longrightarrow & 0 \end{array}$$

Now observe that fixating the first under H and the second one under G yields isomorphic diagrams, where an isomorphism is given by evaluating the second one at 1. Then finish up with naturality of the snake lemma to obtain the isomorphisms.

Exercise : An Alternative Description of Corestriction ***

Let A be a G-module. Consider the morphism $\pi : \mathbf{Ind}_H^G \to A$ given by :

$$f \mapsto \sum_{g \in G/H} g \cdot f(g^{-1})$$

1. Prove that π, in cohomology, yields a natural transformation $H^i(G, I_G^H(\cdot)) \to H^i(G, \cdot)$.
2. Prove that the composition of π^* and the Shapiro isomorphism is the same as the corestriction morphism.

Solution : the first one is just a verification, seeing that π is naturally defined independently of the object A. Precomposing with the Shapiro isomorphism yields a natural transformation $H^i(H, A) \to H^i(G, A)$. Now note that this side of the Shapiro isomorphism has, in degree 0, the morphism from $A^H \to (I_G^H(A))^G$ that sends to a the constant function equal to a. Now clearly this is the same as corestriction so by universality it is the same everywhere.

Exercise : Invariance of Cohomology by Conjugation ***

Let A be a G-module. One has a functor $c_t : \mathbf{Mod}_G \to \mathbf{Mod}_G$ that changes the action of G on A by conjugation : the sets and the morphisms are the same, however, the action of G is now $g \cdot_{c_t} a = tgt^{-1}a$. Prove that changing the action of G does not change the cohomology functor, or in other words, $H^i(G, c_t\_) = H^i(G, \_)$.

Solution : Note that c_t is exact and preserves injectives - which is immediate from the fact that c_t is an automorphism of category of $\mathbf{Mod}_G$, of inverse $c_{t^{-1}}$. Now use super-horseshoe lemma, noticing that $\mathbf{Def}_1^G \circ c_t = \mathbf{Def}_1^G$.

3.3 Modified Cohomology Groups

We now define a refined version of cohomology groups, which are **modified cohomology groups**. They consist in a slight twitch in the definition of cohomology groups, that allow us to formulate new theorems.

3.3.1 Group Homology

In the first section, we introduced group cohomology. Group homology isn't any more difficult to introduce : as expected, it will consist in the left derived functor of a certain right exact functor.

Let G be a finite group. Denote I_G the kernel of the ring morphism $\mathbb{Z}[G] \to \mathbb{Z}, \sum n_g g \mapsto \sum n_g$. It is also the linear combinations of elements of the form $(g-1)$. Now since for any morphism $f : A \to B$, $f(I_G A) = I_G f(A)$, then any such morphism induces a morphism $\tilde{f} : A/I_G A \to B/I_G B$ by quotient. We can check that the functor $A \mapsto A/I_G A$ is right exact : indeed, consider the exact sequence...

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

Then since the arrow $g : B \to C$ is surjective, its composite with the projection $C \to C/I_G C$ is still surjective and thus the quotient $\tilde{g}$ of this map too. Moreover, if $\tilde{g}(x) = 0$, then $g(x) \in I_G C$, so $g(x) = (\sum n_g g)y$. Take a reciprocal image z of y by g, find $x - (\sum n_g g)z \in \mathbf{ker}\ g$. So it is in the image of the morphism before, but then quotienting proves that the class of x is in the image of the morphism before.

One can thus construct its derived functors !

Definition : Group Homology

The functor $A \mapsto A/I_G A$, and sends maps to their right quotients, is right exact and covariant. Its left derived functors are denoted $H_i(G, \cdot)$.

Group homology, in itself, does not have many notable applications in our prospect. However, it can be "attached" to cohomology to construct a longer functor, through a lemma that we will develop in the following section.

3.3.2 Homological Gluing Lemma, and Modified Cohomology Groups

The homological gluing lemma can be stated as follows :

Theorem : Homological Gluing Lemma

Let F and G be covariant left and right exact functors. Denote $R^i F$ and $L_i G$ for $i \geq 0$ denote their right and left derived functors. A natural transformation from $u : G \to F$ yields a δ-functor $(C^n)_{n\in\mathbb{Z}}$, with $C^n = R^n F$ for all $n \geq 1$, $C^0 = \mathbf{coker}\ (u_A : G(A) \to F(A))$, $C^{-1} = \mathbf{ker}\ (u_A : G(A) \to F(A))$ and $C^n = L_{-n-1} G$ for $n \leq -2$.

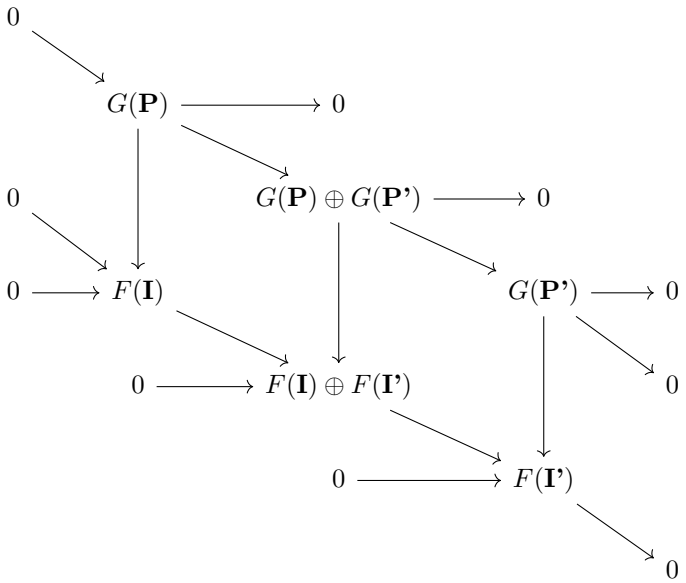
Proof : this is a beautiful homological algebra proof, but which may take a while to digest for a first read.

We will start with an exact sequence $0 \to A \to B \to C \to 0$ and construct the gluing of the two functors. What we will do is start from the construction of derived functors through the horseshoe lemma. It starts by taking injective and projective resolutions of the sequence, and applying F and G. This yields two diagrams :

$$\begin{array}{ccccc}
 & & 0 & & \\
 & & \downarrow & & \\
 & & G(\mathbf{P}) & \longrightarrow & G(A) \longrightarrow 0 \\
 & & \downarrow & & \downarrow \\
G(\mathbf{P}) \oplus G(\mathbf{P'}) & \longrightarrow & G(B) & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \\
G(\mathbf{P'}) & \longrightarrow & G(C) & \longrightarrow & 0 \\
\downarrow & & & & \\
0 & & & &
\end{array}$$

$$\begin{array}{ccccc}
 & & 0 & & \\
 & & \downarrow & & \\
0 \longrightarrow & F(A) & \longrightarrow & F(\mathbf{I}) & \\
 & \downarrow & & \downarrow & \\
0 \longrightarrow & F(B) & \longrightarrow & F(\mathbf{I}) \oplus F(\mathbf{I'}) & \\
 & \downarrow & & \downarrow & \\
0 \longrightarrow & F(C) & \longrightarrow & F(\mathbf{I'}) & \\
 & & & \downarrow & \\
 & & & 0 &
\end{array}$$

Those two diagrams can now be joined through the natural transformation from $G \to F$.



... where the vertical arrows are the composition $G(\boldsymbol{P}_0) \to G(A) \to F(A) \to F(\boldsymbol{I}_0)$.

What we now have is a morphism between exact sequences of complexes, where the first complex is the upper one, with the $G(\boldsymbol{P})$ and the lower one is the one with the $F(\boldsymbol{I})$. Now, use the snake lemma simultaneously on both the upper and the lower complex. Naturality induces a morphism between the two long exact associated to them, which looks like this at the joining point :

$$\begin{array}{ccccccccccc} \dots & \longrightarrow & L_1G(C) & \longrightarrow & G(A) & \longrightarrow & G(B) & \longrightarrow & G(C) & \longrightarrow & 0 & \longrightarrow & \dots \\ & & \downarrow & & \downarrow{\scriptstyle u_A} & & \downarrow{\scriptstyle u_B} & & \downarrow{\scriptstyle u_C} & & \downarrow & & \\ \dots & \longrightarrow & 0 & \longrightarrow & F(A) & \longrightarrow & F(B) & \longrightarrow & F(C) & \longrightarrow & R^1F(A) & \longrightarrow & \dots \end{array}$$

This part of the diagram is precisely where you can use the easy version of the snake lemma once again, to get an exact sequence :

$$\textbf{ker } u_A \longrightarrow \textbf{ker } u_B \longrightarrow \textbf{ker } u_C \longrightarrow \textbf{coker } u_A \longrightarrow \textbf{coker } u_B \longrightarrow \textbf{coker } u_C$$

By the commutativity of the middle diagram, this sequence can be extended by plugging in the morphism $L_1G(C) \to \textbf{ker } u_A$ on the left and $\textbf{coker } u_C \to R^1F(A)$ (factorization of $[F(C) \to R^1F(A)]$) on the right. One now has to check that the obtained sequence is exact at the joining points, but this is immediate by exactness of the lines :

$$L_1G(C) \to G(A) \to G(B)$$

$$F(B) \to F(C) \to R^1F(A)$$

Naturality is obtained by seeing that every single step we took here was natural (I will not fully prove it for it would get us into an absolute mess).

The action on morphisms is obviously defined as action of derived functors where it should be, restriction to kernel in degree -1 and quotienting between cokernels in degree 0.

So now that we have those tools, all we need to gather is a natural transformation from homology to cohomology. Thankfully, one is easily obtained by defining $N_A : A/I_GA \to A^G$, $[x] \mapsto \sum_{g\in G} g \cdot x$. One can easily check that it is well defined, and that it is absolutely a natural transformation.

Definition : Modified Cohomology Groups of G

The modified cohomology functor associated to the finite group G, and denoted $\hat{H}^n(G,\cdot)_{n\in\mathbb{Z}}$ is the δ-functor obtained by gluing the homology and the cohomology functors according to the norm natural transformation.

To be a little more explicit, whenever we have an exact sequence $0 \to A \to B \to C \to 0$, we now have a double sided long cohomology sequence $\hat{H}^n(G,\cdot)_{n\in\mathbb{Z}}$ where

- $\hat{H}^n(G,A) = H^n(G,A)$ for all $n \geq 1$.
- $\hat{H}^0(G,A) = \textbf{coker } (N_A : A/I_GA \to A^G) = A^G/N_AA$.
- $\hat{H}^{-1}(G,A) = \textbf{ker } (N_A : A/I_GA \to A^G)$.
- $\hat{H}^n(G,A) = H_{-n-1}(G,A)$ for $n \leq -2$.

3.3.3 Explicit Description

This new cohomology also has a description with functions, but we will not introduce it because it is not necessary for our current endeavours. One may find it in [1], page 42.

3.3.4 Acyclicity Properties of $\hat{H}^n$

In this section, we describe what objects are acyclic under modified cohomology. The first ones, thankfully, are the induced G-modules.

Proposition : Acyclic Objects for Modified Cohomology

Let $\mathbf{Ind}_1^G(X)$ be an induced G-module. Then $\hat{H}^n(\mathbf{Ind}_1^G(X)) = 0$ for all $n \in \mathbb{Z}$.

Proof : We already know it is true in degrees $n \geq 1$.

In degree 0, notice that G-invariant points of $\boldsymbol{Ind}_1^G(X)$ are constant maps, with the constant map equal to a being the norm of the map which is 0 everywhere and 1 on one unique value of G. So the quotient is 0.

In degree -1, notice that an element of $\boldsymbol{Ind}_1^G(X)$ of norm 0 verifies $\sum_{g\in G} f(g) = 0$. Since $I_G\boldsymbol{Ind}_1^G(X)$ contains all functions of the form $f(\cdot g) - f$, chosing well f yields functions such that $f(g) = u, f(g') = -u$ and that vanish everywhere else. Now all functions of norm 0 can be obtained through the right sum.

In degree $n \leq -2$, it is a little trickier. Notice first that $\boldsymbol{Ind}_1^G(X) \simeq \mathbb{Z}[G] \otimes_{\mathbb{Z}} X$ (by mapping $f \to \sum_{g\in G} g \otimes f(g^{-1}x)$). Then notice that if $\boldsymbol{P} \to X \to 0$ is a projective resolution of X, then $\boldsymbol{P} \otimes \mathbb{Z}[G] \to X \otimes \mathbb{Z}[G] \to 0$ is still a projective resolution of $X \otimes \mathbb{Z}[G]$ (the tensor product is done on $\mathbb{Z}$) : $\mathbb{Z}[G]$ is free so flat so exactness is conserved, and projectiveness too since $\boldsymbol{Hom}(P \otimes \mathbb{Z}[G], B) \simeq \boldsymbol{Hom}(P, \boldsymbol{Hom}(\mathbb{Z}[G], B))$ which is exact as a composition of exact functors). Now notice that $A \otimes \mathbb{Z}[G]/(I_G A \otimes \mathbb{Z}[G]) = A \otimes \mathbb{Z}[G]/I_G \simeq A \otimes \mathbb{Z} \simeq A$, since $\mathbb{Z}[G] \to \mathbb{Z}$ has kernel I_G. So the homology is trivial.

Projective and injective G-modules don't fare better under modified cohomology.

Proposition : Projective and Injectives under $\hat{H}^n$

For a finite group G and for all projective or injective G-module M, $\hat{H}^n(M) = 0$ for all $n \in \mathbb{Z}$.

Proof : in the category of G-modules, we have proven that any G-module M can be injected into an induced module. If M is injective, then it is a direct factor of an induced module and its modified cohomology is thus 0 by the fact the same property for induced modules. If M is projective, M is a direct factor of a free G-module L. However, a free G-module is isomorphic to $\mathbb{Z}[G] \otimes_{\mathbb{Z}} X$ where X is the free abelian group on a basis of L as a G-module. Since G is finite, this is isomorphic to $I_G(X)$, which has zero cohomology in modified groups.

Thus, the same inductions we could make in cohomology we can still make in modified cohomology.

3.3.5 Restriction-Corestriction

The previous result allows us to use a homological algebra theorem stating that if $(F_n)_{n\in\mathbb{Z}}$ and $(G_n)_{n\in\mathbb{Z}}$ are δ-functors such that F kills injectives and G kills projectives, any natural transformation $F_0 \to G_0$ extends uniquely to a morphism of δ-functors between the two (this is an exercise in the **Homological Algebra** chapter of this article). This is what will allow us to theoretically define restriction and corestriction in modified cohomology groups.

Definition : Corestriction and Restriction in modified Cohomology

The natural transformation $A^G/N_G A \to A^H/N_H A$ induced by inclusion induces a natural transformation in all degrees from $\hat{H}(G,\cdot)$ to $\hat{H}(H,\cdot)$. This natural transformation is called **restriction** and is denoted **Res**.

The natural transformation $A^H/N_H A \to A^G/N_G A$ induced by the map $a \mapsto \sum_{g\in G/H} g\cdot a$ is a natural transformation from $\hat{H}^0(H,\cdot)$ to $\hat{H}^0(G,\cdot)$ which induces a natural transfomration of δ-functors from $\hat{H}(G,\cdot)$ to $\hat{H}(H,\cdot)$. This natural transformation is called **corestriction** and is denoted **Cores**.

We leave it to you to prove the following proposition, which is analogous to the non-modified case (*do an induction for the third proof*) :

Proposition : Composition Cores $\circ$ Res and its Consequences

- **Cores** $\circ$ **Res** is multiplication by $[G:H]$ in all degrees.
- $\hat{H}^n(G,A)$ is killed by the order of G.
- If A is of finite type, then all the groups $\hat{H}^n(G,A)$ are finite.

Restriction and corestriction have explicit descriptions in low degrees, that you may find in the reference [1] around page 50.

3.3.6 Cohomology of Cyclic Groups

A beautiful application of modified cohomology is to be able to obtain for few efforts the cohomology of cyclic groups. We prove the following theorem :

Theorem : Cohomology of Cyclic Groups

Let $n \in \mathbb{N}$, $n \geq 1$, and let A be a G-module. Then for all $i \in \mathbb{Z}$, we have isomorphisms :

$$\hat{H}^i(\mathbb{Z}/n, A) \simeq \hat{H}^{i+2}(\mathbb{Z}/n, A)$$

The proof is given underneath as an exercise.

Exercise : Cohomology of Finite Cyclic Groups **

In this exercise, we compute the modified cohomology in all degrees of a cyclic group G of order n, for any G-module A.

1. Let s be a generator of G. Denote $N = \sum_{t\in G} t$ and $D = s-1 \in \mathbb{Z}[G]$. Check that $I_G = (D)$.
2. Let $K(A)$ be the complex which is A in all degrees and where d^i is multiplication by N if i is odd and by D if i is even. Check that :
   (a) $K(A)$ is indeed a complex.
   (b) $A \mapsto K(A)$ can be extended to an exact functor.
   (c) The functors $(H^n(K(\cdot)))_{n\in\mathbb{Z}}$ assemble into a δ-functor.
   (d) For any exact sequence $0 \to A \to B \to C \to 0$, the sequences :

$$\hat{H}^{-1}(G,A) \to \hat{H}^{-1}(G,B) \to \hat{H}^{-1}(G,C) \to \hat{H}^0(G,A) \to \hat{H}^0(G,B) \to \hat{H}^0(G,C)$$

   and :

$$H^{-1}(K(A)) \to H^{-1}(K(B)) \to H^{-1}(K(C)) \to H^0(K(A)) \to H^0(K(B)) \to H^0(K(C))$$

   are isomorphic.
3. Prove that $(H^n(K(\cdot)))_{n\in\mathbb{Z}}$ vanishes on injectives and on projectives.
4. Conclude that the functors $(H^n(K(\cdot)))_{n\in\mathbb{Z}}$ and $(\hat{H}^n(G,\cdot))_{n\in\mathbb{Z}}$ are isomorphic.
5. Prove that the modified cohomology of a cyclic group is 2-periodic, thus determined by the groups $A^G/N_A A$ and **ker** $N_A : A/I_G A \to A^G$.

Solution : Question 1 and 2.a, 2.b, 2.c are immediate. The first slightly tricky part is 2.d. This simply comes from the fact that there are natural isomorphisms between the $\hat{H}^i$ and $H^i(K(\cdot))$ in degree -1 and 0, and naturality of the snake lemma construction that permited the arising of this sequence yields total commutativity. For 3, use 2-periodicity and this fact on $\hat{H}^n$. For 4, apply the cool theorem on long δ-functors which vanish on injectives and projectives. Then conclude.

One new computation, which will reveal itself more important than it seems, is now available to us.

Exercise : The Brauer Group of $\mathbb{R}$ **

Using the exercise above, compute $H^2(\mathbf{Gal}(\mathbb{C}/\mathbb{R}, \mathbb{C}^*))$, seeing $\mathbb{C}^*$ as a $\mathbf{Gal}(\mathbb{C}/\mathbb{R})$ module.

Solution : $Gal(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$ is cyclic, so one can use the latter theorem. We know it is isomorphic to ${\mathbb{C}^*}^G/N(\mathbb{C}^*)$. Now $N(\mathbb{C}^*)$ are the elements of the form $\prod z\overline{z}$ and ${\mathbb{C}^*}^G$ is just $\mathbb{R}^*$. So the result is $\mathbb{R}^*/\mathbb{R}_{+^*} \simeq \mathbb{Z}/2\mathbb{Z}$. This group is called the Brauer group of $\mathbb{R}$.

3.3.7 Exercises

Exercise : Computation of $\hat{H}^{-2}(G,\mathbb{Z})$ ***

Let G be a finite group. In this exercise we will compute $\hat{H}^{-2}(G,\mathbb{Z}) = \hat{H}_1(G,\mathbb{Z})$.

1. Use the exact sequence $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$, where the arrow $\mathbb{Z}[G] \to \mathbb{Z}$ is the norm, to prove that $\hat{H}_1(G,\mathbb{Z}) \simeq I_G/I_G^2$.
2. Prove that $G \to I_G/I_G^2, g \mapsto g-1$ is a group morphism.
3. Prove that it induces an isomorphism between $G^{\mathbf{ab}}$ and I_G/I_G^2.
4. Note that this isomorphism is natural.

Solution : Since $\mathbb{Z}[G]$ is free, its homology groups for $n \geq 1$ are trivial. You thus have an exact sequence $0 \to H^1(G,\mathbb{Z}) \to H^0(G,I_G) \to H^0(G,\mathbb{Z}[G])$. Now notice that the third arrow is induced by the inclusion $I_G \hookrightarrow \mathbb{Z}[G]$, which by definition becomes the zero arrow in homology. So we have the isomorphism. The fact that it is a morphism is checked easily through the equality $gh-1 = (g-1)+(h-1)+(g-1)(h-1)$. Now since I_G/I_G^2 is abelian this induces a group morphism from $G^{\mathbf{ab}} \to I_G/I_G^2$. To prove it is an isomorphism we will construct an inverse morphism : from $I_G \to G^{\mathbf{ab}}$, define $\overline{g-1} \mapsto \overline{g}$ (this is well defined because it is simply a morphism from a free abelian group to another abelian group, defined by the image of a base). This morphism induces a morphism $I_G/I_G^2 \to G^{\mathbf{ab}}$ because of the equality $(g-1)(h-1) = gh-1-(g-1)-(h-1)$, which proves that $(g-1)(h-1)$ is sent to a commutator element. Naturality is a mental exercise.

In the following exercises, we study a notion called the Herbrand Quotient, linked to finite cohomology groups of a cyclic group (which will prove useful later on when reaching class field theory).

Definition : Herbrand Quotient

Let G be a cyclic group and let A be a G-module such that $\hat{H}^0(G,A)$ and $\hat{H}^1(G,A)$ are finite. The **Herbrand Quotient** of A is defined as $h(A) = |\hat{H}^0(G,A)|/|\hat{H}^1(G,A)|$.

Exercise : Herbrand Quotient and Exact Sequences ***

Let $0 \to A \to B \to C \to 0$ be an exact sequence. Prove that if two of the three Herbrand Quotients are defined, prove that the third one is too and that we have $h(B) = h(A)h(C)$.

Solution : Use long cohomology sequence, and the fact that if X and Y are finite and that we have an exact sequence : $X \to K \to Y$ then K is finite too by isomorphism theorem. Then deduce from this an exact sequence $0 \to I \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \to H^1(G,A) \to H^1(G,B) \to H^1(G,C) \to I \to 0$, and thus product of alternate cardinals is 1.

Exercise : Herbrand Quotient of Finite G-modules ***

We want to prove that if A is finite, then $h(A) = 1$.

1. Let s be a generator of G. Prove that we have an exact sequence :

$$0 \to H^0(G, A) \to A \xrightarrow{s-1} A \to H_0(G, A) \to 0$$

2. Let $N = \sum_{g \in G} g \in \mathbb{Z}[G]$. Prove that we have an exact sequence :

$$0 \to \hat{H}^{-1}(G, A) \to H_0(G, A) \xrightarrow{N} H^0(G, A) \to \hat{H}^0(G, A) \to 0$$

3. Conclude.

Solution : the two exact sequences are obvious from the definitions. The first one, exactness is obtained because by cyclicity $x \in A^G \iff (s-1)x = 0$ and because multiplication by s yields $I_G A$ since $s - 1$ generates I_G. For the second one, not more difficult. Then use alternated products of cardinals.

Exercise : Herbrand Quotients and Morphisms **

Let $f : A \to B$ a G-homomorphism with finite kernel and cokernel. Prove that if one of the Herbrand quotients is defined the other one is, and $h(A) = h(B)$.

Solution : the two-out-of-three property is obvious by splitting $0 \to \textbf{\textit{Ker}}\ f \to A \to \textbf{\textit{Im}}\ f \to 0$ and $0 \to \textbf{\textit{Im}}\ f \to B \to \textbf{\textit{Coker}}\ f \to 0$. Everything is obvious from here (use the two last exercises).

Exercise : Restriction, Corestriction and Linear Maps ***

Let A and B be G-modules, and $H \subset G$ a subgroup. A G-linear map $f : A \to B$ functorially induces linear maps between the $\hat{H}^i(G, A) \to \hat{H}^i(G, B)$, as well as $\hat{H}^i(H, A) \to \hat{H}^i(H, B)$. Prove that **Res** and **Cores** commute with f.

Solution : commutativity is clear in degree 0. We will then prove it by induction. For this we use the canonical inclusion $A \to I_G(A)$, $a \mapsto [g \mapsto g \cdot a]$. A linear map $f : A \to B$ induces a commutative diagram :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & I_G(A) & \longrightarrow & A_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle \tilde{f}_*} & & \\ 0 & \longrightarrow & B & \longrightarrow & I_G(B) & \longrightarrow & B_1 & \longrightarrow & 0 \end{array}$$

The acyclicity of the $I_G(A)$ allow us to prove it in all positive degrees by induction. For decreasing degrees, the proof is the same bu using this time the canonical projection $I_G(A) \to A$, $f \mapsto \sum_{g \in G} g \cdot f(g^{-1})$, and noticing that the same kind of diagram arises.

3.4 Cup-Products and Tate-Nakayama

In this section we study **cup-products**, operations in cohomology induced by bilinear coupling : a $\mathbb{Z}$-bilinear map such that $g \cdot \phi(a, b) = \phi(g \cdot a, g \cdot b)$.

Let A, B and C be three G-modules, and let $\phi : A \times B \to C$ be a bilinear coupling.

ϕ induces a bilinear coupling $K^p(G,A) \times K^q(G,B) \xrightarrow{\cup_\phi} K^{p+q}(G,C)$ (this time the K^p are homogeneous cochains), by defining :

$$(f,g) \mapsto [f \cup_\phi g : g_0, ..., g_{p+q} \mapsto \phi(f(g_0, ..., g_p), g(g_p, ..., g_{p+q}))]$$

Note that for this to work, ϕ cannot be a $\mathbb{Z}[G]$-bilinear map (else the image of a, b would not be a homogeneous cochain).

Proposition : $\cup$ and Differentials

For all $(a,b) \in K^p(G,A) \times K^q(G,B)$, we have $d(a \cup_\phi b) = (da) \cup_\phi b + (-1)^p (a \cup_\phi db)$.

Proof : a computation.

Definition : The Cup-Product in Cohomology

The map $f, g \mapsto f \cup_\phi g$ induces a bilinear map in cohomology :

$$H^p(G,A) \times H^q(G,B) \xrightarrow{\cup_\phi} H^{p+q}(G,C)$$

Verification : the formula above tells us that elements of $\boldsymbol{Ker}\ d_A \times \boldsymbol{Ker}\ d_B$ *are sent to elements of* $\boldsymbol{Ker}\ d_C$*. It also tells us that* $\boldsymbol{Im}\ d_A \times \boldsymbol{Ker}\ d_B$ *is sent to an element of* $\boldsymbol{Im}\ d_C$ *(and identically if you switch A and B). So the induction of the maps works by factoring through each component (check with the adjunction property of bilinear maps).*

The next proposition is a useful one, saying that all of the cup-products are induced by the cup-product associated to the tensor product (we write $A \otimes B$ for $A \otimes_{\mathbb{Z}} B$). $A \otimes_{\mathbb{Z}} B$ is given a structure of G-module by defining $g \cdot (a \otimes b) = g \cdot a \otimes g \cdot b$ (this is done so that the map $\otimes_{\mathbb{Z}}$ is a coupling).

Proposition : Cup Products are Induced by the Tensor Product

Let A, B, C be three G-modules, and $\phi : A \times B \to C$ be a bilinear coupling. ϕ induces a linear map $\tilde{\phi} : A \otimes B \to C$. Then the two compositions :

$$H^p(G,A) \times H^q(G,B) \xrightarrow{\cup_\phi} H^{p+q}(G,C)$$

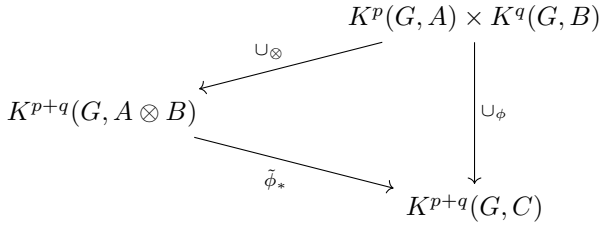
... and :

$$H^p(G,A) \times H^q(G,B) \xrightarrow{\cup_\otimes} H^{p+q}(G, A \otimes B) \xrightarrow{\tilde{\phi}_*} H^{p+q}(G,C)$$

... are the same.

This will be useful, because a lot of computations about cup-products can now be made on just the tensor product and extended by linearity to all bilinear couplings.

Proof : simple observation from the following commutative diagram, that you can push to cohomology.



Exercise : Description of the cup-product in low degrees **

Describe explicitly the cup product in the cases were $p = q = 0$ and when just $p = 0$ or $q = 0$.

Solution : In degree 0, it is simply the map $A^G \times B^G \to C^G, a, b \mapsto \phi(a, b)$. When p is zero, for $x \in K^0(G, A) \simeq A^G$ and $f \in K^q(G, B)$, you obtain the map $G \to C$, $(g_0, ..., g_q) \mapsto \phi(x, f(g_0, ..., g_q))$.

Proposition : Cup Products and Long Cohomology Sequences

Let $0 \to A' \to A \to A'' \to 0$ and $0 \to C' \to C \to C'' \to 0$ short exact sequences of G-modules. Let ϕ be a bilinear map $A \times B \to C$ such that $\phi(A' \times B) \subset C'$.

- ϕ induces bilinear maps $\phi' : A' \times B \to C'$ and $\phi'' : A'' \times B \to C''$, and thus three cup products $(\cup_{\phi'}, \cup_\phi, \cup_{\phi''})$ from $H^p(G, A^{(n)}) \times H^q(G, B) \xrightarrow{\cup} H^{p+q}(G, C^{(n)})$ where $n = 0, 1, 2$.
- The linking homomorphisms of the long cohomology sequence associated to $0 \to A' \to A \to A'' \to 0$ are linked to that of the $0 \to C' \to C \to C'' \to 0$ exact sequence by the following formula : for all $b \in H^q(G, B), a \in H^p(G, A'')$...

$$(\delta a) \cup_{\phi'} b = \delta(a \cup_{\phi''} b) \in H^{p+q+1}(G, C')$$

Let $0 \to B' \to B \to B'' \to 0$ and $0 \to C' \to C \to C'' \to 0$ short exact sequences of G-modules. Let ϕ be a bilinear map $A \times B \to C$ such that $\phi(A \times B') \subset C'$.

- ϕ induces bilinear maps $A \times B' \to C'$ and $A \times B'' \to C''$, and thus three cup products $(\cup_{\phi'}, \cup_\phi, \cup_{\phi''})$ from $H^p(G, A) \times H^q(G, B^{(n)}) \xrightarrow{\cup} H^{p+q}(G, C^{(n)})$ where $n = 0, 1, 2$.
- The linking homomorphisms of the long cohomology sequence associated to $0 \to B' \to B \to B'' \to 0$ are linked to that of the $0 \to C' \to C \to C'' \to 0$ exact sequence by the following formula : for all $a \in H^p(G, A), b \in H^q(G, B'')$...

$$a \cup_{\phi'} \delta(b) = (-1)^p \delta(a \cup_{\phi''} b) \in H^{p+q+1}(G, C')$$

This proof is long but is a great exercise to make sure you understood how the cup product works. Let's prove the first one.

A first lemma is that for all q, the functor $A \mapsto K^q(G, A)$ is exact. Indeed, it is of the form $\boldsymbol{Hom}_G(\mathbb{Z}[G^{q+1}], A)$, and $\mathbb{Z}[G^{q+1}]$ is clearly free so projective.

Take a^* a representent of $a \in K^p(G, A'')$ and a^{**} a pre-image of $a^* \in K^p(G, A)$, which is possible by exactness. Applying d gives you $d(a^{**}) \in K^{p+1}(G, A') \subset K^{p+1}(G, A)$. Notice that we reproduced the construction in the snake lemma, so the class of $d(a^{**})$ in $H^{p+1}(G, A')$ is δa.

Now remember that $(\delta a) \cup_{\phi'} b$ is the projection on $H^{p+q+1}(G, C')$ of $(\delta a)^* \cup_\phi b^* \in K^{p+q+1}(G, C')$, where $(\delta a)^*$ and b^* are representants of δa and b. So $(\delta a) \cup_{\phi'} b$ is the projection of $d(a^{**}) \cup_{\phi'} b^*$ where b^* is any representant of b.

Now, using the formula of last page, we now that $d(a^{**}) \cup_{\phi'} b^* = d(a^{**}) \cup_{\phi'} b^* = d(a^{**}) \cup_\phi b^* = d(a^{**} \cup_\phi b^*) - (-1)^p(a^{**} \cup_\phi db^*) = d(a^{**} \cup_\phi b^*)$.

The only last check to make is that $d(a^{**} \cup_\phi b^*)$ is projected as $\delta(a \cup_{\phi''} b)$. We will proceed like we did above : $a \cup_{\phi''} b$ is nothing but the projection of $a^* \cup_{\phi''} b^*$. By definition of ϕ'', this can be pulled back to an element of $K^{p+q}(G, C)$ as $a^{**} \cup_\phi b^*$. By the same argument as earlier, the projection of $d(a^{**} \cup_\phi b^*)$ on $H^{p+q+1}(G, C')$ is $\delta(a \cup_{\phi''} b)$. This finishes this verification. The second case is identical.

To make sure the methods of this proof are clear, here is another exercise in the same style.

Exercise : Another Coupling Theorem ***

Let $0 \to A' \to A \to A'' \to 0$ and $0 \to B' \to B \to B'' \to 0$ be two exact sequences, and let ϕ be a bilinear coupling $A \times B \to C$ such that $\phi(A' \times B') = 0$. Similarly as above, ϕ induces couplings $\phi' : A' \times B'' \to C$ and $\phi'' : A'' \times B' \to C$. Prove that the induced cup-products

$$\cup_{\phi'} : H^p(G, A') \times H^q(G, B'') \to H^{p+q}(G, C)$$

and...

$$\cup_{\phi''} : H^p(G, A'') \times H^q(G, B') \to H^{p+q}(G, C)$$

verify the following long exact sequences compatibility property :

$$(\delta a) \cup_{\phi'} b = (-1)^p a \cup_{\phi''} \delta(b)$$

Solution (sketchy) : We still have the fact that there is an element a^* such that δa is represented by da^*. Now $(\delta a) \cup_{\phi'} b$ is nothing but the projection of $\phi(da^*, b^*)$, which in turn is $d(\phi(a^*, b^*)) + (-1)^p \phi(a^*, db^*)$ which concludes once you push this down to cohomology.

Here's something we will admit for the rest of the section (it would be a lot of unnecessarily tedious work to define).

Definition : Cup-Products in Modified Cohomology

For all bilinear couplings $\phi : A \times B \to C$, and $p, q \in \mathbb{Z}$ there is a bilinear map :

$$\hat{H}^p(G, A) \times \hat{H}^q(G, B) \xrightarrow{\cup_\phi} \hat{H}^{p+q}(G, C)$$

... which is induced by $\phi : A^G \times B^G \to C^G$ in degree 0 and follows the same commutativity property relative to long exact sequences. It is the **cup-product in modified cohomology**.

3.4.1 Some Computations with the Cup-Product

Doing computations with the cup product is not so easy. Most of the time, they are done by induction, using the property above, writing elements as δ of others element, and trying to say things about this δ. Many examples will be treated in the following section, all as exercises.

Exercise : $a \cup b$ and $b \cup a$ ***

Let ϕ be a bilinear coupling $A \times B \to C$ and $\phi_s : B \times A \to C$ the same map with reversed inputs. We will prove that in all degrees $p, q \in \mathbb{Z}$, $a \cup_\phi b = (-1)^{pq}(b \cup_{\phi_s} a)$.

1. Check that it is true in degree 0.
2. Prove by induction that it is true in all degrees, using the existence of the following split exact sequences (over $\mathbb{Z}$) :

$$0 \to A \hookrightarrow I_G(A) \to A_1 \to 0$$
$$0 \to A^{-1} \hookrightarrow I_G(A) \to A \to 0$$

... as well as the fact that those sequences stay split when tensorized, and finally the commutativity facts about long cohomology sequences.

Solution : We will prove it for the tensor product only (the other properties come from there). It is true for $p = q = 0$, by identification of $A \otimes B$ and $B \otimes A$. Let's prove it for $p = 1$ and $q = 0$. We will use the exact sequences $0 \to A \hookrightarrow I_G(A) \to A_1 \to 0$ and $0 \to A \otimes B \hookrightarrow I_G(A) \otimes B \to A_1 \otimes B \to 0$. Since $I_G(A)$ has modified cohomology 0, the δ are isomorphisms in the long exact sequence associated to the first one. We thus have $a \cup b = \delta(a^*) \cup b$ for some $a^* \in H^0(K, A_1)$. But this is also $\delta(a^* \cup b) = \delta(b \cup a^*) = (-1)^0 b \cup \delta(a^*) = b \cup a$. We leave it to the reader to continue the induction: it shouldn't be too hard from there. Also, since multiplication by (-1) commutes with a linear map, there is no problem from going from the tensor product to an arbitrary bilinear coupling.

Exercise : Restriction, Corestriction and the Cup-Product ***

1. In a similar fashion, prove that $\mathbf{Res}(\alpha) \cup_\phi \mathbf{Res}(\beta) = \mathbf{Res}(\alpha \cup_\phi \beta)$.
2. Still in a similar way, prove that we have $\mathbf{Cores}(\alpha \cup_\phi \mathbf{Res}(\beta)) = \mathbf{Cores}(\alpha) \cup_\phi \beta$ (for $\alpha \in \hat{H}^p(H, A)$ and $\beta \in \hat{H}^q(G, B)$).

Solution : For the first question, we prove it first with the tensor product. It is obvious in degree 0 since restriction is explicitly described in terms of elements of K^0 and clearly commutes with the tensor product. Then it also uses the fact that restriction is a morphism of δ-functors, so it commutes with the δs. Then it is an induction. Then we prove it for arbitrary couplings : we use the fact that restriction commutes with linear maps (which is an exercise above).

For the second question, once again, all it takes is a proof in degree 0, which is very direct : the restriction of an element fixed by G does not care about the corestriction.

To finish this section, we will expose a few computations in low degree.

Exercise : Explicit Computations in degree $(1, -1)$ and $(1, -2)$ ***

1. For any $f \in Z^1(G, B)$ and $a \in \mathbf{Ker}\ N$, we have $\overline{f} \cup \overline{a} = -\overline{\sum_{t \in G} (t \cdot a) \otimes f(t)}$.
2. Recall that $\hat{H}^{-2}(G, \mathbb{Z})$ is naturally isomorphic to $G^{\mathbf{ab}}$. Then, we have $\overline{s \cup f} = \overline{f(s)}$.

Solution : not proven here. Long and not especially relevant.

3.4.2 Statement of the Tate-Nakayama Theorem

The Tate-Nakayama theorem is a very precise theorem about certain isomorphisms one can obtain between cohomology at $\mathbb{Z}$ and cohomology at other modules. We will not prove it, for its proof is long and very complicated. One can find a complete proof in [1] in the dedicated chapter.

Theorem : Tate-Nakayama Theorem

Let A be a G-module, and $a \in H^2(G, A)$. Suppose that for all prime number p :

- $H^1(G_p, A) = 0$.
- $H^2(G_p, A)$ is the same order as G_p and is cyclic, generated by $\mathbf{Res}(a)$.

Then for any torsion-free module D and $H \subset G$, the cup-product by $\mathbf{Res}_H(a) \in H^2(H, A)$ induces isomorphisms :

$$\hat{H}^n(H, D) \to \hat{H}^{n+2}(H, A \otimes D)$$

...for all $n \in \mathbb{Z}$. In particular, we have isomorphisms :

$$\hat{H}^n(H, \mathbb{Z}) \to \hat{H}^{n+2}(H, A)$$

By "the cup product by $x \in H^m(H, A)$", one means the map induced by $K^n(H, A) \to K^{n+m}(H, A \otimes D)$, $u \mapsto u \cup_\phi x \in K^{n+m}(H, A \otimes D)$.

3.5 Comological Triviality

In this first part, we expose properties of cohomologically trivial modules.

Definition : Cohomologically Trivial Modules

Let A be a G-module. A is said to be **cohomologically trivial** if for all H subgroup of G and for all $n > 0$, $H^n(H, A) = 0$. This last condition can equivalently be replaced by : $\forall n \in \mathbb{Z}$, $\hat{H}^n(H, A) = 0$.

One of the main focuses of this section will be to prove this equivalence, as well as to give more precise ideas on what the equivalence implies.

To begin with, a few lemmas, presented as nice little exercises :

Exercise : A Notation **

Let A be a G-module.

1. Observe there is a natural injection $A \to \mathbf{Ind}_1^G(A)$, $a \mapsto [f : g \mapsto g \cdot a]$.
2. Observe there is a natural surjection $\mathbf{Ind}_1^G(A) \to A$, $f \mapsto \sum_{g \in G} g \cdot f(g^{-1})$.
3. Let A_1 be the cokernel of the injection, and define by induction for $n \geq 0$, $A_0 = A$ and $A_{n+1} = (A_n)_1$. Let A_{-1} be the kernel of the surjection and define by induction $A_0 = A$ and $A_{n-1} = (A_n)_{-1}$ for $n \leq 0$. Prove the formula, for all $n, r \in \mathbb{Z}$:

$$\hat{H}^n(G, A) = \hat{H}^{n-r}(G, A_r)$$

solution : the third question is a simple induction using induction techniques (essentially the long cohomological sequence).

Exercise : A few lemmas ***

1. Let A be a G-module of p-primary torsion. Let G be a finite p-group. Prove that $A^G \neq \{0\}$.
2. Let $H \subset G$ be a subgroup such that $[G : H]$ is coprime with p. Then $\mathbf{Res} : H^n(G, A)\{p\} \to H^n(H, A)$ is injective.
3. Let B be an induced G-module. Prove that $\mathbf{Hom}_{\mathbb{Z}}(A, B)$, where the action of G is $f \mapsto g \cdot f \cdot g^{-1}$, is also induced. *Use the fact that an induced G module is of the form $\oplus_{g\in G} g.X$ where X is abelian and the action of G is obvious.*
4. Suppose A is a projective G-module and B any G-module. Then $A \otimes_{\mathbb{Z}} B$ (with action by g on the first factor) is a direct factor of an induced G-module.

Solution : for the first question, we just need to prove it for finite modules whose cardinal is a power of p, and this is just a consequence that $|A| = p^n = \sum_{O_a \text{ orbit of } a} |O_a|$, that $|O_a|$ is of order a power of p and that 0_A is alone in its orbit.

For the second one notice that post-composition with ***Cores*** *necessarily has kernel* 0.

For the third question, use the fact that being induced is the same thing as being a G-module of the form $\oplus_{g\in G} g.X$ where X is abelian and the action of G is obvious, then use that $\boldsymbol{Hom}(A, \oplus g.X) = \oplus \boldsymbol{Hom}(A, g.X) = \oplus g \cdot \boldsymbol{Hom}(A, X)$.

For the fourth question notice that a projective G-module is a direct factor of an $\oplus\mathbb{Z}[G]$. Tensorize with B, commute with direct sums and you get a direct factor of $\oplus(\mathbb{Z}[G] \otimes B)$. However, $\mathbb{Z}[G] \otimes B$ is isomorphic to $\boldsymbol{Ind}_1^G(B)$, which is induced, and a direct sum of induced modules is still induced.

Here's another exercise, a little bit harder :

Exercise : Cohomologically trivial G-modules and p-Sylows ***

For each prime number p, let G_p be a p-Sylow of G. We suppose that A is a cohomologically trivial G_p-module for all p.

1. Prove that for any p-Sylow G'_p, we also have $H^n(G'_p, A) = 0$. *You may use a similar approach than to the exercise at the end of section 2.2 about the invariance of cohomology by conjugation.*
2. Prove that A is cohomologically trivial.

Solution : the first one comes from using a super-horseshoe lemma, seeing that the change of group $\boldsymbol{Mod}_{G_p} \to \boldsymbol{Mod}_{G'_p}$ does not modify cohomology in any way (it is an isomorphism which of abelian categories). The second one comes from the fact that for any subgroup H, and for all p-Sylows H_p of H (contained in p-Sylows of G by definition), the restriction $H^n(H, A) \to H^n(H_p, A)$ is injective. And thus the $H^n(H, A)$ has to be 0.

We can now prove the core of this subsection.

Proposition : p-Groups and Modified Cohomology Groups

Let G be a finite p-group, and A a p-torsion G-module. Then if there is q such that $\hat{H}^q(G, A) = 0$, then A is induced (so in particular, it is cohomologically trivial).

Proof : This is once again a long proof, but a nice proof.

The first step is to find a free $\mathbb{F}_p[G]$-module V such that $A^G \simeq V^G$. There's nothing much to do here : take I a basis of A^G as an $\mathbb{F}_p$ vector space, and put $V = \sum_I \mathbb{F}_p[G]$. Clearly $V^G = \sum_I \mathbb{F}_p \simeq A^G$.

Let's extend the isomorphism $V^G \simeq A^G$ to a morphism $A \to V$. The key is to see that in the category of $\mathbb{F}_p$ vector spaces, V is free thus projective and hence we have an exact sequence :

$$0 \to \mathbf{Hom}(A/A^G, V) \to \mathbf{Hom}(A, V) \to \mathbf{Hom}(A^G, V) \to 0$$

It is a mental check to see that this sequence is also an exact sequence of G-modules for the action $f \mapsto g \cdot f \cdot g^{-1}$ defined above. Now we have seen than since V is free as an $\mathbb{F}_p[G]$-module, it is also induced (since $\mathbb{F}_p[G]$ is isomorphic to $\mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{F}_p$). So by an exercise above, $\boldsymbol{Hom}(A/A^G, V)$ is induced and thus cohomologically trivial. So in particular $H^1(G, \boldsymbol{Hom}(A/A^G, V)) = 0$ and thus we have a surjection of $\boldsymbol{Hom}_G(A, V) \to \boldsymbol{Hom}_G(A^G, V)$. This allows us to extend our isomorphism $A^G \to V^G$ to a morphim $j : A \to V$.

Now, our map j is injective, since the G-module $\boldsymbol{ker}(j)$ verifies $\boldsymbol{ker}(j)^G = 0$ (since the restriction $j : A^G \to V^G$ is an isomorphism), and is a p-torsion G-module where G is a p-group.

We now have the exact sequence $0 \to A \xrightarrow{j} V \to C \to 0$, and thus

$$0 \to A^G \xrightarrow{j} V^G \to C^G \to H^1(G, A)$$

. So we know that if $H^1(G, A) = 0$ then $C^G = 0$ and thus $C = 0$ by the same argument as above, and thus j is surjective.

Now we just need to prove that $\hat{H}^q(G, A) = 0 \implies H^1(G, A) = 0$. Using the notations of the first exercise of this section, we know that $\hat{H}^q(G, A) = 0 \implies \hat{H}^1(G, A_{q-1}) = 0$. So A_{q-1} is a free $\mathbb{F}_p[G]$-module. Now $\hat{H}^1(G, A) = \hat{H}^{2-q}(G, A_{q-1}) = 0$, which allows us to conclude.

Theorem : Equivalence Between Definitions of Cohomological Triviality (and more...)

Let G be any finite group and let A be any G-module.

- Suppose that for all prime number p, there is $q \in \mathbb{Z}$ such that $\hat{H}^q(G_p, A) = \hat{H}^{q+1}(G_p, A) = 0$ (where G_p is a p-Sylow of A). Then A is cohomologically trivial.
- A cohomologically trivial module which is free as a $\mathbb{Z}$-module is projective as a $\mathbb{Z}[G]$-module.
- A cohomologically trivial module is also trivial in modified cohomology in all degrees, and there is a projective resolution of A of the form :

  $$0 \to R \to F \to A \to 0$$

  ...where F is free as a $\mathbb{Z}[G]$-module and R is projective as a $\mathbb{Z}[G]$-module.

Proof : First of all, write an exact sequence $0 \to R \to F \to A \to 0$ where F is a free G-module. Since F is cohomologically trivial, we know that $\hat{H}^{q+1}(G_p, R) = \hat{H}^{q+2}(G_p, R) = 0$. By the exact sequence $0 \to R \to R \to R/pR \to 0$, we can thus apply our previous lemma to obtain that R/pR is induced as a G_p-module.

Firstly, let's prove our theorem if A is free on $\mathbb{Z}$. Denote $M = \boldsymbol{Hom}_{\mathbb{Z}}(A, R)$ with its usual G-action. This module has trivial cohomology in degree 1. Indeed, we have an isomorphism :

$$M/pM \simeq \mathbf{Hom}_{\mathbb{Z}}(A, R/pR)$$

Thus M/pM is induced as a G_p-module. So $H^1(G_p, \boldsymbol{Hom}_{\mathbb{Z}}(A, R/pR)) = 0$. Now the exact sequence $0 \to M \to M \to M/pM \to 0$ proves that $H^1(G_p, M) \xrightarrow{\cdot p} H^1(G_p, M)$ is an isomorphism, and thus that the p torsion of $H^1(G_p, M)$ is zero. Finally since $H^1(G, M) \to H^1(G_p, M)$ is injective, this proves that the p-torsion of $H^1(G, M)$ is zero, and thus it is zero in all degrees.

Now considering this fact, we have an exact sequence of $\mathbb{Z}$-modules, since A is free :

$$0 \to \mathbf{Hom}_{\mathbb{Z}}(A, R) \to \mathbf{Hom}_{\mathbb{Z}}(A, F) \to \mathbf{Hom}_{\mathbb{Z}}(A, A) \to 0$$

And since $H^1(G, M) = 0$, this sequence stays exact after taking fixed points under $\boldsymbol{Def}_1^G$, which proves that there is a surjection $\boldsymbol{Hom}_G(A, F) \to \boldsymbol{Hom}_G(A, A) \to 0$. So we can take the inverse image of identity to get that as G-modules, $F \simeq A \oplus K$. This proves points 1.

The rest of the proof is fairly easy. If A is so, apply what we just did to R, which is a free $\mathbb{Z}$-module as a submodule of F, and apply the long cohomology sequence. This proves point 1 generally.

Point 2 has been proven in our first paragraph, as A was proven to be a direct factor of a free module.

Point 3 is just a consequence of everything we just did (remember that a projective G-module is also a projective H-module).

Exercise : Tensorizing by cohomologically trivial modules **

Let A be cohomologically trivial and let B be another G-module, torsion-free. Prove that $A \otimes_{\mathbb{Z}} B$ (with action of G on the first factor) is cohomologically trivial.

Solution : Since B is torsion-free on $\mathbb{Z}$, it is flat. Thus the sequence $0 \to R \otimes B \to F \otimes B \to A \otimes B \to 0$ is still exact. Now use the fact that if a G-module is projective.

Note that this is still the case if the action of G is now on the two factors. Indeed, now we get that $\mathbb{Z}[G] \otimes_{\mathbb{Z}} B$ becomes isomorphic to $\boldsymbol{Ind}_1^G(B)$ with action $g \cdot f : x \mapsto gf(g^{-1}x)$ (define $b \otimes g \mapsto [g \mapsto b_g]$), which, it is easy to check, is also cohomologically trivial. All proofs work the same from here.

3.6 Cohomology of Profinite Groups

We will now generalize what we did earlier to the category of profinite groups. For an overview of the topic, see the dedicated chapter.

3.6.1 The Category Of Discrete G-modules

A profinite group G comes with its profinite topology. The category in which we will work to define our theory of cohomology for profinite groups is that of discrete G-modules.

Definition : Discrete G-Modules

Let M be a G-module. M is said to be **discrete** if the maps :

$$G \to M$$

$$g \mapsto g \cdot m$$

... are continuous for the profinite topology on G and the discrete topology on M. It is equivalent to ask that the groups subgroups of G, $g \in G$, $g \cdot m = m$ are open.

Verifications : Direct implication is clear, converse implication is easy : each point of $\cdot m^{-1}(n)$ contains a stabilizer of m as a neighborhood.

Since G is compact, then any point of M has a finite orbit under G since the stabilizers are open and thus have finite index.

Discrete G-modules form a full subcategory of $\mathbf{Mod}_G$.

However, nothing in this category guarantees that there are enough projectives or enough injectives. The following proposition settles the case.

Proposition : Projective and Injective Discrete G-Modules

The category of discrete G-modules has enough injectives, but not enough projectives.

Proof : Let A be a discrete G-module. Then there is an injective G-module I and an injection $A \hookrightarrow I$. Now let $I' = \cup_{U \text{ open in } G} I^U$. Since A is discrete, then the injection is actually an injection of $A \to I'$. It is then easy to verify that I' is injective in the category of discrete G-modules by the same arguments.

The fact that this category does not have enough projectives is just a matter of finding counter-examples : one can be found in [1] as an exercise of chapter 4. It is not however too enlightening. It is better to keep in mind that, for example, $\mathbb{Z}[G]$ is nowhere close to being a discrete G-module.

In the category of discrete G-modules, for any closed subgroup $H \subset G$, the relations between G-modules and G/H modules induced by deflation and inflation functors works strictly the same way, and the proofs can be transcribed verbatim.

However, the description is not exactly the same when it comes to induction.

Definition : Restriction and Induction for Discrete G-modules

Let G be a profinite group, H be a closed subgroup of G, and let A be a discrete G-module. The restriction functor from discrete G-modules to discrete H-modules works exactly like the finite case.

If A is a discrete H-module, the induction functor is constructed by sending A to the G-module of continuous functions $G \to A$ that verify $\forall h \in H$, $f(hg) = h \cdot f(g)$ and with action of G given by $(g \cdot f)(x) = f(xg)$.

Verifications : the constructed module is indeed discrete. To see this, note that a continuous function $f : G \to A$ only has a finite number of images thanks to compacity of G and discreteness of A. Now let $x_1, ..., x_n$ be elements of G so that $f : \{x_1, ..., x_n\} \to f(G)$ is surjective. Consider open subgroups U_i such that $f(x_i U_i) = \{x_i\}$ (which is possible by continuity). Then for every $g \in \cap_{i=1}^n$, $g \cdot f = f$, so stabilizers of points are open.

Keeping in mind the crucial fact that elements of $\mathbf{Ind}_H^G(A)$ have finite image, we can retrieve our adjunctions.

Proposition : Restriction/Induction Adjunction for Discrete G-Modules

The restriction and induction functors are respectively left and right adjoint functors of one another. In other words, for all discrete G-module A and discrete H-module B, there is a natural isomorphism :

$$\mathbf{Hom}_H(\mathbf{Res}_H^G(A), B) \simeq \mathbf{Hom}_G(A, \mathbf{Ind}_H^G(B))$$

Proof : given an H-morphism $f : A \to B$, one can construct a morphism $\tilde{f}$ from $A \to \boldsymbol{Ind}_H^G(A)$, by sending $x \in A$ to the function from $G \to B$, $g \mapsto f(g \cdot x)$]. Since A is discrete, this is of course continuous.

Conversely, given a map $f : A \to \boldsymbol{Ind}_H^G(B)$, one can construct an H-morphism $A \to B$ by $a \mapsto f(a)(1)$ (remember that $f(a)$ is itself a continuous map). We leave it to you to check that these maps are reciprocal bijections.

Naturality is left as an exercise for the immensely patient reader.

Proposition : Homological Properties of Induction for Discrete G-modules

If B is an injective H-module, then $\mathbf{Ind}_H^G(B)$ is an injective G-module. Also, the functor $\mathbf{Ind}_H^G$ is exact.

Proof : the preservation of injectivity comes from the fact that ***Res*** *is clearly exact. Exactness requires a different proof than in the finite case, since induction is defined differently. We will prove it directly. Let* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *be an exact sequence of discrete* G*-modules, and let :*

$$0 \to \mathbf{Ind}_H^G(A) \xrightarrow{f_*} \mathbf{Ind}_H^G(B) \xrightarrow{g_*} \mathbf{Ind}_H^G(C) \to 0$$

... be the corresponding image sequence. Clearly, the first map f_* *stays injective. Now let* $t \in \boldsymbol{Ind}_H^G(B)$ *suppose that* $g \cdot t = 0$*. Then the finite set* $\boldsymbol{Im}(t)$ *is in the kernel of* g *so in the image of* f*. Define* $\tilde{t} : G \to A$*,* $g \mapsto f^{-1}(t(g))$*. It is clearly locally constant so continuous, and thus* $\boldsymbol{Ker}(g_*) = \boldsymbol{Im}(f_*)$*. Surjectivity of* g_* *is similar.*

Unfortunately, we do not have the converse adjunction (except when H is open G : in this case the proof can be reinvested). However, the following fact is still true :

Proposition : Injectives as discrete G and H-modules

Let I be an injective discrete G-module. Then $\mathbf{Res}_H^G(I)$ is also an injective discrete H-module.

*Proof : We do not include it in this version, for the proof is fairly complicated. However, one can be found in [***1***], chapter* 4*.*

3.6.2 Definition of Cohomology of Profinite Groups, First Properties

Now we need to define the cohomology of a profinite group. There are two obvious ways to do it, that mimic what we did so far. Let G be a profinite group and A be a discrete G-module.

- The additive deflation functor $\mathbf{Def}_1^G : A \to A^G$ is clearly left exact. Define the cohomology groups $H^i(G, A)$ as the right derived functors of F applied to A (this is a valid construction, since the category of discrete G-modules has enough injectives).
- Consider the complex $K^i(G, A)$ consisting of the continuous functions $G^i \to A$ where A is given the discrete topology, and the differential operators are defined as usual. Denote $H^i(G, A)$ as the i-th cohomology group of this complex.

However, there is a third one, that requires attention.

- Consider a projective description of $G = \varprojlim G/U$ and the inductive description of $A = \varinjlim A^U$ (which is valid because A is discrete : every $x \in A$ has an open stabilizer and thus is fixed by an open normal subgroup).
- One may construct arrows $H^i(G/V, A^V) \to H^i(G/U, A^U)$ whenever $U \subset V$, in the following way : consider the explicit description of $H^i(G/V, A^V)$ by quotients of the groups $K^i(G/V, A^V)$ of functions $(G/V)^i \to A^V$. When $U \subset V$, one can define a map between the complexes $K^i(G/V, A^V) \to K^i(G/U, A^U)$ by precomposing by $G/U \twoheadrightarrow G/V$ and post-composing by $A^V \hookrightarrow A^U$. Thus, it factors into maps $H^i(G/V, A^V) \to H^i(G/U, A^U)$.
- One can check that with those maps, the $H^i(G/U, A^U)$, indexed by U, form an inductive system.
- Let $H^i(G, A) := \varinjlim H^i(G/U, A^U)$.

This is a hard theorem that we will not prove in this paper.

Theorem : Different Constructions of the Cohomology of Profinite Groups

The three latter constructions define isomorphic cohomological universal δ-functors.

Proof : a proof can be found in [1] in the fourth chapter.

The third proposition is the most useful one, as we will see in the next section.

3.6.3 Properties of Cohomology of Profinite Groups

This section will be dedicated to understanding which properties of cohomology that we proved in the finite case may be extended to the profinite case.

First Properties

- It is not true anymore that the $H^i(G, A)$ are always finite (there will be examples later on. However, they are still torsion in degree ≥ 1 as inductive limits of torsion modules, and multiplication by $|A|$ (if $|A|$ is finite) still kills the $H^i(G, A)$, thanks to the inductive limit description.
- If G acts trivially on A, then $H^1(G, A) = \mathbf{Hom_{Gp}}(G, A)$ (where **Gp** denotes the category of groups). This is a consequence of the fact that the description of $H^i(G, A)$ through the function groups $K^i(G, A)$ is identical in the profinite case.

Induction Techniques

Modules of the form $\mathbf{Ind}_1^G(A)$ still have trivial cohomology in degree ≥ 1 thanks to the derived functor description. This is because if :

$$0 \to A \to I_1 \to I_2 \to ...$$

... is an injective resolution of A, then its image by $\mathbf{Ind}_1^G$ is an injective resolution of $\mathbf{Ind}_1^G(A)$, and $\mathbf{Def}_1^G \circ \mathbf{Ind}_1^G$ is the identity. So of course, we will obtain trivial cohomology groups.

Thus, induction techniques as described in the dedicated section for the finite case still work the same.

Restriction and Corestriction

If $H \subset G$ is **open** (of finite index), we can define in the exact same way restriction and corestriction. Notice that this is impossible if H is not of finite index. We thus still have the fact that the composition $\mathbf{Cores} \circ \mathbf{Res}$ is multiplication by $[G : H]$ in degree ≥ 1.

The Hoschild-Serre Spectral Sequence

Since the deflation/inflation adjunction still exists, and inflation is exact, then injective G-modules are injective H-modules when H is closed in G. Thus the Hoschild-Serre exact sequence still workds just as well.

The Shapiro Isomorphism

I leave it to you that the solution of the exercise "The Shapiro Isomorphism" can be transposed verbatim to the profinite case : namely, if H is closed in G, we have an isomorphism of δ-functors:

$$H^i(G, \mathbf{Ind}_H^G(\cdot)) \to H^i(H, \cdot)$$

... with input the category of discrete H-modules.

Modified Cohomology

Modified Cohomology can also be described in some form in the case of profinite groups, however we will not describe it completely since we will not need it. However, if G is procyclic (its quotients G/U are cyclic) then its cohomology is 2-periodic after rank 1, which is an obvious consequence of the finite case and of the inductive limit description. Moreover, one can define a $\hat{H}^0(G, A)$ group in modified cohomology, which is defined this time as the inductive limit of the groups $\hat{H}^0(G/U, A^U)$, where the arrow $\hat{H}^0(G/U, A^U) \to \hat{H}^0(G/V, A^V)$ when $V \subset U$ is via the norm homomorphism, $A^U/N_U A \to$

$A^V/N_V A, [x] \mapsto [\sum_{t\in U/V} t\cdot x]$. In the cyclic case, the isomorphisms $H^{2n}(G/U, A^U) \simeq \hat{H}^0(G/U, A^U)$ make the following squares commute :

$$\begin{array}{ccc} \hat{H}^0(G/U, A^U) & \xrightarrow{\simeq} & H^{2n}(G/U, A^U) \\ \downarrow & & \downarrow \\ \hat{H}^0(G/V, A^V) & \xrightarrow{\simeq} & H^{2n}(G/V, A^V) \end{array}$$

This allows us to prove that the groups $H^{2n}(G, A)$ are in this case isomorphic to the groups $\hat{H}^0(G, A)$, and gives an explicit way of computing them.

3.7 Cohomological Dimension

3.7.1 Definition and Properties

In this section, we introduce a useful notion called cohomological dimension, which is fairly impressive and which is a great occasion to do a few exercises on the notions we have seen so far.

Definition : Cohomological Dimension

Let G be a profinite group. The **p-cohomological dimension of G** is the smallest integer $n \in \mathbb{N}\cup\{+\infty\}$ such that for all $q > n$ and for all **torsion** discrete G-module, $H^q(G, A)\{p\} = 0$. It is denoted $\mathbf{cd}_p(G)$.

The **cohomological dimension** of G is the upper bound of of the $\mathbf{cd}_p(G)$ when p ranges over the prime numbers. It is denoted $\mathbf{cd}(G)$.

Strict p-cohomological dimension and **strict cohomological dimension** are defined similarly by requiring the vanishing condition for all discrete G-modules (not just torsion ones). It is denoted $\mathbf{scd}_p(G)$ or $\mathbf{scd}(G)$.

Cohomological dimension is a notion which is proper to profinite groups : as we will see later, for a finite group G, it contains strictly less information than the cardinal of G.

Exercise : When p is Coprime to the Order of G **

Let G be a profinite group. Let p be a prime number which is coprime with $[G : 1]$. Prove that the strict p-cohomological dimension of G is 0.

Solution : For a G-module A, all of the elements of $H^i(G, A)$ for $i > 1$ come from a certain $H^i(G/U, A^U)$, and thus have n-torsion where $n|[G : 1]$ as supernatural numbers. Now having n-torsion and q-torsion with $n \wedge q = 1$ is equivalent to being 0.

Exercise : Cohomological Dimension of Finite Groups **

Let G be a finite group. What is the p-cohomological dimension of G for each p, in terms of the cardinal of G ? You may assume the fact (which we will prove later) that for $H \subset G$, then $\mathbf{cd}_p(H) \leq \mathbf{cd}_p(G)$.

Solution : when $p \wedge |G| = 1$, it is zero. When $p||G|$, G contains a cyclic group of order p. Take a module which has non trivial cohomology under this cyclic group (for example, itself with trivial action) and use the fact that $\mathbf{cd}_p(H) \leq \mathbf{cd}_p(G)$ to find that the p-cohomological dimension of G is infinite.

Finding out what cohomological dimension is isn't that easy. Here's a few lemmas that help us compute it.

Proposition : Characterization of Cohomological Dimension

The three following propositions are equivalent :

- $\mathbf{cd}_p(G) \leq n$
- For all discrete p-primary torsion G-modules A, and for all $q > n$ $H^q(G, A) = 0$.
- For all simple p-torsion discrete G-module, $H^{n+1}(G, A) = 0$.

Proof : $1 \implies 2$ *is by definition,* 2 *implies* 1 *is obtained by decomposing* A *as a direct sum of its primary torsions, using additivity of cohomology and noticing that the primary* p*-torsions of cohomology is the cohomology of the primary* p*-torsions. Obviously* $2 \implies 3$. $3 \implies 2$ *is by induction for the finite case : for* $A = 0$ *there is nothing to prove. Now if* A *is finite and non zero, take an element of order* p*, construct an exact sequence of smaller order* $0 \to A_1 \to A \to A_2 \to 0$ *and use the long cohomology sequence. For the infinite case notice that* A *is the inductive limit of its finite sub-modules. To prove that the higher cohomology groups verify the same property throw* $A \hookrightarrow I_G(A)$ *which is still* p*-primary and so the quotient is too, and use the long cohomology sequence.*

The third property is of course the most important.

Proposition : Characterization of Cohomological Dimension for pro-p groups

Let G be a pro-p group. Then $\mathbf{cd}(G) \leq n \iff H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$.

One way is evident. For the other way, let A *be a simple discrete* G*-module of* p*-torsion. Since it is simple and of* p*-torsion, it has a single generator (under* G*) which is of order* p*. By discreteness,* A *is finite. Now since* A *is finite, it is a* G/U*-module for some* U*. Now the class formula proves that* A^G *is not just* $\{1\}$*, and so it is* A*. So* G *acts trivially. So* A *is actually* $\mathbb{Z}/p\mathbb{Z}$ *because it has a single generator...*

One would think that there is a wide step between cohomological dimension and strict cohomological dimension. Actually, it's not that wide.

Proposition : A Link between Cohomological Dimension and Strict Cohomological Dimension

We have the upper bound $\mathbf{scd}_p(G) \leq \mathbf{cd}_p(G) + 1$.

Proof : This comes from the fact that multiplication by p *in a module* M *yields two exact sequences :*

$$0 \to pM \hookrightarrow M \to M/pM \to 0$$

$$0 \to M[p] \hookrightarrow M \to pM \to 0$$

Going to long exact sequences of cohomology shows that for all $q > n + 1$ *the arrows :* $H^q(G, M) \to H^q(G, pM)$ *(obtained from the second one) and* $H^q(G, pM) \to H^q(G, M)$ *(obtained from the first one) are injective. Their composition is multiplcation by* p*, so it is also in* H^q*, and thus* $H^q(G, M)$ *has no* p*-torsion.*

Finally, there are the two beautiful following facts :

Theorem : Subgroups, Quotients and Cohomological Dimension

Let G be profinite group and H be a closed subgroup of G. The following properties hold :

- $\mathbf{cd}_p(H) \leq \mathbf{cd}_p(G)$, with equality if $[G : H]$ is coprime with p or if H is open and G is of finite p-cohomological dimension.
- If H is normal, $\mathbf{cd}_p(G) \leq \mathbf{cd}_p(G/H) + \mathbf{cd}_p(H)$

They follow from two lemmas :

Proposition : Two lemmas about cohomological dimension

- If p is coprime with $[G : H]$, then **Res** : $H^q(G, A)\{p\} \to H^q(H, A)\{p\}$ is injective for all $q > 0$.
- If additionally H is open and $n = \mathbf{cd}_p(G) < +\infty$, then **Cores** : $H^n(H, A)\{p\} \to H^n(G, A)\{p\}$ is surjective.

Proof : this is easy in the finite case because $\boldsymbol{Cores} \circ \boldsymbol{Res}$ *is injective since* m *is coprime with* p*. The profinite case follows from an exercise above that describes* **Res** *as an inductive limit, which stays injective by exactness. Note that taking* p*-primary torsion and inductive limit is commutative.*

The second result comes by from shapiro, using the fact that corestriction $H^i(H, A) \to H^i(G, A)$ *is the same as taking to cohomology a certain morphism* $H^i(G, I_G^H(A)) \to H^i(G, A)$*. Taking the kernel of this morphism gives an exact sequence :*

$$0 \to B \to I_G^H(A) \to A \to 0$$

... which leads to a long exact sequence in cohomology. Then, notice that $\{p\}$ *functor is exact and use the fact that* $H^{n+1}(G, B)\{p\}$ *is* 0*.*

We can now prove our theorem.

Proof of the theorem : For the first one, the fact that $H^n(H, A) = H^n(G, I_G^H(A))$ *gives* $\boldsymbol{cd}_p(H) \leq \boldsymbol{cd}_p(G)$*. If* $[G : H]$ *is coprime with* p*, equality comes from the injection. If* H *is open and of finte index, equality comes from the surjection. The second theorem is a direct application of the Hoschild-Serre spectral sequence, noticing that in degree greater than* $\boldsymbol{cd}_p(G/H) + \boldsymbol{cd}_p(H)$*,* $H^n(G, A)p$ *will be filtered by null groups.*

This shows that to find what $\mathbf{cd}_p(G)$ is, we can just look to its p-Sylows.

Finally, here's a last criterion for equality between cohomological and strict cohomological dimension.

Proposition : A Criterion for when $\mathbf{cd}(G) = \mathbf{scd}(G)$

Let G be a profinite group of finite cohomological dimension equal to n. Then its strict cohomological dimension is also equal to n if and only if for all open subgroups of $U \subset G$, $H^{n+1}(U, \mathbb{Z}) = 0$.

Proof : the condition is necessary thanks to the upper bound we just proof. Sufficience is more subtle : Shapiro says that $H^{n+1}(U, \mathbb{Z}) = H^{n+1}(G, I_G^U(\mathbb{Z}))$*. Let* M *be a discrete* G*-module of finite type. Then if* U *is an open subgroup that acts trivially on* M *(which exists because* M *is of finite type), we have an exact sequence :*

$$0 \to B \to \mathbb{Z}[G/U]^r \to M \to 0$$

But $\mathbb{Z}[G/U]^r = I_G^U(\mathbb{Z}^r) \simeq I_G^U(\mathbb{Z})^r$. So cohomology gives 0, use long sequence and then use that M is inductive limit of its finite type submodules (don't forget to use the bound at various places to show that $H^{n+2}(G,\cdot) = 0$).

3.7.2 The example of $\hat{\mathbb{Z}}$

To finish up this section, here is a complete computation of the (strict) cohomological dimension of $\hat{Z} = \prod_{p \text{ prime}} \mathbb{Z}_p$ for every prime number p. Giving it a go yourself first would be great training.

Since $[\hat{\mathbb{Z}} : \mathbb{Z}_p]$ is coprime with p, we have :

$$\mathbf{cd}_p(\hat{\mathbb{Z}}) = \mathbf{cd}_p(\mathbb{Z}_p)$$

Now, see that the p-cohomological dimension of $\mathbb{Z}_p$ is at least 1. Indeed, thanks to the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, and to the fact that $\mathbb{Q}$ with trivial action by $\mathbb{Z}_p$ has zero cohomology since it is uniquely divisible, we know that $H^1(\mathbb{Z}_p, \mathbb{Q}/\mathbb{Z}) \simeq H^2(\mathbb{Z}_p, \mathbb{Z})$. However, since $\mathbb{Z}_p$ is procyclic, the application of modified cohomology to the profinite case allows us to prove that $H^2(\mathbb{Z}_p, \mathbb{Z}) \simeq \hat{H}^0(\mathbb{Z}_p, \mathbb{Z})$ which is the inductive limit of the groups $\mathbb{Z}/p^n\mathbb{Z}$ where arrows are mutiplication by p. So $H^1(\mathbb{Z}_p, \mathbb{Q}/\mathbb{Z}) = H^2(\mathbb{Z}_p, \mathbb{Z}) = \mathbb{Z}_{p_\infty}$. Note that we have also proven that its strict cohomological dimension is at least 2.

To prove that the cohomological dimension of $\mathbb{Z}_p$ is exactly 1, the quickest way to go is to prove that $H^2(\mathbb{Z}_p, \mathbb{Z}/p\mathbb{Z}) = 0$. But this is fairly simple, since it is equal by the same token as above to the inductive limit of the groups $\mathbb{Z}/p$ where induction arrows are multiplication by p. This yield a trivial inductive limit since all arrows are 0.

Chapter 4

Field Theory and Galois Theory

In this section, we will try and understand one of the most beautiful pieces of mathematics I know : Galois Theory. Galois Theory can have many definitions, here's mine : Galois theory is the study of field extensions by roots of some polynomials. For example, extensions of the form $\mathbb{Q}[\sqrt{2}] \simeq \mathbb{Q}[X]/X^2 - 2$. Our focus will be on certain particularly well behaved extensions, called **Galois Extensions**, that are defined as verifying two important properties : separability and normality. Our goals will be as follows :

- A first part of this document is a first course in field theory. We wish to...
  1. Remind you of the basic properties of fields, more precisely of field extensions.
  2. Study more precisely polynomials with coefficients in a given field, and their links with field extensions.
  3. Study what algebraic closures are, why they exists and why they are important.
  4. Understand field morphisms, displacements, and the fundamental isomorphism extension theorem.
- A second part of this document focuses on Galois Theory more precisely.
  1. We will study the first fundamental question of Galois Theory : normality. What it is, and how it works. This should be a fairly short section.
  2. We will then study the second fundamental question of Galois Theory : separability. This should take a little more time, for it is full of quite subtle points.
  3. We will then finally be able to turn to Galois Theory properly speaking, citing and proving the fundamental theorem of Galois Theory.
  4. A last chapter will be dedicated to some consequences of this fundamental theorem.
- A third part of this document will be dedicated to examples of famous Galois Extensions, with the theorem associated to them. This document only contains finite fields, but extensions should be added soon.
- A last part of our document will provide a refinement in Galois theory : infinite Galois theory.

4.1 Field Theory

Of course, in this document, all rings are commutative with 1.

4.1.1 Basic Properties of Field Extensions

Here we go ! As I expect you to know...

Definition : Fields

A field is a ring where all non-zero elements are invertible. Equivalently, it is a ring whose only proper ideal is 0.

You should know some examples : $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}/p$... For practice, here's another sometimes less well-known example.

Exercise : Formal Series **

Let k be any field, and let A denote the ring of formal series with coefficients in K, of the form :

$$\sum_{i=-m}^{\infty} a_i X^i$$

... with $a_{-m} \neq 0$. Multiplication and addition are obviously defined. Prove that A is a field.

Solution : constructing an inverse to any element is a fairly straightforward. To simplify the computations, perhaps factorize have the first non zero coefficient at index 0.

Now, here's the object we study in this first section :

Definition : Field Extensions

A **field extension** is simply a field K containing a field F. We denote such an extension K/F.

Field extensions aren't interesting as simple inclusions of sets. They become interesting once you notice that the action of F on K endows K with a structure of F-vector space. Here's a concrete example of such a phenomena happening.

Exercise : Study of a Field Extension **

Let $\mathbb{Q}[\sqrt{2}]$ denote the subring of $\mathbb{R}$ of elements of the form $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$.

1. Prove that $\mathbb{Q}[\sqrt{2}]$ is a field which contains $\mathbb{Q}$. Thus we have a field extensions $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$.
2. Prove that $\mathbb{Q}[\sqrt{2}]$ is two dimensional as a $\mathbb{Q}$-vector space.

Solution : the first one is just writing, the second one comes from the fact that the description of $\mathbb{Q}[\sqrt{2}]$ *proves that its dimension is at most* 2*, and irrationality of* $\sqrt{2}$ *proves that it is at least* 2*.*

The above situation is formalized with the following definition.

Definition : Degree of a Field Extension

Let K/F be a field extension. The **degree** of the extension K/F is the dimension of K as an F-vector space. It is denoted $[K : F]$. If it is finite, the extension K/F is said to be **finite**. If it is infinite, the extension is said to be **infinite**.

In our exercise above, our extension is finite, of degree 2. We will meet many infinite extensions as we go on. Here is an important fact about field extensions :

Proposition : Telescopic Base Theorem

Let $K \supset L \supset F$ be fields. The extension K/F is finite if and only if the extensions K/L and L/F are finite.

Moreover, if (α_i) is a base of L as an F-vector space and (β_j) is a base of K as an L vector space, then $(\alpha_i\beta_j)$ is a base of K as an F-vector space. This yield the equality :

$$[K : F] = [K : L][L : F]$$

Proof : If K/F is finite, of course K/L is finite since L contains F and L/F is finite since L is a sub-F-space of K. Conversely, if L/F and K/L are finite, proving the second part of the theorem suffices.

It is straightforward to check that the proposed family is free over F, and straightforward too to check that it generates everyone. Thus here we are.

We finish this first short chapter by mentioning extensions generated by certain subsets. This is very similar to the analogous situation with vector spaces.

Definition : Field Extension Spanned by a Subset

Let K/F be a field extensions, and S a subset of K. The field extension spanned by S is the smallest field extension (the intersection of all extensions) of F containing S. It is denoted $F(S)/F$.

As with vector spaces, spanned subextensions have explicit descriptions.

Proposition : Explicit Description of Spanned Extensions

Let K/F and S be as above. Denote R the image in $F(S) \subset K$ of the ring morphism :

$$F[X_s, s \in S] \to K$$
$$X_s \mapsto s$$

Then $F(S)$ consists of elements of the form ab^{-1} where $a, b \neq 0$ and $a \in R$ and $b \in R^{-1}$.

Proof : Such a subset is clearly stable by multiplication and inversion. Seeing it is stable by addition is done through noticing that $ab^{-1} + cd^{-1} = (ad + cb)(bd)^{-1}$. Clearly, it contains S, and every field that contains s contains it.

This expression is a bit clumsy, but will be simplified with an additional condition on the field extension (see algebraic field extensions later).

Exercise : Finite Extensions, Finitely Generated Extensions **

We say that a field extension K/F is finitely generated if $K = F(S)$ where S is a finite subset of K. Prove that a finite extension is finitely generated. What about the converse ?

Proof : just choose a base ! The second answer is no, considering $k(x)/k$ where k is any field.

Definition : Composite Extensions

Let $K \supset L_1, L_2$ be fields. Then the composite extension $L_1L_2 \subset K$ is the smallest extension containing both L_1 and L_2.

Composite extensions have easy properties that are derived from the above.

Proposition : Properties of Composite Extensions

Let $K \supset L_1, L_2$ be as above. Then :

- $L_1L_2 = L_1(L_2) = L_2(L_1)$.
- If $L_1 = F(S_1)$ and $L_2 = F(S_2)$, then $L_1L_2 = F(S_1 \cup S_2)$.

Proof : For the first one, the smallest subfield of K containing L_1 and L_2 is the smallest extension of L_1 containing L_2 and conversely. Second one is clear.

More will be said about those extensions once we will have understood what algebraic extensions are.

4.1.2 Reminders about Polynomials With Coefficients in a Field

Before going any further, we need a few reminders about properties of polynomials with coefficient in a field. If the words roots, repeated roots, split, irreducible, don't ring a bell, I advise you to go check a basic algebra textbook. The properties we will use the most are reminded here :

Proposition : Properties of Polynomials with Coefficients in a Field

Let k be any field.

- The ring $k[X]$ of polynomials with coefficients in k is a principal ideal domain. Thus...
- $k[X]$ is a UFD.
- All prime ideals of k are maximal.
- Irreducible polynomials of $k[X]$ are exactly those which generate a prime / maximal ideal.
- If k is the fraction field of a domain A, then the irreducible polynomials of $A[X]$ are exactly the irreducible elements of A as well as the primitive polynomials irreducible in $k[X]$.

Proof of those results can be found in most basic commutative algebra texts.

4.1.3 Algebraic Extensions

Polynomials will be paramount to the study field extensions. The central notions are defined here :

Definition : Algebraic Element, Algebraic Extension, Minimal Polynomial

Let K/F be a field extension. Let $\alpha \in K$. α is said to be **algebraic** over F if there is a polynomial $f \in F[X]$ such that $f(\alpha) = 0$.

The extension K/F is said to be **algebraic** if every element of K is algebraic over F.

The ideal of $k[X]$ generated by the polynomials that vanish on an algebraic element α is generated by a single element written $\min(\alpha, F)$. It is the **minimal polynomial** of α ofer F.

Such a polynomial $\min(\alpha, F)$ is necessarily irreducible, since it must be the polynomial of smallest degree that vanishes on α.

Algebraicity allows us to characterize finite extensions in a very comfortable way.

Proposition : Characterization of Finite Extensions

An extension $F(\alpha)/F$ is finite if and only if α is algebraic. Its degree is the same as the degree $\min(\alpha, F)$.

More generally, an extension K/F is finite if and only if it is algebraic and finitely generated. We have then have the bound $[F(\alpha_1, ..., \alpha_n) : F] \leq \prod_{i=1}^{n} \deg \min(\alpha_i, F)$.

Proof : if α is algebraic, then the proof is the first part of the proof of the next proposition. If α is not algebraic, then $1, \alpha, \alpha^2, ...$ is an infinite free family.

Now, if the extension K/F is finite, then clearly it is algebraic because for every element $\alpha \in K$ the family $(1, \alpha, \alpha^2, ...)$ is linearly dependent. Clearly it is finitely generated over F : just take S to be the elements of a base. Conversely, suppose K/F is algebraic and finitely generated. If it is generated by one element, and is algebraic, then it is the what we have just proven. If this is true for n elements, then say $K = F(\alpha_1, ..., \alpha_n, \alpha_{n+1}) = F(\alpha_1, ..., \alpha_n)(\alpha_{n+1})$. Then of course α_{n+1} is algebraic over $F(\alpha_1, ..., \alpha_n)$ with minimal polynomial of degree $\leq \min(\alpha_{n+1}, F)$, since $\min(a_{n+1}, F(\alpha_1, ..., \alpha_n))|\min(\alpha_{n+1}, F)$. The first fact then tells us that $F(\alpha_1, ..., \alpha_n)(\alpha_{n+1})$ is indeed finite and the inequality $\deg \min(a_{n+1}, F(\alpha_1, ..., \alpha_n)) \leq \deg \min(\alpha_{n+1}, F)$ gives us the bound.

Algebraicity also allows us to give an explicit description of spanned extensions in a simple way.

Proposition : Descriptions of Spanned Expansions for Algebraic Extensions

Let K/F be a field extension.

1. If $\alpha \in K$ is algebraic over F, then $F(\alpha)/F$ is the image of the map $F[X] \to K$, $X \mapsto \alpha$. A basis of $F(\alpha)$ as an F vector space is given by the elements $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ where $n = \deg \min(\alpha, F)$.
2. If $(a_1, ..., a_n)$ are all algebraic over F, then $F(a_1, ..., a_n)$ is the image of $F[X_1, ..., X_n] \to K$, $X_i \mapsto a_i$.
3. If S is an arbitrary set of elements of K, algebraic over F, then $F(S)$ is the image of $F[X_s, s \in S] \to K$, $X_s \mapsto s$.

Proof : the image of this morphism is isomorphic to $F[X]/\min(\alpha, F)$, which is irreducible. Thus it is a field which contains α. Clearly it is the smallest. And clearly a basis is $1, X, ..., X^{\deg \min(\alpha, F)-1}$. So projecting gives the expected basis.

The next fact is proved by induction : suppose it is true for n. Let (c_i) be an F-base of $F(a_1, ..., a_n)$. Then by the former proposition and because a_{n+1} is algebraic over $F(a_1, ..., a_n)$, an F-base of $F(a_1, ..., a_n, a_{n+1})$ is given by $(a_{n+1}^j c_i)$ for a finite number of j, by telescopic base. Clearly, the image of our morphism is contained into $F(a_1, ..., a_{n+1})$ and contains the base $(a_{n+1}^j c_i)$, so it is surjective, which finishes the proof.

For the last fact, note that $F(S) = \cup_{x \text{ finite }, x \subset S} F(x)$ (use explicit description). Then see that from the former proof, $F(x)$ is indeed in the image of the morphism, which proves its surjectivity.

Such facts allow us to make many proofs fairly simple. For example :

Proposition : Transitivity of Algebraicity

Let $F \subset L \subset K$ be fields. Then K is algebraic over F if and only if K is algebraic over L and L is algebraic over F.

Proof : Clearly if K is algebraic over F, then K is over L and L is over F. Now if K is algebraic over L and L is algebraic over F, then any element of K is killed by a polynomial with coefficients in L. Since L is algebraic over F, so are all the coefficients of this polynomial. Denote F' the extension of F spanned by those coefficients. It is finite, and $F'[\alpha]/F'$ is finite too. By telescopic base, $F'[\alpha]/F$ is finite, and so α is algebraic over F.

Proposition : Spanned Extensions and Algebraicity

Let K/F be a field extension, and S be a set of elements of K, algebraic over F. Then $F(S)/F$ is algebraic.

Proof : Using once again that $\cup_{x \text{ finite }, x \subset S} F(x)$, every element of $F(S)$ is contained in an $F(x)$ which is generated by a finite number of algebraic elements, and is thus algebraic thanks to transitivity.

This also allows us to complete our propositions on composite extensions.

Proposition : Properties of Composite Extensions, part 2

Let $F \subset L_1, L_2 \subset K$ be fields. Then :

1. L_1L_2/F is finite if and only if L_1/F and L_2/F are finite. Moreover, we have $[L_1L_2 : F] \leq [L_1 : F][L_2 : F]$.
2. L_1L_2/F is algebraic if and only if L_1/F and L_2/F are finite.

If L_1L_2/F are finite clearly L_1/F and L_2/F are finite. Conversely, we then have $L_1 = F(a_1, ..., a_n)$ and $L_2 = F(b_1, ..., b_n)$ where all are algebraic. Thus $L_1L_2 = F(a_1, ..., a_n, b_1, ..., b_n)$ is finitely generated by algebraic elements so it is finite.

For the bound (from the first part of the statement, a proof need only be given when all degrees are finite), see that $[L_1L_2 : L_2] \leq [L_1 : F]$: indeed, if $L_1 = F(1, x_1, ..., x_n)$, $L_1L_2 = L_2(1, x_1, ..., x_n)$ (it is an extension which contains L_2 and F, and is clearly the smallest so). Now see that $[L_1L_2 : F]^2 = [L_1 : F][L_2 : F][L_1L_2 : L_1][L_1L_2 : L_2]$.

For the second fact, clearly if L_1L_2/F is then all of its subextensions are too. Then if L_1/F and L_2/F are algebraic, then $L_1L_2 = F(L_1, L_2)$, but both L_1 and L_2 are algebraic over F.

Let us now understand the concept of splitting fields.

4.1.4 Splitting Fields

As its name suggests, here is a definition of a splitting field of a polynomial $f \in F[x]$, where F is a field.

Definition : Splitting Field

A **splitting field** of a polynomial $f \in F[x]$ is an extension K such that f is split over K and if $\alpha_1, ..., \alpha_n$ are the roots of f in K, then $K = F(\alpha_1, ..., \alpha_n)$.

A **splitting field** of a set S of polynomials $F[x]$ is an extension K such that every polynomial $f \in S$ is split over K and if K is generated by the roots in K of the polynomials $f \in S$.

We might firstly wonder if such fields even exists. Good news : they do.

Proposition : Existence of Fields over which a Polynomial Splits

Let $f \in F[x]$. There is a finite extension K of F such that $[K : F] \leq n$ and f has a root in $K[x]$. Moreover, there is an extension K' of F with $[K' : F] \leq n!$ over which f splits.

Proof : for the first result, let p be an irreducible factor of f. If p is of degree 1, f has a root. If p is not of degree 1, consider $F[x]/p$. It is a field extension of f of degree lower than n, and $f([x]) = 0$ in this field. So all good. For the next part, we proceed by induction. For f of degree 1, nothing to show (already split). If it is shown for degree n and f is of degree $n + 1$, then take an extension of degree $\leq n + 1$ where f has a root and use induction on the remaining factor.

Proposition : Splitting Fields for Finite Sets of Polynomials

Let $f_1, ..., f_n$ be a finite set of polynomials in $F[x]$. Then there is a splitting field of $f_1, ..., f_n$.

Proof : if there is only one polynomial, take a field over which f splits completely, and take only the extension by the roots of f. It is easy to show by induction that a polynomial splits over a field if and only if all of its roots are in this field, which concludes. Do the same for more polynomials, or for the product of those polynomials (and prove in your head through the property of factorial rings why if a polynomial splits, all of the factors also split).

Now two natural questions arise.

- Can we upgrade this definition for arbitrary set of polynomials ?
- Are splitting fields unique up to isomorphism ?

Both of the answers are yes, which we will explore in the next two sections.

4.1.5 Algebraic Closures

Definition : Algebraically Closed Field and Algebraic Closure

Let K be a field. K is said to be **algebraically closed** if it follows one of the equivalent following properties :

- K has no non-trivial finite / algebraic extension.
- Every polynomial in $K[x]$ splits completely / has a root in K / every irreducible polynomial is degree 1.

If K/F is an algebraic extension such that K is algebraically closed, then K is called an **algebraic closure** of F.

Verification : the equivalences on one line are head exercises. That $1 \implies 2$ is the fact that every polynomial splits in an algebraic extension. So if all such extensions are trivial, all polynomials split. For $2 \implies 1$, this is simply because a non-trivial finite extension implies an extension by an irreducible polynomial, which is necessarily trivial if we suppose 2.

Exercise : Algebraic Closure of $\mathbb{Q}$ ***

Let $\overline{\mathbb{Q}} = \{a \in \mathbb{C}, a \text{ is algebraic over } \mathbb{Q}\}$. Prove that $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$.

It is an algebraic extension by definition. Let's prove that $\overline{\mathbb{Q}}$ is algebraically closed : if $p \in \overline{\mathbb{Q}}[x]$, then denote L the extension of $\mathbb{Q}$ spanned by the coefficients of p. It is finite. The roots in $\mathbb{C}$ of p are algebraic over L, and since L is algebraic over $\mathbb{Q}$ then the roots are algebraic over $\mathbb{Q}$. So its roots are in $\overline{\mathbb{Q}}$. This method proves more generally that an algebraic extension of any field F that splits every polynomial in $F[x]$ is algebraically closed.

Exercise : Algebraically Closed Fields are Infinite ***

Let K be an algebraically closed field. Prove that K is infinite.

Solution : If K were finite, prove that for a certain n there are more polynomials of degree n in $K[x]$ than split polynomials (the main reason being that for all $k \in \mathbb{N}$, $\binom{n+k+1}{n-1} = \frac{(n+k-1)!}{(n-1)!k!} << k^n$).

It is interesting to prove, yet not very enlightening in regards to Galois theory, the following result :

Theorem : Existence of an Algebraic Closure

Every field F has an algebraic closure.

Proof : not included in this version, but uses Zorn's lemma somewhere.

Proposition : Consequences of the Existence of an Algebraic Closure

- Any set of non constant polynomials has a splitting field.
- The splitting field of the set of all nonconstant polynomials over F is an algebraic closure of F.

Proof : the two are easy. For the first one, take $F(X)$ with X the roots of those elements in an algebraic closure. Note that this argument could not have been used before proving there existed an algebraic closure, since we didn't know there existed a field that contained the roots of an arbitrary set of polynomials. For the second one it is the same argument than for a previous exercise about the roots of $\overline{\mathbb{Q}}$.

So now, we know that we can split all the polynomials we want, if we're ready to consider extensions large enough. But as for splitting fields, what about the "uniqueness" of an algebraic closure ? We must turn to field morphisms more generally.

4.1.6 The Isomorphism Extension Theorem

Remember that a field morphism with domain K is necessarily injective, since it must send K^* to K^* and thus must not kill any element which is not 0.

But there is much more to be said about field morphisms : actually, this is what Galois Theory is about. Through the following propositions we will show a super important property: the isomorphism extension theorem. The starting point is the following observation.

Proposition : A First Lemma for the Isomorphism Extension Theorem

Let $\sigma : F \to F'$ be a field isomorphism. Let $f \in F[x]$ be irreducible and denote $f' = \sigma(f) \in F'$. Let α be a root of F in some extension K of F and α' be a root of f' in some extension K' of F'. Then there is a field isomorphism $F(\alpha) \to F'(\alpha')$ that coincides with σ on F and that sends α to α'.

Proof : Prove that σ extends to an isomorphism $F[x]/f(x) \simeq F'[x]/f'(x)$. Then prove that there is an F isomorphism $F[x]/f(x) \simeq F(\alpha)$ and same with F'.

Theorem : The Isomorphism Extension Theorem

- Let $\sigma : F \to F'$ be a field isomorphism, f be a polynomial in $F[x]$, let K be a splitting field of f over F and K' be a splitting field of $\sigma(f)$ over F'. Then σ extends to an isomorphism $\tau : K \to K'$. Additionally, for any $\alpha \in K$, and α' a root of $\sigma(\min(F, \alpha))$ in K', then τ can be chosen to send $\alpha \mapsto \alpha'$.
- The same theorem also stands if you replace K and K' by splitting fields of S and $\sigma(S)$ where S is an arbitrary set of polynomials in $F[x]$.

Proof : We will prove the first case : the second one is the same but with Zorn's lemma. If f is split over F then of course its image is split over F', then $K = F$, $K' = F'$ and there's nothing to prove. If f is not split, then apply the former theorem to an irreducible factor of f, to extend σ to an isomorphism $K \supset F[\alpha] \simeq F'[\alpha'] \subset K'$ where f has one more root. Keep on doing so until f is split : you will obtain an isomorphism between splitting fields of f over F contained in K and of $\sigma(f)$ over F' contained in K'. Both must then be K and K' respectively by definition of splitting fields.

This theorem has great corollaries, in particular the one we expected all along.

Proposition : Uniqueness of Splitting Fields

Let S be an arbitrary set of polynomials in $F[x]$. Two splitting fields of S over F are F-isomorphic. In particular, this is true for algebraic closures.

Proof : this is just applying the former theorem to extend $\boldsymbol{id} : F \to F$. For algebraic closures, then S must just the set of all polynomials with coefficients in F.

Here's the second important corollary.

Proposition : Embedding of Algebraic Extensions in an Algebraic Closure

Let K/F be an algebraic extension of F and N be an algebraic closure of F. Then K is F-isomorphic to a subfield of N.

Proof : Consider an algebraic closure N' of K. Then of course it is also an algebraic closure of F. Then N' and N are F-isomorphic. The restriction of this isomorphism to K suffices.

Exercise : What the Isomorphism Extension Theorem does NOT say ***

1. Find fields $F \subset K$ and an isomorphism $F \to F$ that cannot be extended to an isomorphism $K \to K$.
2. Let M be an extension of F, α and α' distinct roots of $\min(\alpha, F)$ and β, β' distinct roots of $\min(\beta, F)$, such that $\alpha, \alpha', \beta, \beta'$ are in M and $\alpha \neq \beta$. Prove that there is not always an F-automorphism of M that sends $\alpha \to \alpha'$ and $\beta \to \beta'$.

Solution : consider $F = \mathbb{Q}(\sqrt{2})$ and $K = \mathbb{Q}(2^{\frac{1}{4}})$. Consider the isomorphism that sends $\sqrt{2} \to -\sqrt{2}$. An automorphism of $\mathbb{Q}(2^{\frac{1}{4}})$ sends $\mathbb{Q}$ to $\mathbb{Q}$ so sends $2^{\frac{1}{4}}$ to another real root of $X^4 - 2$. The only possibility is $-2^{\frac{1}{4}}$. But in this case $\sqrt{2}$ is necessarily sent to itself. The second exercise has the same solution for $2^{\frac{1}{4}} \mapsto -2^{\frac{1}{4}}$ and $\sqrt{2} \mapsto -\sqrt{2}$. Notice that it works for the third example too.

4.2 Galois Theory

After this first course in field theory, let's now move on to Galois Theory properly speaking. We firstly have to introduce two important notions : normality and separability.

4.2.1 Normality

Definition : Normal Extensions

A field extension K/F is said to be **normal** if it is algebraic and satisfies one of the following equivalent properties :

- For any irreducible $f \in F[x]$, if f has a root in K then f splits completely over K.
- K is the splitting field of a set of polynomials over F.

Verifications : $1 \implies 2$ *: if* K/F *verifies this property, then* K *is the splitting field of all the polynomials of the* $\min(\alpha, F)$ *for* $\alpha \in K$*. Indeed,* K *splits all those polynomials so contains their splitting field, and every element of* K *is a root of one of those polynomials since the extension is algebraic.* $2 \implies 1$ *is more difficult : suppose we have* 2 *and let* f *be a polynomial in* $F[x]$*. Suppose that* f *is irreducible over* F *and has a root* $\alpha \in K$*, and let* N *be an algebraic closure of* K*. Then for any other root* α' *of* f *in* N*, then there is an isomorphism* $N \supset F[\alpha] \simeq_F F[\alpha'] \subset N$ *which extends to an isomorphism* $N \to N$*. However, since* K *is a splitting field of a set of polynomials with coefficients in* F*, hence* K *is generated by roots of polynomials and thus its image under any* F*-automorphism of* N *is* K *itself. Thus* $F[\alpha'] \subset K$ *and hence our theorem is proven.*

In a sense that will be made more precise later, a "normal" extension in an algebraic closure should be thought of just like a "normal" subgroup. Indeed, a normal subgroup $H \subset G$ is a subgroup which is invariant under conjugation. Similarly, a normal extension $F \subset K \subset N$ where N is an algebraic closure of K, can be characterized by its invariance under F-automorphism of N.

Exercise : Another Characterization of Normal Extensions **

Justify the claim above : let K/F be an algebraic extension and let N be an algebraic closure of K. Choose an embedding $K \hookrightarrow N$ so that K and F can be seen as sub-extensions of N. Then K/F is normal if and only if for any F-automorphism of K, σ, $\sigma(K) \subset K$. Moreover prove that if this is the case then we even have $\sigma(K) = K$.

Solution : If the extension is normal we clearly have $\sigma(K) \subset K$ *and even equality, since any subset of roots of a finite number of polynomials is injectively permuted by an* F*-automorphism. Now if* $\sigma(K) \subset K$ *for all* F*-automorphism, following the proof above we get that if an irreducible polynomial over* F *has a root then all the other roots must also be in* K*.*

What the above exercise essentially says is that normal extensions are extensions where the isomorphism extension theorem actually works.

Proposition : The Isomorphism Extension Theorem For Normal Extensions

Let K/F and be a normal extension. Let $F \subset L, L' \subset K$ be fields and give an F-isomorphism $L \to L'$. Then this isomorphism extends to an F-isomorphism of K.

Proof : embed K into an algebraic closure N. By the isomorphism extension theorem, the F-isomorphism $L \to L'$ extends to an isomorphism of N, which by the former exercise sends K to itself. So restriction of this isomorphism to K is an automorphism of K which extends our original isomorphism $L \to L'$.

As with any property we define for field extensions, there are two checks to make : how does normality behave in terms of transitivity and in terms of composites ? For transitivity, things do not go too well.

Proposition : Transitivity of Normality

Let $F \subset L \subset K$ be a tower of extensions. If K/F is normal then K/L is normal but L/F is not necessarily normal. Also, K/L and L/F may be normal, but K/F need not be normal.

Proof : If K/F is normal, then clearly every irreducible polynomial with coefficients in L that has a root α in K divides the minimal polynomial of α over F, which splits completely over K by normality of K/F. Then it has to split completely over K. For counterexamples, check that $\mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q}$ is not normal although $\mathbb{Q}(2^{\frac{1}{4}}, i)/\mathbb{Q}$ is. Also check that in the tower $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(2^{\frac{1}{4}})$ each intermediary extension is normal (because of degree 2).

For composites, things do not go quite better.

Proposition : Normality and Composites

Let $F \subset L_1, L_2 \subset K$ be extensions. If L_1/F and L_2/F are normal, then L_1L_2/F is normal. Other obvious transitivity properties are false.

Proof : if L_1 and L_2 are splitting fields of F-polynomials sets S_1 and S_2, then L_1L_2 is obviously the splitting field of $S_1 \cup S_2$. For the others property, if L_1L_2/F is normal we may have one of the two components not normal or even the two not normal (can you find one ?).

We also have a notion of "normal closure" for any algebraic extension.

Definition : Normal Closure of an Extension

Let K/F be an algebraic field extension. The normal closure of K/F is the splitting field of all polynomials $\min(\alpha, F)$ with $\alpha \in K$.

Here are some easy properties of normal closures.

Proposition : Some Properties of the Normal Closure

Let N denote the normal closure of K/F. Then :

- N is a minimal normal extension of F containing K.
- If $K = F(a_1, ..., a_n)$, then N is the splitting field over F of $\min(a_1, F), ..., \min(a_n, F)$.
- If K/F is finite then N/F is finite.

Proof : you should handle those proofs as exercises. For the first one, N is clearly normal (splitting field) and any normal extension containing K splits all minimal polynomials so contains N. For the second one, the proposed extension is clearly normal (it is a splitting field) and is a smallest normal extension containing all those elements and thus K. For the third, apply the one above since a finite extension is generated by a finite number of algebraic elements.

The normal closure is characterized by the first of the properties above.

Proposition : Characterization of the Normal Closure

Two normal closures of an algebraic field extension are F-isomorphic.

Proof : apply the isomorphism extension theorem from the identity of F to $N \to N'$ (which are splitting fields of a given set of polynomials). Since N' is a smallest normal extension containing F, and that $\sigma(N)$ is normal over F (splitting field of polynomials) then $\sigma(N) = N'$, which yields the isomorphism.

4.2.2 Separability

Definition : Separable Polynomial, Separable Element, Separable Extension

Let K/F be an algebraic field extension.

- An irreducible polynomial $f \in F[x]$ is said to be **separable over** F if it has no repeated roots over any splitting field of f / any extension of F. A polynomial is said to be separable if all of its factors are separable.
- An element $\alpha \in K$ is said to be **separable over** F if $\min(F, \alpha)$ is separable over F.
- An extension K/F is said to be **separable** if all the elements of K are separable over F.

This definition may be a little confusing at first. The first reason is that one may at first think that whether or not a polynomial has repeated roots may depend on the splitting field, but this cannot be true : indeed, if a polynomial has no repeated roots in one of its splitting fields, it is the case in any other splitting field since they all are isomorphic (similarly for repeated roots). The second reason why this may be confusing is the lack of examples. Separable polynomials are the "norm", in some way. For example, the polynomial $X^2 - 2$ is separable over $\mathbb{Q}$, since it splits in $\mathbb{Q}[\sqrt{2}]$ as $(X - \sqrt{2})(X + \sqrt{2})$ which has distinct roots.

But inseparable polynomials also happen. Let k be a field of characteristic p, and consider the field extension $k(x)/k(x^p)$. The polynomial $X^p - x^p$ is irreducible over $k(x^p)$ by Eisenstein's criterion. However, in $k(x)$ it splits as $(X - x)^p$ which has repeated roots in $k(x)$. Here's a criterion to easily check whether or not a polynomial is separable or not.

Proposition : Criterion for Separability

Let $f \in F[x]$. Then f is separable over F if and only if $\gcd(f, f') = 1$ in $F[x]$.

Proof : If this is true in $F[x]$, the equality also holds in any extension $K[x]$, so f and f' have no common roots so f has no repeated root. If f and f' do not have any common roots in any extension, then in a splitting field of both of them (denoted K) we have $\gcd(f, f') = 1$. A common divisor of f and f' in $F[x]$ must divide 1 in $K[x]$, so it must be 1.

This directly yields that there are some fields in which inseparability just does not happen, and allows us to describe inseparable polynomials very easily.

Definition : Perfect Fields

A field F is called **perfect** if all algebraic extensions of F are separable.

Proposition : Inseparability in Characteristic 0

Fields of characteristic zero are perfect fields.

Proof : Irreducibles are all of degree > 2 *and so have non constant derivatives. They are coprime with their derivative (because they are irreducible), so no repeated roots.*

Proposition : Separability and Perfectness in Characteristic $p > 0$

Let F be a field of characteristic p.

1. An irreducible polynomial f is inseparable $\iff f'(x) = 0, \iff f$ is of the form $g(x^{p^r})$ for some $r \in \mathbb{N}$ and a separable irreducible polynomial g.
2. F is perfect $\iff F^p = F$.

Proof : It is evident that $f'(x) = 0 \iff f(x) = h(x^p)$.

If $f'(x) = 0$ *then the polynomial is of the form* $f(x^p)$. *In an algebraic closure it is of the form* $\prod(x^p - b_i) = \prod(x - a_i)^p$ *where* $a_i^p = b_i$. *So it is not separable. If* $f'(x) \neq 0$, *then by the same argument that in the zero characteristic case, it is separable.*

If f *is of the form* $g(x^{p^r})$ *clearly it is not separable. If* f *is not separable, take the greatest* r *such that you can write* $f = g(x^{p^r})$. g *has to be irreducible or else* f *would not be, and* g *is not in* $F[x^p]$ *by maximality of* r.

Now if $F^p = F$, *then* $F[x^p] = (F[x])^p$ *so no polynomial in here is irreducible. If* F *is perfect, in the right splitting field* $x^p - a$ *factors as* $(x - b)^p$. *By separability all the* F*-irreducible factors of* $x^p - a$ *have to be separable, so they have to be of degree* 1. *So* $b \in F$ *and* $F^p = F$.

This proves that finite fields are perfect because Frobenius is a field homomorphism thus it is injective and thus surjective.

So now, we have settled the case for when inseparability happens or not : it can only happen on fields of characteristic p in which there are elements which do not have a p^{th}-root. In particular, they must be infinite.

A few lemmas to start with :

Proposition : Properties of Separable Polynomials

- If $g|f$ and f separable, then g separable.
- If f_1, f_2 are separable then $f_1 f_2$ is.
- If f is separable over F, then f is separable over any extension of F.

Proof : For the first one, irreducible factors of g *are factors of* f. *For the second one, factors of* $f_1 f_2$ *are the factors of* f_1 *and* f_2. *For the third one, say* f *is separable over* F. *If an irreducible polynomial* f *is not separable over* $K \supset F$, *then there is a splitting field of* f *over* K *where* f *has repeated roots. But this contains a splitting field of* f *over* F, *where it should have repeated roots, nonsense. Alternatively : notice that any irreducible factor of* f *over* K *divides at least one of the irreducible factors of* f *over* F *(take minimal polynomial) but those have no repeated roots...*

Before proving anything about separability, we need an important number, which quantifies in some way the separability of a given element over a field.

Definition : Separable Degree

Let F be a field and N be an algebraic closure of F. We define the **separable degree of** $\alpha \in N$ as the number $|\mathbf{Hom}_F(F(\alpha), N)|$. More generally, we define the separable degree of an algebraic field extension L/K as the number $|\mathbf{Hom}_K(L, N)|$ (N being an algebraic closure of K).

This number has important properties, which justifies its name.

Proposition : Properties of the Separable Degree

Let $F \subset L \subset K$ be a tower of algebraic extensions. Then we have the following properties :

- $|\mathbf{Hom}_F(K, N)| = |\mathbf{Hom}_L(K, N)| \cdot |\mathbf{Hom}_F(L, N)|$
- $|\mathbf{Hom}_F(K, N)| \leq [K : F]$.
- If K/F is finite, then $|\mathbf{Hom}_F(K, N)| = [K : F]$ if and only if the extension K/F is separable.

Proof : the first property requires a bit of work. We will describe a bijection between the set $|\boldsymbol{Hom}_F(K, N)|$ and the product $|\boldsymbol{Hom}_L(K, N)| \times |\boldsymbol{Hom}_F(L, N)|$. To do so, for each element of $|\boldsymbol{Hom}_F(K, N)|$, one easily obtains by restriction a unique element of $|\boldsymbol{Hom}_F(L, N)|$ and an element of $|\boldsymbol{Hom}_{L\to\sigma(L)}(K, N)|$, which is an element of $|\boldsymbol{Hom}_F(K, N)|$ which sends $L \to \sigma(L)$.

Now define an equivalence relation on the elements of $|\boldsymbol{Hom}_F(K, N)|$ by $\sigma \simeq \sigma' \iff \sigma|_L = \sigma'|_L$. For each of the classes, using the axiom of choice, choose an extension $\tilde{\sigma}$ of the mapping $\sigma(L) \to L$ to an isomorphism $N \to N$. For each σ' in the class of σ, one obtains by post-composition by $\tilde{\sigma}$ a bijection $|\boldsymbol{Hom}_{L\to\sigma(L)}(K, N)| \simeq |\boldsymbol{Hom}_L(K, N)|$. We have thus described a mapping $|\boldsymbol{Hom}_F(K, N)| \to |\boldsymbol{Hom}_L(K, N)| \times |\boldsymbol{Hom}_F(L, N)|$. It is injective, since if σ and σ' are the same on L then the second component is obtained by composition by the same isomorphism, and thus this forces $\sigma = \sigma'$. It is also surjective, since any element of the product σ, τ is obtained by taking the element of $\boldsymbol{Hom}_F(K, N)$ defined by considering the class of τ in $\boldsymbol{Hom}(K, N)$, and considering a pre-image of σ through the bijection $|\boldsymbol{Hom}_{L\to\tau(L)}(K, N)| \simeq |\boldsymbol{Hom}_L(K, N)|$.

To obtain the second property, it is evident for an extension of the form $F(\alpha)/F$ since the only choices for α are the roots of $\min(F, \alpha)$ which are in number lower than $[F(\alpha) : F]$. It is obtained in globality by basic induction on the number of generators using the property above.

To obtain the third property, first of all see that for an element $\alpha \in K$, α is separable if and only if $|\boldsymbol{Hom}_F(F(\alpha), N)| = [F(\alpha) : F]$ (this is an easy consequence of the isomorphism extension theorem). Now if K/F is finite and separable, write $K = F(\alpha_1, ..., \alpha_n)$. We have $[K : F] = [L_n : L_{n-1}][L_{n-1} : L_{n-2}]...[L_1 : L_0]$ where $L_i = F(\alpha_1, ..., \alpha_i)$ and $L_0 = F$. Since each of those extension is done by a separable element we have equality with the hom sets, and then use the multiplicativity of the hom sets.

Conversely, if this equality is verified, for all elements $x \in K$ we have $[K : F] = [K : F(x)][F(x) : F] = |\boldsymbol{Hom}_{F(x)}(K, N)| \cdot |\boldsymbol{Hom}_F(F(x), N)|$. Since each element of both products are inferior or equal to the other, there must be equality $[F(x) : F] = |\boldsymbol{Hom}_F(F(x), N)|$.

This proof allows us to derive nice properties of separability, regarding extensions, transitivity and composition.

Proposition : Extensions by Separable Elements

Suppose K/F is a field extension and S is a subset of K of elements separable over F. Then $F(S)/F$ is separable.

Proof : remember that $F(S)/F$ is just the field of polynomial images in element of F, and thus we just need to prove that $F(s)/F$ where $s \subset S$ is separable. But this has been done in the penultimate paragraph of the last proof.

Separability behaves better than normality in terms of transitivity.

Proposition : Transitivity of Separability

Let $F \subset L \subset K$ be a tower of algebraic extensions. Then K/F is separable if and only if K/L and L/F are.

Proof : Remember that algebraicity is already transitive. Suppose K/F is separable. Then every irreducible polynomial over L divides an irreducible polynomial over F, which is separable over K. So it must be separable over K. Thus K/L must be separable. Now if a polynomial is separable over F, then it is separable over any extension of F, including L and K. So L/F is separable. Now suppose K/L and L/F are separable. Then for all $x \in K$, consider the minimal polynomial $\min(x, L)$. It has simple roots. The finite extension of F by the coefficients of $\min(x, L)$ is thus separable, and x is separable over this extension. But an extension by successive separable elements is separable by proofs above, and thus the extension $F(x)/F$ is separable as a subextension of a separable extension. This proves that K/F is separable.

It also behaves well in terms of composition.

Proposition : Separability and Composition

Let $F \subset L_1, L_2 \subset L$ be fields. Then L_1/F and L_2/F are separable if and only if L_1L_2/F is separable.

Proof : nothing to prove in terms of algebraicity. If L_1L_2/F are separable then L_1/F and L_2/F are as subextensions, and if both are then $L_1(L_2)/L_1$ is separable since the elements of L_2 are separable over F and thus over L_1. So by transitivity L_1L_2/F is separable.

Finally, as with normality, we also have a notion of closure.

Definition : Separable Closure

Let K/F be an algebraic field extension. Then the set $S = \{x \in K, x \text{ separable over } F\}$ is a field, called the **separable closure** of F in S. It is a maximal separable extension of F contained in K.

Verifications : From what we have proven above, this is clearly a field since α, β are separable over F, then the field extension $F(\alpha, \beta)/F$ is separable as a composition of separable extensions. Clearly it also is a maximal separable subextension of K/F by transitivity.

4.2.3 Objects of Galois Theory

We now introduce the main objects of Galois theory, with first of all the Galois group of an arbitrary extension.

Definition : Galois Group of a Field Extension

Let K/F be a field extension. The **Galois group** of the extension K/F, denoted $\mathbf{Gal}(K/F)$, is the group of field automorphisms of K/F that are the identity on F.

Note that two field morphisms coincide on a generating set they coincide everywhere. For obvious reasons, any $\sigma \in \mathbf{Gal}(K/F)$ permutes the roots of polynomials with coefficients in K (of minimal polynomials in particular). This allows us to say that for a finite extension the Galois Group is finite : the generators of the extension can only be sent to a finite number of points.

Exercise : Some Computations **

Compute the following Galois Groups :

1. $\mathbf{Gal}(\mathbb{C}/\mathbb{R})$
2. $\mathbf{Gal}(\mathbb{Q}(2^{\frac{1}{3}})/\mathbb{Q})$
3. $\mathbf{Gal}(\mathbb{F}_2(t)/\mathbb{F}_2(t^2))$
4. $\mathbf{Gal}((\mathbb{F}_2(t)/(1+t+t^2))/\mathbb{F}_2)$

*Solution : first one is $\mathbb{Z}/2$ because sends i to i or $-i$. Second one is **Id** because otherwise complex numbers. The third one is **Id**, since the minimal polynomial of t over $\mathbb{F}_2(t^2)$ is $X^2 - t^2 = (X-t)^2$, which has just one root. The fourth one is obtained by factoring (X^2+X+1) in this new field which yields $(X+t)(X+1+t)$ and noticing that we still have a homomorphism.*

Note that it is easy to retrieve subfields from subgroups H of the Galois Group : just take the subfield of fixed elements under H. This association can be written $H \mapsto \mathcal{F}(H)$. Reciprocally, if $F \subset L \subset K$ is an intermediate extension, we can write $\mathbf{Gal}(K/L)$ for the subgroup of $\mathbf{Gal}(K/F)$ that fixes L pointwise. Those maps are the central objects of Galois theory : they relate subgroups of the Galois group and subfields of the field extension. We have the following propositions:

Proposition : Properties of $\mathcal{F}$ and $\mathbf{Gal}(K/\cdot)$

- Both of those maps are decreasing.
- $\mathcal{F} \circ \mathbf{Gal}(K/\cdot)$ and $\mathbf{Gal}(K/\mathcal{F}(\cdot))$ are greater than identity.
- For all subgroup $H \subset \mathbf{Gal}(K/F)$, we have $\mathcal{F}(\mathbf{Gal}(K/\mathcal{F}(H))) = \mathcal{F}(H)$.
- For all subfield L such that $F \subset L \subset K$, we have $\mathbf{Gal}(K/L) = \mathbf{Gal}(K/\mathcal{F}(\mathbf{Gal}(K/L)))$.

Proof : the first one is a joke, the second one too. The two after take one minute each to know what they mean but are ultimately very simple.

So what this says is that if you have applied $\mathcal{F}$, then the composition $\mathcal{F} \circ \mathbf{Gal}(K/\cdot)$ is identity, and the other way around if you already applied $\mathbf{Gal}(K/\cdot)$. So we have a one to one correspondance between the subfields of the form $\mathcal{F}(H)$ and the subgroups of the form $\mathbf{Gal}(K/L)$. Our main question is the following : when does $L \mapsto \mathbf{Gal}(K/L)$ **achieve a correspondance between subgroups and subfields** ?

This is a question which will be answered in the next section. First of all, let's give a first result on the cardinal of the Galois group.

Proposition : Cardinal of the Galois Group

Let K/F be a finite field extension. then $|\mathbf{Gal}(K/F)| \leq [K:F]$.

Proof : this result can easily be obtained through the fact that we have an injection $\boldsymbol{Gal}(K/F) \to \boldsymbol{Hom}(K,N)$, where N is an algebraic closure of K, by postcomposing any element of $\boldsymbol{Gal}(K/F)$ with an inclusion of $K \to N$. It is also classically obtained through the theorem of linear independence of characters.

4.2.4 The Fundamental Theorem of Galois Theory

In this section, we define Galois extensions and prove that they follow the fundamental relation we want them to follow.

Definition : Galois Extension

Let K/F be an algebraic field extension. K/F is said to be **Galois** if it follows one of the two equivalent properties :

- K/F is normal and separable.
- $\mathcal{F}(\mathbf{Gal}(K/F)) = F$.

Verifications : if K/F is normal and separable, let x be not in F. Then x has a conjugate over F which is in K by normality, denoted y. There is an F-isomorphism $F(x) \to F(y)$ which sends x to y. Then use the isomorphism extension theorem for normal extensions.

Conversely, if $\mathcal{F}(\boldsymbol{Gal}(K/F)) = F$, then for any element $x \in K$, then the set $S_x = \{\sigma(x), \sigma \in \boldsymbol{Gal}(K/F)\} \subset K$ is finite since x can only be sent to roots of the minimal polynomial of x over F which are in finite number. Then consider the polynomial $\prod_{u \in S_x}(X - u)$. We easily verify that its coefficients are stable under $\boldsymbol{Gal}(K/F)$ since they are symmetric polynomials in the elements of S_x which $\boldsymbol{Gal}(K/F)$ permutes. It is clearly separable, and has all its roots in K, which proves that K/F is normal and separable.

In the finite case, which is the one we will focus on at the moment, we have another characterization of Galois extensions.

Proposition : Characterization of Galois-ness in the Finite Case

Let K/F be a finite field extension. Then K/F is Galois if and only if $|\mathbf{Gal}(K/F)| = [K : F]$.

Proof : If an extension is normal and separable, we have an inclusion $\boldsymbol{Gal}(K/F) \to \boldsymbol{Hom}_F(K, N)$, and by finiteness and separability, an equality $|\boldsymbol{Hom}_F(K, N)| = [K : F]$. Now because the extension K/F is normal, then this inclusion $\boldsymbol{Gal}(K/F) \to \boldsymbol{Hom}_F(K, N)$ actually is a bijection : indeed, any element of $\boldsymbol{Hom}_F(K, N)$ sends K to itself, so by restriction we have an inverse injection $\boldsymbol{Hom}_F(K, N) \to \boldsymbol{Gal}(K/F)$. This proves the equality of cardinals. Conversely, if we have this equality, then this forces $|\boldsymbol{Hom}_F(K, N)| = [K : F]$ so the extension is separable. Moreover, it forces normality since every element of $\boldsymbol{Hom}_F(K, N)$ send K to itself, and so do all those morphisms which sends elements to their conjugates.

This allows us to prove a quite subtle point which will be central to the following proof.

Proposition : Certain Galois Extensions

Let G be a finite group of automorphisms of K. Then the extension $K/\mathcal{F}(G)$ is Galois, has Galois group G and is finite of degree $|G|$.

Proof : that it is Galois simply comes from the equality $\mathcal{F}(\boldsymbol{Gal}(K/\mathcal{F}(G))) = \mathcal{F}(G)$. Then we clearly have $G \subset \boldsymbol{Gal}(K/\mathcal{F}(G))$ and $|\boldsymbol{Gal}(K/\mathcal{F}(G))| = [K : \mathcal{F}(G)]$. All we have to prove is that $[K : \mathcal{F}(G)] \leq |G| = n$. Suppose it is greater. Take elements $\alpha_1, ..., \alpha_{n+1}$ of K which are linearly independent over $\mathcal{F}(G)$. Then the matrix $(g_i(\alpha_j))_{1 \leq i \leq n, 1 \leq j \leq n+1}$ has linearly dependent lines over K, and can thus be arranged to obtain a minimal linear combination $\sum_{j=1}^{k} c_j g_i(\alpha_j)$ for i between 1 and n, with $c_j \in K$. We can say $c_1 = 1$. If all the c_i are in $\mathcal{F}(G)$, then this yields $g_i(\sum_{j=1}^{k} c_j \alpha_j) = 0 \implies \sum_{j=1}^{k} c_j \alpha_j = 0$,

which leads to a contradiction. Now for all $\sigma \in G$ we have $\sum_{j=1}^{k} \sigma(c_j) g_i(\alpha_j)$ by permutation. Now since $c_1 = 1$ and by minimality, substracting equalities yields $\sum_{j=1}^{k} (c_j - \sigma(c_j)) g_i(\alpha_j) = 0$ which breaks minimality and forces all the terms to be 0. Thus the c_j are fixed under G, which yields the contradiction.

This proof, to be remembered, is the *hard proof* of Galois theory. Notice that it essentially works because we are working with finite subgroups of the automorphisms of K : it would never otherwise. This will be the source of significant complications when studying infinite Galois extensions.

We can now state and prove the fundamental theorem of Galois theory.

Theorem : The Fundamental Theorem of Galois Theory (Finite Case)

Let K/F be a finite Galois extension. Then the maps $\mathcal{F}$ and $\mathbf{Gal}(K/\cdot)$ are inverse bijections from the set of subextensions of K/F to the set of subgroups of $\mathbf{Gal}(K/F)$.

Moreover, this map sends normal subgroups to Galois sub-extensions. In this case, the restriction morphism is well defined, $\mathbf{Gal}(K/F) \to \mathbf{Gal}(L/F)$, which leads to an exact sequence :

$$1 \to \mathbf{Gal}(K/L) \to \mathbf{Gal}(K/F) \to \mathbf{Gal}(L/F) \to 1$$

Proof : Firstly, we prove that $\mathcal{F}(\boldsymbol{Gal}(K/L)) = L$. As we have seen before, it contains L. Now for all element $x \in K$ not in L, since the extension K/L is still normal, one can use the isomorphism extension theorem to construct an L-isomorphism which sends x to one of its L-conjugates, and thus prove that it is not in $\mathcal{F}(\boldsymbol{Gal}(K/L))$.

We know that $\boldsymbol{Gal}(K/\mathcal{F}(H)) = H$ because H is a finite subgroup of the automorphisms of K.

It is elementary to prove that $\sigma\mathcal{F}(H) = \mathcal{F}(\sigma H \sigma^{-1})$. This implies that H is normal if and only if $\sigma\mathcal{F}(H) = \mathcal{F}(H)$ (thanks to the bijection we just exposed) for all $\sigma \in \boldsymbol{Gal}(K/F)$. But $\sigma(L) \subset L$ for all $\sigma \in \boldsymbol{Gal}(K/F)$ is equivalent to L/F being Galois (if it is Galois, this is clear, if it is so, then it must be Galois by extension theorem that switches the roots around).

And finally, about the quotient, this comes from the fact that restriction is now a homomorphism of $\boldsymbol{Gal}(K/F) \to \boldsymbol{Gal}(L/F)$, surjective, and of kernel $\boldsymbol{Gal}(K/L)$.

We will now try and convince you of how deep this theorem is by citing some of its most notable applications.

4.3 Applications of Galois Theory

4.3.1 The Primitive Element Theorem

We have a spent a good deal of time working with simple extensions, that is, extensions of the form $F(\alpha)/F$. It would be nice to know when a finite extension is indeed simple. Galois theory helps us answer this question. First of all, an important lemma.

Proposition : Characterization of Simple Extensions

An finite algebraic extension K/F is **simple** if and only if there are finitely many intermediate subfields $F \subset L \subset K$.

Proof : If F is infinite: if there is a finite number of subfields this is easy, because then K can be written as a finite union of $F(\alpha)/F$, and on an infinite field a finite union of vector spaces is a vector space if and only if one contains all of them (one element of the union contains infinitely many $(1, \lambda, ..., \lambda^n)$). If K/F is of the form $F(\alpha)/F$, Let M be an intermediate extension. Then $K = M(\alpha)$. Consider the minimal polynomial q of α over M and denote M_0 the field generated by the coefficients of q. $M_0 \subset M$ but $[K : M] \geq [K : M_0] = [K : M][M : M_0]$ which proves that $[M : M_0] = 1$ (the first inequality comes from the fact that $K = M(\alpha)$, so K is generated over M_0 by a polynomial of smaller degree than over M). Thus M is determined by the coefficients of q. But there are a finite number of divisors of p.

If F is finite, there are a finite number of subfields and also K^* is cyclic so just take him for a generator (proof with roots and exponent of a group).

Theorem : The Primitive Element Theorem

If K/F is finite and separable, then there is $\alpha \in K$ such that $K = F(\alpha)$. In characteristic 0, all finite extensions are thus simple.

Proof : If K/F is finite separable, it is a subextension of the normal closure of L/F where L is the normal closure of K over F which is normal, finite, and separable as an extension of K by separable elements (conjugates of generators of K/F which are all separable by hypotheses on K/F). Galois Theory (more precisely the fact that $\mathcal{F}(\boldsymbol{Gal}(L/M)) = M$ for all $F \subset M \subset L$) proves that all intermediate fields between K and F come from subgroups of $\boldsymbol{Gal}(L/M)$ which is finite. And since there are a finite number of subgroups, there are a finite number of subfields.

Note that this proof only requires a little bit of Galois theory, since it only uses the rather simple fact that $\mathcal{F}(\mathbf{Gal}(L/M)) = M$ for all $F \subset M \subset L$. Another way of proving the fundamental theorem of Galois theory would have been to prove this theorem first using this fact, and then working on a primitive element to obtain the lower bound $[K : \mathcal{F}(H)] \leq |H|$.

4.3.2 Symmetric Polynomials

Galois theory can also elegantly be used to find out which elements of $k(x_1, ..., x_n)$ are stable under S_n, where k is any field and S_n acts in the obvious way by permutation of the variables. We present this theorem as a small problem.

Exercise : The Fixed Field of S_n **

Define the usual action of S_n on $k(x_1, ..., x_n)$. Let $s_1, ..., s_n$ be the elementary symmetric polynomials. We wish to find the fixed field of S_n.

1. Let $f(t) = \prod(t - x_i) \in k(x_1, ..., x_n)[t]$. Prove that $f \in k(s_1, ..., s_n)[t]$.
2. Deduce that $k(x_1, ..., x_n)/k(s_1, ..., s_n)$ is Galois.
3. Prove that $[k(x_1, ..., x_n) : k(s_1, ..., s_n)] \geq n!$.
4. Prove that $[k(x_1, ..., x_n) : k(s_1, ..., s_n)] \leq n!$.
5. Conclude that $\mathbf{Gal}(k(x_1, ..., x_n)/k(s_1, ..., s_n)) = S_n$ and thus that the only elements of $k(x_1, ..., x_n)$ fixed under S_n are generated by the elementary symmetric polynomials $s_1, ..., s_n$.
6. For any finite group G, prove that there exists a finite Galois extension K/F with Galois group G.

Solution : First one is evident. Second one too : it is exactly the field generated by the roots. For the third one, a lower bound is given by Galois inequation : S_n injects into the Galois group. For the fourth one, an upper bound is given by splitting field inequation. For the fourth we thus know that this extension is Galois, of degree $n!$ so that its Galois group is exactly S_n. And so the base field is indeed the fixed field. The fifth point comes from the fact that any group is a subgroup of some S_n, and thus taking K/L where L is the fixed field of this subgroup is Galois and has the right Galois group.

4.4 Examples

This section of this document is dedicated to seeing Galois groups in action, in the context of some concrete field extensions.

4.4.1 Finite Fields

In this section, we make a complete survey of finite fields, their properties, and of course, shed light on the Galois theory that goes on here.

First of all, some observations.

Proposition : Some Properties of Finite Fields

- A finite field is of strictly positive, characteristic, which a prime number p. Additionnally, the cardinal of such a field must be a power of this prime number.
- If F is a finite field of cardinal p^m, then its elements are exactly the roots of the polynomial $X^{p^m} - X$.

Proof : Because of finiteness, the characteristic must be strictly positive, and because a field is a domain the characteristic must be a finite field. Such a field then contains the field $\mathbb{Z}/p\mathbb{Z}$, and must be a finite extension of this field. Its cardinal is thus a power of p.

Since the multiplicative group of F is of order $p^m - 1$, its elements make up $p^m - 1$ disctinct roots of the polynomial $X^{p^m} - X$, and thus all of them.

This is enough to prove the most fundamental fact about finite fields :

Theorem : Uniqueness of Finite Fields of a Certain Cardinal

Let p be a prime number and $n \in \mathbb{N}$, $\mathbb{N} \geq 1$. Then there exists exactly one finite field of cardinal p^n up to isomorphism. We usually denote it $\mathbb{F}_{p^n}$.

Proof of existence : Let N_p be an algebraic closure of the field $\mathbb{Z}/p$. The roots of the polynomial $X^{p^m} - X$ clearly forms an additive group (remember than in characteristic p, $x \mapsto x^p$ is additive), is stable under multiplication and inversion. So its roots form a field. Moreover, since the polynomial $X^{p^m} - X$ is separable, its roots are disctinct. So we do have a field of cardinal p^m. Let $\mathbb{F}_{p^m}$ denote this field.

Proof of uniqueness : Let F be a field of cardinal p^m. Since F is an algebraic closure of $\mathbb{Z}/p$, it can be embedded in N_p. However, since all elements of F are killed by the polynomial $X^{p^m} - X$, then they must also be so in N_p. So the embedding $F \to N_p$ sends $F \to \mathbb{F}_{p^m}$. Then for reasons of cardinal, this is an isomorphism.

Any finite field $\mathbb{F}_{p^n}$ of characteristic p has a chosen automorphism, namely the frobenius automorphism, denoted ϕ, which sends $x \to x^p$. This automorphism completely characterizes the Galois theory of finite fields, which is surprisingly simple.

Theorem : Galois Theory of Finite Fields

Let $\mathbb{F}_{p^n}$ be a finite field. Then, the following hold :

1. The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois.
2. ϕ is of order n in $\mathbf{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.
3. $\mathbf{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\phi\rangle \simeq \mathbb{Z}/n\mathbb{Z}$.

Proof : $\mathbb{F}_{p^n}/\mathbb{F}_p$ is separable since $\mathbb{F}_p$ is perfect. Additionnally, $\mathbb{F}_{p^n}$ $\mathbb{F}_p$-embeds itself into an algebraic closure N_p of $\mathbb{F}_p$ as the roots of the polynomial $X^{p^n} - X$. Thus any other $\mathbb{F}_p$-embedding of $\mathbb{F}_{p^n}$ into N_p verifies the same property and thus sends $\mathbb{F}_{p^n}$ to the same subfield (once an embedding $\mathbb{F}_p \to N_p$ is chosen, all extensions to $K \to N_p$ have the same domain). This characterizes normality.

ϕ's order divides n since all elements of $\mathbb{F}_{p^n}$ are roots of $X^{p^n} - X$. Now if ϕ's order was lower than n, then the elements of $\mathbb{F}_{p^n}$ would be the roots of $X^{p^k} - X$ with $k < n$. But $\mathbb{F}_{p^n}$ does not have enough elements.

Now the last property is easy : since $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois, then the cardinal of the Galois group is the same as the dimension, n. But $\langle\phi\rangle$ is already of cardinal n.

Now time to see Galois theory in practice : since we know that the subgroups of $\mathbb{Z}/n\mathbb{Z}$ are the $\mathbb{Z}/m\mathbb{Z}$ for $m|n$, we thus obtain for free the following fact :

Proposition : Subfields of $\mathbb{F}_{p^n}$

If p is a prime number and n is an integer greater than 1, the subfields of $\mathbb{F}_{p^n}$ are exactly given by the elements fixed by ϕ^m for $m|n$, namely the roots of the polynomial $X^{p^m} - X$ over $\mathbb{F}_p$. This field is $\mathbb{F}_{p^m}$.

Proof : this can be proven directly, but here can be proven as a direct application of the fundamental theorem of Galois theory.

So the algebraic closure of $\mathbb{F}_p$ can now explicitly be described.

Proposition : Structure of the Algebraic Closure of $\mathbb{F}_p$

An algebraic closure of $\mathbb{F}_p$ can be described as the inductive limit of the $\mathbb{F}_{p^n}$ for $n \in \mathbb{N}$, with respect to the inclusion arrows $\mathbb{F}_{p^m} \to \mathbb{F}_{p^n}$ if $m|n$.

Proof : this inductive limit is well defined since the composition of two inclusion arrows is clearly an inclusion arrows : the roots of $X^{p^m} - X$ are the same in $\mathbb{F}_{p^{nm}}$ than in $\mathbb{F}_{p^{n'm}}$. It is clearly a field. It contains $\mathbb{F}_p$. It is algebraically closed over $\mathbb{F}_p$ since it contains subfields isomorphic to $\mathbb{F}_{p^n}$ for all n. It is clearly algebraic over $\mathbb{F}_p$.

The same argument with the polynomial $X^{p^n} - X$ proves that this algebraic closure contains exactly one subfield isomorphic to $\mathbb{F}_{p^n}$ for all n.

Finite fields may seem deadly abstract : however, they aren't. Computers can work with finite fields, because they can be explicitly described, thanks to the following token.

Proposition : Explicit Description of Finite Fields

For every prime number p, and for every integer $n \geq 1$ there exists a polynomial of degree n, irreducible over $\mathbb{F}_p$. $\mathbb{F}_{p^n}$ may thus be concretely obtained as $\mathbb{F}_p[X]/(P)$ for P such a polynomial.

Proof : Consider the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$. It is Galois so primitive : $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$. Now consider the minimal polynomial of α over $\mathbb{F}_p$.

The proof we gave is not constructive. Explicitly finding irreducible polynomials over $\mathbb{F}_p$ is not an easy task theoretically. However, as the following exercise justifies, in practice irreducible polynomial over finite fields are fairly easy to find.

Exercise : Proportion of Irreducible Polynomials Over a Finite Field ****

Let $\mathbb{F}_q$ be a finite field. Prove that the proportion of polynomials in $\mathbb{F}_q[X]$ of degree n, irreducible over $\mathbb{F}_q$, goes to 0 as $n \to \infty$.

Proof : We will prove this fact by a counting argument. Let P be an irreducible polynomial of degree n over $\mathbb{F}_q$. Thus we have $\mathbb{F}_{q^n} \simeq \mathbb{F}_q[X]/(P)$. Since $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois, P splits completely over $\mathbb{F}_{q^n}$, and its roots are all of the images of the class of X by the Galois group, which must be $X, \phi(X), ..., \phi^{n-1}(X)$ and must all be different. Irreducible polynomials of degree n over $\mathbb{F}_q$ are thus exactly the products of the form $\prod_{k=0}^{n-1}(X - \phi^k(a))$, where $a \in \mathbb{F}_{q^n}$ and not in any other subfield, so that the $\phi^k(a)$ are all different. How many such polynomials are there ? There are at most $\frac{q^n-1}{n}$ such polynomials, since for each a, n other choices lead to the same polynomial. Meanwhile, there are q^{n-1} monic polynomials of degree n. The ratio $\frac{q^n-1}{nq^{n-1}}$ tends to 0 when $n \to \infty$, which gives the answer.

4.5 Refinements

4.5.1 A Tiny Bit of Inverse Galois Theory

The main question of inverse Galois Theory is the following : does every finite group G arise as the Galois group of Galois extension of $\mathbb{Q}$? In this section, we give you a fun proof that it is case for every commutative finite group.

The first part consists in proving the following interesting result : for every prime number p, there exists infinitely many prime numbers which are 1 modulo p^t for all t.

Exercise : Infinitely Many Primes are 1 modulo 2^t ***

Let $F_k = 1 + 2^{2^k}$.

1. Prove the well known identity $\prod_{i=0}^{n} F_i = F_{i+1} - 2$ and deduce that the numbers F_k are mutually coprime.
2. Let q be a prime number that divides F_k. Prove that 2 has order 2^{k+1} in $(\mathbb{Z}/q)^*$.
3. Deduce that for all $1 \leq t \leq k+1$, q is 1 modulo 2^t.
4. Conclude that there are infinitely many primes which are 1 modulo 2^t.

Hints : For question 2 prove first that the order of 2 is a power of 2, and that it cannot be less 2^{k+1} since we would then have $2^{2^n} - 1$ divisible by q, but q is linked to F_k and $2^{2^n} - 1$ is linked to other numbers F_i. Use the Lagrange theorem for question 3.

This result can be generalized to prime numbers $p > 2$.

Exercise : Infinitely Many Primes are 1 modulo p^t for $p > 2$ ***

Suppose there are finitely many primes $\{q_1, ..., q_r\}$ which are 1 modulo p^t, let $a = 2q_1...q_r$, and let $c = a^{(p^{t-1})}$. Moreover let $M = 1 + c + ... + c^{p-1}$.

1. Prove that $c = 2$ modulo p.
2. Prove that $c - 1$ and M are coprime.
3. Let q be a prime factor of M. Prove that a has order p^t in $\mathbb{Z}/q$.
4. Conclude that there are infinitely many primes which are 1 modulo p^t.

Hints : Question 1 *is clear, question* 2 *comes down to seeing that* $c-1$ *and* pc^{p-1} *are coprime, the product* $M(c-1)$ *proves that* a *has order* p^t *and it cannot have order less since* c *is not* 1 *modulo* p^t*. For the last question use Lagrange theorem too to see that* $p^t | q-1$*. Notice that* q *is coprime with* a*.*

Now using those too facts, it is easy to conclude : a finite abelian group is of the form $\prod_{i=1}^{n}(\mathbb{Z}/p_i^{n_i})$. So simply take for each p_i a prime number q_i which is 1 modulo $p_i^{n_i}$, take $n = q_1...q_n$. Then we have :

$$\mathbf{Gal}(\mathbb{Q}(e^{\frac{2i\pi}{n}})/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_{i=1}^{n}(\mathbb{Z}/q_i)^* \simeq \prod_{i=1}^{n}(\mathbb{Z}/(q_i-1))$$

... and all the $\mathbb{Z}/(q_i - 1)$ have subgroups isomorphic to $\mathbb{Z}/p_i^{n_i}$. Now use the Galois correspondance on the right subgroup to obtain the right Galois subextension.

4.5.2 Infinite Galois Theory

The fundamental theorem of Galois theory only gives you information on finite Galois extensions. But some very interesting Galois extensions are far from being finite. A good example is $\overline{\mathbb{Q}}/\mathbb{Q}$, the field automorphisms of algebraic numbers that fix $\mathbb{Q}$ pointwise (it is separable because $\mathbb{Q}$ is characteristic 0, and it is clearly Galois). However, it is clearly infinite because it contains bigger and bigger extensions of $\mathbb{Q}$. More generally, it is the case over any perfect field whose algebraic closure is of infinite degree above it (for example, the extension $N_p/\mathbb{F}_p$ where N_p is an algebraic closure of $\mathbb{F}_p$.

The problem, however, is that the Galois Correspondence does not hold in the infinite case. One can construct subgroups of $\mathbf{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ whose subfield of fixed elements is $\mathbb{F}_p$ but which is distinct from $\mathbf{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. Such a subgroup is given by the iterations of the Frobenius morphism and its inverse, isomorphic to $\mathbb{Z}$. We will prove this fact (unconstructively, though) at the end of this section.

Looking back at the proof, we always have $L \subset K^{\mathbf{Gal}(K/L)}$ and $H \subset \mathbf{Gal}(K/K^H)$. The equality $L = K^{\mathbf{Gal}(K/L)}$ still holds in the infinite case (the proof involves no finiteness arguments). However, the proof of the equality $H = \mathbf{Gal}(K/K^H)$ is riddled with finiteness arguments. And for good reasons, mentioned above.

In some way, there are **too many subgroups** in comparison with **extensions**. In order to recover a Galois correspondence, one has to limit the subgroups involved to those that satisfy a certain property. Unexpectedly, the characterization comes from a certain topology on the Galois group: the profinite topology. For the rest of this read, you will need quite a bit of knowledge about profinite groups, which can be found in my dedicated page.

Indeed, for an arbitrary algebraic galois extension K/F, the Galois group $\mathbf{Gal}(K/F)$ has a canonical profinite group structure.

Proposition : Profinite Structure Of Galois Groups

Let K/F be a Galois extension. Then the group $\mathbf{Gal}(K/F)$ is isomorphic to the projective limit of the finite groups $\mathbf{Gal}(L/F)$ where $F \subset L \subset K$ is a finite Galois extension, where the projective limit is done through the following directed system of morphisms : if $F \subset L \subset L' \subset K$ are two subextensions such that L/F and L'/F is Galois, there is a restriction arrow $\sigma_{L',L}$ from $\mathbf{Gal}(L'/F) \to \mathbf{Gal}(L/F)$.

Proof : it is clear that this ordering and those morphisms clearly form a projective system. The arrow $\boldsymbol{Gal}(K/F) \to \varprojlim_L \boldsymbol{Gal}(L/F)$ *is given by assigning to each element of* $\sigma \in \boldsymbol{Gal}(K/F)$ *the element sequence of elements* $(\sigma|_L)_L$ *which is obviously an element of* $\varprojlim_L \boldsymbol{Gal}(L/F)$*. This morphism is clearly injective, since if two elements of* $\boldsymbol{Gal}(K/F)$ *are different they differ at least on a finite Galois extension. For surjectivity, given an element of* $\varprojlim_L \boldsymbol{Gal}(L/F)$*, say* $(\sigma_L)_L$*, define an element of* $\boldsymbol{Gal}(K/F)$ *by* $\forall x \in K$*, take the normal closure* N_x *of* $F(x)/F$ *in* K/F*, and set* $\sigma(x) = \sigma_{N_x}(x)$*. It is easy to prove that this is indeed a field morphism : for example, if* $x, y \in \sigma$*, then* $\sigma(x+y) = \sigma_{N_{x+y}}(x+y) = \sigma_L(x+y)$ *for* L *some finite Galois extension containing both the normal closure of* x *and of* y*. Now* $\sigma_L(x+y) = \sigma_L(x) + \sigma_L(y) = \sigma_{N_x}(x) + \sigma_{N_y}(y) = \sigma(x) + \sigma(y)$*, and similarly for other operations.*

Thus the group $\mathbf{Gal}(K/F)$ inherits a topology from $\varprojlim_L \mathbf{Gal}(L/F)$, which is the profinite topology. More concretely, it is the topology on G where a base of open sets is given by $\sigma\mathbf{Gal}(K/L)$, where L is a finite Galois extension. Indeed : under the profinite topology, a base of open sets of $\varprojlim_L \mathbf{Gal}(L/F)$ is given by the elements aH where H is are open normal subgroups of finite index, namely the kernels of the projections on a finite number of components. From our bijection above, the open normal subgroup $\mathbf{1}_{L_1} \times ... \times \mathbf{1}_{L_n} \times \prod_{L \neq L_1,...,L_n} \mathbf{Gal}(L/F) \cap \varprojlim_L \mathbf{Gal}(L/F)$ are pulled back to $\mathbf{Gal}(K/F)$ as the groups $\mathbf{Gal}(K/C)$ where C is the composite of the extensions $L_1, ..., L_n$.

The main properties of $\mathbf{Gal}(K/F)$ with this topology are as follows : it is a topological group which is **compact**, **Hausdorff**, **totally discontinuous**, and has a **base of neighborhoods** of the identity given by the open normal subgroups $\mathbf{Gal}(K/L)$ where L are the intermediate finite Galois subextensions $F \subset L \subset K$. Since it is a topological group, we remind you that open subgroups are also closed.

This observation gives us the answer for generalizing Galois Theory to infinite extensions. As everywhere in profinite groups theory, there seems to be a preference from closed subgroups. It is also the case here.

Theorem : The Fundamental Theorem of Galois Theory (Infinite Case)

Let K/F be a Galois extension. Then the maps $\mathcal{F}$ and $\mathbf{Gal}(K/\cdot)$ are inverse bijections from the set of subextensions of K/F to the set of **closed subgroups** of $\mathbf{Gal}(K/F)$.

Moreover, this map sends open subgroups to finite sub-extensions, and normal subgroups to Galois sub-extensions. In this case, the restriction morphism is well defined, $\mathbf{Gal}(K/F) \to \mathbf{Gal}(L/F)$, which leads to an exact sequence :

$$1 \to \mathbf{Gal}(K/L) \to \mathbf{Gal}(K/F) \to \mathbf{Gal}(L/F) \to 1$$

This proof will take some work, but we invite the reader to consider how cleverly the finite case is reused to prove the infinite case.

From the proof of the finite case, $K^{\boldsymbol{Gal}(K/L)} = L$ *is still true for any subextension* $F \subset L \subset K$*. We also still have for any subgroup of the Galois group,* $H \subset \boldsymbol{Gal}(K/\mathcal{F}(H))$*. What we have to prove is equality. The idea of the proof is to reuse the finite theorem on finite, Galois subextensions* $L/\mathcal{F}(H)$ *(which are still separable).*

*Let H be a subgroup of $\mathbf{Gal}(K/F)$, and consider a subextension $\mathcal{F}(H) \subset L \subset K$ such that $L/\mathcal{F}(H)$ is finite and Galois. By restriction to L, one obtains a restriction map $H \to \mathbf{Gal}(L/\mathcal{F}(H))$. Since $\mathcal{F}(H)$ is **exactly** the field of pointwise invariant elements under H, finite Galois theory tells us that the mapping is surjective: the subgroup $\tilde{H}$ corresponding to the image of H has fixed field $\mathcal{F}(H)$, and by injectivity of the Galois Correspondence in the finite case, we have $\tilde{H} = \mathbf{Gal}(L/\mathcal{F}(H))$.*

*Now, how far does this tell us that $\mathbf{Gal}(K/\mathcal{F}(H)) \subset H$? Let $\sigma \in \mathbf{Gal}(K/\mathcal{F}(H))$. For any finite subextension $L/\mathcal{F}(H), \exists \tau \in H$, $\tau|_L = \sigma|_L$. So this means that $\tau \in H \cap \sigma\mathbf{Gal}(K/L)$. Now the important observation is that the groups $\sigma Gal(K/L)$ with $[L : \mathcal{F}(H)] < +\infty$ form a basis of neighborhoods of $\sigma \in \mathbf{Gal}(K/\mathcal{F}(H))$, **so σ is in the closure of H in $\mathbf{Gal}(K/\mathcal{F}(H))$**. Note that we are talking about the profinite toplogy on $\mathbf{Gal}(K/\mathcal{F}(H))$, not on $Gal(K/F)$. So H is dense in $\mathbf{Gal}(K/\mathcal{F}(H))$.*

However, since H is closed in $\mathbf{Gal}(K/F)$, this implies that it is also closed in $\mathbf{Gal}(K/\mathcal{F}(H))$. Indeed, for any element σ which is not in H, there is an open subgroup $\mathbf{Gal}(K/A)$ such that $\sigma\mathbf{Gal}(K/A)$ is not in H. But $\sigma\mathbf{Gal}(K/A)$ contains $\sigma\mathbf{Gal}(K/A\mathcal{F}(H))$ (where $A\mathcal{F}(H)$ is the composite of the two extensions), and $A\mathcal{F}(H)/\mathcal{F}(H)$ is Galois and finite. Thus H is closed in $\mathbf{Gal}(K/\mathcal{F}(H))$. So $H = \mathbf{Gal}(K/\mathcal{F}(H))$, which finishes the proof.

From this work, we can understand what the operation $H \to \mathbf{Gal}(K/\mathcal{F}(H))$ does to an arbitrary subgroup H : it outputs a closed subgroup which contains H. Moreover, any closed subgroup containing H also contains $\mathbf{Gal}(K/\mathcal{F}(H))$, since the map $H \to \mathbf{Gal}(K/\mathcal{F}(H))$ is increasing. So $\mathbf{Gal}(K/\mathcal{F}(H))$ is **the closure of** H in $\mathbf{Gal}(K/F)$.

Now it is easy to see that $\mathbf{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ is isomorphic to $\hat{\mathbb{Z}}$, and that $\mathbb{Z}$ (represented by the iterations of the Frobenius) is distinct from $\hat{\mathbb{Z}}$ by a countability argument. Yet is it dense it $\hat{\mathbb{Z}}$, so its fixed field is $\overline{\mathbb{F}_p}$ (this can also be verified explicitly).

To finish up our work, here is a beautiful fact about Galois theory and profinite groups, which in a certain way is a generalization of the exercise in which we proved that for any finite group G, there exists a Galois Extension K/F whose Galois group is G.

Exercise : Profinite Groups as Galois Groups ***

In this exercise, we prove that for any profinite group G, there exists a Galois extension K/F with Galois group G.

1. Let k be any field, and consider the field $k(T_U)$, the fields of rational fractions with coefficients T_U where U ranges over the cosets of the open normal subgroups of G, with finite index G. Define an action of G on $k(T_U)$ by $\gamma T_U = T_{\gamma U}$. Verify that G acts by field automorphisms on $k(T_U)$.
2. Denote $\mathcal{F}(G)$ the fixed field of $k(T_U)$ under action of G. Check that the extension $k(T_U)/\mathcal{F}(G)$ is Galois.
3. Prove that the map $G \to \mathbf{Gal}(k(T_U)/\mathcal{F}(G))$ is an injective group morphism.
4. Prove that the map $G \to \mathbf{Gal}(k(T_U)/\mathcal{F}(G))$ is continuous with respect to the profinite topology on the two groups.
5. Conclude that the map $G \to \mathbf{Gal}(k(T_U)/\mathcal{F}(G))$ is an isomorphism.

Proof : the first check is just writing. For the question, notice that any element T_U is killed by the polynomial $\prod_{\gamma U \text{ coset of } U}(X - T_{\gamma U})$, which is separable and has all of its roots in $k(T_U)$. This makes the extension normal and separable and thus Galois. Injectivity of the mapping comes from the fact that if $g_1 \neq g_2$, then by Hausdorffness of G there is an open normal subgroup U such that $g_1U \cap g_2U = \emptyset$, and thus the image of T_U under those two elements is different.

To obtain continuity of the mapping, notice that the inverse image of $\boldsymbol{Gal}(k(T_U)/L)$ *where* $L/\mathcal{F}(G)$ *is finite and Galois is generated by a finite number of fractions, say* $F_1, ..., F_n$*. Let* $U_1, ..., U_m$ *the subgroups appearing in those fractions. Then the inverse image of* $\boldsymbol{Gal}(k(T_U)/L)$ *contains* $\cap_{i=1}^{m} U_i$*, which is open (and remember that a profinite subgroup which contains an open subgroup is open, since it contains the cosets of this open subgroup around each of its elements). So the inclusion is indeed continuous.*

Now that continuity has been proven, notice that by compactness of G*,* G *is closed in* $\boldsymbol{Gal}(k(T_U)/\mathcal{F}(G))$*. It has fixed field* $\mathcal{F}(G)$*, so by the fundamental theorem of Galois theory it is equal to* $\boldsymbol{Gal}(k(T_U)/\mathcal{F}(G))$ *whole.*

Chapter 5

Theory of Valuations and Local Fields

These notes essentially follow Neukirch's approach on the matter, from the second chapter of his famous book.

5.1 p-adic numbers

5.1.1 Initial Observations

Firstly, note the following easy result :

Proposition : Representations of classes modulo a^n

Let $n \in \mathbb{N}$ be an integer greater than 2 and let m be an integer greater than 1. Then any number class $c \in \mathbb{Z}/n^m\mathbb{Z}$ can be represented in a unique way as :

$$c = a_0 + a_1 n + a_2 n^2 + ... + a_{m-1} n^{m-1} \ \textbf{mod} \ n^m$$

... with $0 \leq a_i < n$.

*Proof : by induction on m. For $m = 1$, the answer is clear. Suppose it is proven for m. Let c be a class modulo n^{m+1}. Then c is uniquely represented as $c = a_0 + a_1 n + a_2 n^2 + ... + a_{m-1} n^{m-1}$ **mod** n^m. Lifting the congruence, we have $c = a_0 + a_1 n + a_2 n^2 + ... + a_{m-1} n^{m-1} + g n^m$ **mod** n^{m+1}, for a certain $0 < g \leq n-1$, which proves the existence. For uniqueness, we find that the coefficients up to $m-1$ are unique by induction, and then a_m is uniquely determined as the diffenrece of c with the former terms.*

Take a prime number p and a rational number $r = \frac{a}{b}$, where b is coprime with p. To r one may associate a sequence in $(\mathbb{Z}/p\mathbb{Z})^n$ in the following way : for all n, the class of ab^{-1} is represented in a unique way modulo p^n as in the proposition above : the coefficients in the expansion yield the n first terms of the sequence. Note that this is well defined, since if :

$$ab^{-1} = a_0 + a_1 p + a_2 p^2 + ... + a_{m-1} p^{m-1} + a_m p^m \ \textbf{mod} \ p^{m+1}$$

...then :

$$ab^{-1} = a_0 + a_1 p + a_2 p^2 + ... + a_{m-1} p^{m-1} \ \textbf{mod} \ p^m$$

... since the class of b^{-1} modulo p^m can be deduced from the class modulo p^{m+1} by reduction (indeed, $bb^{-1} = 1$ holds modulo anything).

Those developments are however not always easy to obtain, since computing b^{-1} modulo large prime numbers is not an easy matter.

Exercise : Development of $\frac{1}{2}$ **

Write a few first terms of the development of $\frac{1}{2}$ for $p = 5$, and conjecture a general law for the development of $\frac{1}{2}$ modulo any odd prime. Then, prove this law.

Solution : we must compute the inverses of 2 *modulo* 5^n*. For* $n = 1$*, we get* 3*, for* $n = 2$ *we get* 13*, for* $n = 3$ *we get* 63*, for* $n = 4$ *we get* 313*... so the first terms are* $a_0 = 3$*,* $a_1 = 2$*,* $a_2 = 2$*,* $a_3 = 2$*... one could continue and see that this sequence stays at* 2 *forever. The reason for this is the equality :* $2 \times (3 + 2 \times 5 + 2 \times 5^2 + ... + 2 \times 5^n) = 6 + 4 \times 5 + 4 \times 5^2 ... + 4 \times 5^n = 1 + 5^{n+1}$*. The development of* $\frac{1}{2}$ *modulo any odd prime* p *has, by the exact same proof,* $a_0 = \frac{p+1}{2}$ *and* $a_n = \frac{p-1}{2}$ *for all* $n \in \mathbb{Z}$*.*

Exercise : Development of -1 **

Find the development of -1 modulo any prime number.

Solution : For any number p *we have the equality* $p - 1 + (p - 1)p + ... + (p - 1)p^n = -1 + p^{n+1}$*, which proves that the development of* -1 *is constant equal to* $p - 1$*.*

Exercise : Development of negative integers ***

Find the general form of the development of negative integers modulo p.

Solution : Let $-n$ *be a negative integer and let* k *be such that* $0 < n < p^k$*. Write the positive integer* $p^k - n$ *as* $\sum_{i=0}^{m} a_i p^i$*. Then for all index* $l > k$*, one has* $-n + p^l = -n + p^k - p^k + p^{k+1} - p^{k+1} ... - p^{l-1} + p^l = \sum_{i=0}^{m} a_i p^i + (p - 1)p^k + (p - 1)p^{k+1} ... + (p - 1)p^{l-1}$*, which proves that the development is* $p - 1$ *after a certain rank.*

Exercise : Development of $\frac{1}{1-p}$ **

Let p be any prime number. Find the development of $\frac{1}{1-p}$ modulo p.

Solution : One finds that $(1 - p)(1 + p + p^2 ... + p^n) = 1 - p^{n+1}$*. Thus the development of* $\frac{1}{1-p}$ *is constant equal to* 1*.*

Now, if $r = \frac{a}{b}$ under irreducible form has a denominator which is not coprime to p, we can write $r = \frac{a}{c} p^{-m}$. We then assign a development of r which is as follows : if l_i for $i \geq 0$ is the development of $\frac{a}{c}$, we put $l_i = 0$ for $i < 0$ and define a development of r indexed by $\mathbb{Z}$ by $a_i = l_{i+m}$ for all $i \in \mathbb{Z}$.

A fundamental fact is the following :

Proposition : Injectivity of the Mapping

The association described so far defines an injection of $\mathbb{Q} \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}}$.

Solution : we only have to prove it for rational numbers with denominator coprime to p*, since the index rule we set differentiates outputs if the* p*-valuation at the denominator differs. Injectivity is clear for positive integers, since their development injectively comes from their development in base* p*, which is unique. For more general integers* a *and* b*, say* $a < b$*, note that* $b - a$ *is a positive integer with* 0 *development at all indices and is thus* 0 *in* $\mathbb{Z}$*. For arbitrary rationals (with denominator coprime to* p*)* $r_1 = \frac{a}{b}$ *and* $r_2 = \frac{c}{d}$*, notice that* $dr_2 - br_1$ *(or the opposite) is a positive integer with zero development, and is thus* 0 *which proves that* $r_1 = r_2$*. The key to this proof is that the development of a product* ab *can be easily retrieved from their development at index* n *by multiplying their developments in* $\mathbb{Z}/p^n\mathbb{Z}$*.*

Exercise : An Almost Null Development *

Let r be a rational number such that the development of r modulo a prime number p is zero after a certain rank. Prove that r is a positive integer.

Solution : Every positive integer corresponds to a single development which is 0 *after a certain rank. The result comes from injectivity of the inclusion.*

5.1.2 The Ring $\mathbb{Z}_p$

In the former section, given a prime number p, we injectively associated to each rational with a denominator coprime to p (we will call this set, which is a subring of $\mathbb{Q}$, $\mathbb{Z}_{(p)}$) a sequence in $(\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}}$, with potentially inifinitely many non zero terms. For such a rational r, such a sequence is called the **p-adic expansion** of r. We will now make this more formal.

Definition : The set of p-adic integers $\mathbb{Z}_p$

The set $\mathbb{Z}_p$ is the set of formal power series :

$$\sum_{i\in\mathbb{N}} a_i p^i$$

...with $0 \leq a_i < p$.

By associating to each rational with denominator coprime to p the power serie associated to its p-adic expansion, we define an injection of $\mathbb{Z}_{(p)}$ in $\mathbb{Z}_p$.

Exercise : $\mathbb{Z}_p$ is striclty larger than $\mathbb{Z}_{(p)}$ *

Prove that the above inclusion is strict.

Solution : $\mathbb{Z}_p$ is clearly uncoutable.

This set is obviously some sort of ring. For example, you want to be able to define addition, that would work the following way : the sum of $\sum_{n\in\mathbb{N}} a_i p^i$ and $\sum_{n\in\mathbb{N}} b_i p^i$ would be computed by computing one by one the $a_i + b_i$. Then, for i going from 0 to infinity, if $a_i + b_i < p$, then define $c_i = a_i + b_i$, and if $a_i + b_i \geq p$, define $c_i = a_i + b_i - p$ and for the next term define $c_{i+1} = a_{i+1} + b_{i+1} + 1$ and repeat the same process. This addition would make the injection $\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p$ a group morphism. Similarly, you could define multiplication. However, this will obviously become very messy as soon as any slightly involved computation has to be achieved. To convince yourself of this fact, solve the following (useful) exercise :

Exercise : The opposite of a p-adic integer ****

Let $a = \sum_{i=0}^{\infty} a_i p^i$ a p-adic integer. Devise an algorithm to compute the expansion of the additive inverse of a in $\mathbb{Z}_p$. Conclude that if a has a p-adic expansion which is periodic after a certain rank, then so does its opposite.

Solution : A working algorithm is as so.

Initialization : *WLOG we can suppose that a_0 is non zero. Then put $b_0 = p - a_0$.*

Heredity : *suppose b_i has been constructed, such that $a + \sum_{n=0}^{i} b_n p^n \in p^{i+1}\mathbb{Z}_p$. If $a_j = p - 1$ for all $j > i$, then stop the algorithm here. If not, let $i < k$ be the highest integer such that $0 \leq a_k < p - 1$. Then for all $i < j < k$, put $b_j = 0$ and $b_k = p - 1 - a_k$. It is easy to check that we now have $a + \sum_{n=0}^{k} b_n p^n \in p^{k+1}\mathbb{Z}_p$.*

Then I leave it to you to check that the series $\sum_{i=n}^{\infty} b_n p^n$ converges to $-a$.

To address the last question, suppose that (a_i) is periodic after rank n_0 (so the period is entirely described by $a_{n_0+1}, ..., a_{n_0+l}$ if it is of length l). If all of the $a_{n_0+1}, ..., a_{n_0+l}$ are $p-1$, then b_i is zero after a certain rank and thus there is nothing to prove. Say that a_{n_0+i} is the first term which is not $p-1$ and a_{n_0+j} is the last (we obviously have $i \leq j$). We must now distinguish several cases.

If $i = 1$ and $j = l$, then it is easy to see (by doing the algorithm above in your head) that the b_n will loop with the a_n.

If $1 < i \leq l$, and $j = l$, it's the same (do the algorithm in your head again).

The other cases are left to you, but I'm sure you will figure them out. Try writing out a few cases on paper if you're struggling.

This is why we take a different point of view on $\mathbb{Z}_p$, by showing that $\mathbb{Z}_p$ is isomorphic to another object which has a clearer ring structure. To do so, for each $n \in \mathbb{N}$, we define the ring morphism $p_{n+1} : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ by reduction. This yields a projective system $(\mathbb{Z}/p^n\mathbb{Z}, p_n)_{n\geq 1}$. The projective limit of those rings, $\varprojlim(\mathbb{Z}/p^n\mathbb{Z})$ has a clear ring structure, by addition and multiplication componentwise. We now argue that :

Proposition : Another Reprensentation of $\mathbb{Z}_p$

The map $\mathbb{Z}_p \to \varprojlim(\mathbb{Z}/p^n\mathbb{Z})$, defined by :

$$\sum_{i\in\mathbb{N}} a_i p^i \mapsto (\sum_{i=0}^{n-1} a_i p^i \ \textbf{mod}\ p^n)_{n\in\mathbb{N}}$$

...is a bijection.

Proof : injectivity and surjectivity are immediate from the fact that all classes modulo p^n can be represented in a unique way as such a series.

Exercise : Some properties of $\mathbb{Z}_p$ **

1. Prove that $\mathbb{Z}_p$ is an integral domain, and find its units.
2. Conclude that $\mathbb{Z}_p$ is a local ring, and find its maximal ideal.
3. Furthermore, prove that all ideals of $\mathbb{Z}_p$ are principal, and of the form $p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p, v_p(x) \geq n\}$.

Solution : suppose that x, y have non zero first term. Then because $\mathbb{Z}/p\mathbb{Z}$ is an integral domain it is clear that this is also the case for xy. Now if x and y are non zero, then $x = p^n x'$ and $y = p^m y'$ with x' and y' having a non zero first term. The multiplication yields $p^{n+m}x'y'$ which is non zero. Now, for the units of $\mathbb{Z}_p$, it is clear that any unit must have non zero first term. If (x_i) has non zero first term, then define (y_i) as so : $y_0 = x_0^{-1}$, and chose the only y_{n+1} such that $(\sum_{i+j=n+1, i\neq 0} x_i y_j) y_{n+1}^{-1} = -x_0$. We leave it to you to compute explicitly the first few terms to see how this works.

For the second question, the ideal $\mathfrak{m}$ defined by those elements that have zero first term is indeed a maximal ideal, and is the only one since every element not in $\mathfrak{m}$ is a unit.

For the third question, take an ideal I, take an element of smallest p-adic valuation. This elements generates $p^n\mathbb{Z}_p$, so $p^n\mathbb{Z}_p \subset I$. Also, I is contained in $p^n\mathbb{Z}_p$.

5.1.3 The Field $\mathbb{Q}_p$

To complete the inclusion of $\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p$ to an inclusion $\mathbb{Q}$ into some set, we associated to terms with denominator of the form $p^n r$ with $r \wedge p = 1$, a development with negative terms. We thus take the same two parallel approach to describe an extension of $\mathbb{Z}_p$, $\mathbb{Q}_p$, called the **p-adic numbers**.

Definition : The set of p-adic numbers $\mathbb{Q}_p$

The set $\mathbb{Q}_p$ is the set of formal power series :

$$\sum_{i=-m}^{\infty} a_i p^i$$

...with $0 \leq a_i < p$, $m \in \mathbb{N}$ and $a_{-m} \neq 0$.

We then have an inclusion of $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ defined as above, that sends $\mathbb{Z} \to \mathbb{Z}_p$. Defining a ring structure on $\mathbb{Q}_p$ is once again fairly intuitive, but not easy to formulate. To do so, we turn once again to our algebraic representation of $\mathbb{Z}_p$.

Proposition : Another Representation of $\mathbb{Q}_p$

The map $\mathbb{Q}_p \to \mathbf{Frac}(\mathbb{Z}_p)$, defined by :

$$\sum_{i=-m}^{\infty} a_i p_i \mapsto \frac{\iota(\sum_{i=0}^{\infty} a_{i-m} p^i)}{p^m}$$

...where ι is the isomorphism $\mathbb{Z}_p \simeq \varprojlim(\mathbb{Z}/p^n\mathbb{Z})$, is a bijection.

Proof : this is clearly injective. Having $\frac{\iota(\sum_{i=0}^{\infty} a_{i-m} p^i)}{p^m} = \frac{\iota(\sum_{i=0}^{\infty} b_{i-l} p^i)}{p^l}$ *would force* $m = l$ *and then equality after simplification. For surjectivity, we prove that every element is of this form by showing that* $\frac{a}{b} = \frac{a}{p^n b'}$ *where* b' *is a unit, which is equal to* $\frac{a(b')^{-1}}{p^n}$.

5.2 The p-adic Absolute Value : An Analytic Presentation of $\mathbb{Q}_p$

In this section, we give another equivalent presentation of $\mathbb{Q}_p$, which is very different in the way that it proceeds from an essentially analytic point of view.

5.2.1 The p-adic absolute value, and a construction of $\mathbb{Q}_p$

Definition : The p-adic absolute value on $\mathbb{Q}$

Any rational $\frac{a}{b}$ element of $\mathbb{Q}$ can be written in an only way as $p^m \frac{a'}{b'}$ with $a'b' \wedge p = 1$ and $m \in \mathbb{Z}$ (we put $m = \infty$ if $a = 0$). This defines a function $\mathbb{Q} \to \mathbb{Z} \cup \infty$ called the **p-adic valuation**, and is denoted v_p. The **p-adic absolute value** is given by $\frac{a}{b} \mapsto p^{-v_p(\frac{a}{b})}$, and is denoted $||_p$.

For example, the 3-adic absolute value of $243 = 3^5$ is $\frac{1}{3^5}$. The 3-adic valuation of 2 is 1.

Proposition : Properties of $||_p$

1. $|a|_p = 0 \iff |a| = 0$.
2. $|ab|_p = |a|_p|b|_p$.
3. $|a+b|_p \leq \mathbf{max}(|a|_p, |b|_p) \leq |a|_p + |b|_p$, with $|a+b|_p = \mathbf{max}(|a|_p, |b|_p)$ if $|a|_p \neq |b|_p$.

Proof : the first property is evident, the second property is too, the third one comes from the fact that $p^m \frac{a}{b} + p^n \frac{c}{d} = p^{\min(m,n)} \frac{u}{v}$ *where* $\frac{u}{v}$ *has positive p-adic valuation. This proves that* $v_p(a+b) \geq \boldsymbol{min}(v_p(a), v_p(b))$*, and the inequality follows by inversion. If the valuations are different, a small calculation proves equality.*

Additionally, we define $||_\infty$ as the regular absolute value on $\mathbb{Q}$. See that with those axioms, $\mathbb{Q}$ becomes a $\mathbb{Q}$ normed vector space of dimension 1 for the absolute value $||_p$.

Exercise : An Observation **

Make the following observation : we have for all rational number r the equality...

$$\prod_p |r|_p \cdot |r|_\infty = 1$$

Solution : this is almost immediate, as the $|r|_p$ *spell out the prime decomposition of the inverse of* r*.*

We then take the usual path to construct the completed of a field for a given absolute value. Let's do it once again.

A Cauchy sequence in $\mathbb{Q}$ for $||_p$ is a sequence (x_i) such that for all $\epsilon > 0$, $|x_i - x_j|_p < \epsilon$ for all i, j above a certain N. It is clear by triangle inequality that a sum of Cauchy sequences is still Cauchy, a product too by substraction and addition. Also, the constant sequence equal to 1 is a 1 for multiplication. So the Cauchy sequences form a ring. Additionally, the sequences converging to 0 form an ideal.

We prove that the ideal of nullsequences is maximal : indeed, consider the ideal generated by a nullsequence and by a sequence x which does not converge to 0. Since for arbitrarily large values of n, x_n stays ϵ away from zero, and terms are $\epsilon/2$ apart from one another after a certain rank, x_n is non zero after a certain term N. Replace x_n by $x_n + e$ where e is the sequence that is 1 where x_n is 0. It is a null sequence. $x_n + e$ has no null terms. Now for such a sequence, the inverse sequence is also Cauchy since $|\frac{x_n - x_m}{x_n x_m}|_p = \frac{|x_n - x_m|_p}{|x_n x_m|_p}$ with a lower term bounded away from 0 after a certain point. Now multiply by this inverse, you get 1. Thus the null Cauchy sequence forms a maximal ideal.

Denote R the ring of null sequences and $\mathfrak{m}$ this maximal ideal. Consider the field $R/\mathfrak{m}$. We call it $\mathbb{Q}_p$, the field of p-adic numbers. We can extend $||_p$ to $\mathbb{Q}_p$ by taking the limit of the norm of any representative (it converges because it is Cauchy in $\mathbb{R}$ and does not change under addition of a null sequence). Notice that it can only converge to 0 or to a number of the form p^n for a certain $n \in \mathbb{Z}$ (either it is adherent to zero either it converges in a discrete set).

We also have an inclusion of $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ by associating r to the constant sequence equal to r.

We will prove that $\mathbb{Q}_p$, an object of a very analytical nature, is actually the same object as the one we algebraically constructed earlier. Before doing so, here are a few considerations on $\mathbb{Q}_p$'s topology.

5.2.2 A Few Considerations on $\mathbb{Q}_p$'s topology

Now that $\mathbb{Q}_p$ has a norm, it is given a topology in the usual way : the open sets are arbitrary reunions of open balls of radius ϵ for real numbers $\epsilon > 0$. Now, the identity $|a+b|_p \leq \mathbf{max}(|a|_p, |b|_p)$ yields a lot of strange consequences on the topology of $\mathbb{Q}_p$, one of them being the following :

Exercise : Convergent Series in $\mathbb{Q}_p$ **

Let (a_n) be a sequence of p-adic numbers. Prove that $\sum_{n\in\mathbb{N}} a_n$ converges if and only if $a_n \to 0$ when $n \to \infty$. Equivalently, prove that a sequence (a_n) is Cauchy if and only if $|a_n - a_{n+1}|_p \to 0$ when $n \to \infty$.

Solution : the fact that we must have $a_n \to 0$ is the usual proof consisting in taking the difference of two partial sums. Now if $a_n \to 0$, the difference of two partial sums of arbitrary indices has lower norm than the maximum of the norms of the summands between the two bounds, which tends to 0.

Exercise : $\mathbb{Q}_p$ is a topological field **

Prove that $\mathbb{Q}_p$ a topological field.

Solution : We firstly need to prove that affine maps, $x \mapsto \lambda x + y$, for λ and $y \in \mathbb{Q}_p$ are continuous, but this is immediate. Then we need to check that the function $\mathbb{Q}_p \times \mathbb{Q}_p$, $x, y \mapsto xy$ is continuous. This is also true because for $\epsilon > 0$, then for all a, b close enough to x and y we have $|xy - ab| \leq |x||y - b| + |b||x - a|$ which is arbitrarily small when a and b are close enough to x and y. For the condition of topological field to be fulfilled, we just have to check that inversion is continuous. But this is easily checked thanks to the condition $|x|_p^{-1} = |x^{-1}|_p$. We have more generally proved that a field with a sub-additive and multiplicative absolute value is a topological field for the topology associated to this absolute value.

Exercise : The Closed Unit Ball ***

Prove that the closed unit ball of $\mathbb{Q}_p$ is equal to the closure of $\mathbb{Z}$ with respect to $||_p$.

*Solution : We prove that the closure of $\mathbb{Z}$ contains the rationals of norm lower or equal to 1, whose closure is the closed unit ball (a p-adic number of norm $l > 0$ is a limit of rationals of norm 1, a p-adic number of norm 0 is a limit of rationals of norm lower than 1). To do so consider a rational number of the form $p^m \frac{a}{b}$ with $(ab, p) = 1$. Then for all $n \in \mathbb{Z}$, we have $p^m \frac{a}{b} - n = \frac{p^m a - nb}{b}$. Now since b is a unit modulo p^r for all r, we can chose n such that $p^m a - nb = 0$ **mod** p^r and thus $|\frac{p^m a - nb}{b}| \leq p^{-r}$, which is enough to conclude.*

5.2.3 Identification of the Algebraic and Analytic $\mathbb{Q}_p$

We will now proves that the two objects we have constructed and called the same are actually isomorphic. In the last section, in the first exercise, we introduced the closed unit ball of $\mathbb{Q}_p$, or equivalently the closure of $\mathbb{Z}$. We will call (for reason that will become clear) this closed unit ball $\mathbb{Z}_p$. We now have a lemma :

Proposition : $\mathbb{Z}_p$'s Properties as a Ring

$\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$, which is a principal ideal domains with ideals $p^n\mathbb{Z}_p = \{x \in \mathbb{Z}_p, |x|_p \leq p^{-n}\}$. Additionally, $\mathbb{Q}_p$ is the fraction field of $\mathbb{Z}_p$.

Proof : by multiplicativity of the norm it is clearly a subring. Now it is clear that every element in $\mathbb{Q}^p$ can be written $p^m u$ with $u \in \mathbb{Z}_p^*$, and in a unique way so. Now to prove this fact, take an ideal of $\mathbb{Z}_p$, take an element of maximum norm, prove that it generates $p^n\mathbb{Z}_p$, and notice that the ideal is also contained in $p^n\mathbb{Z}_p$. The fact that $\mathbb{Q}_P$ is the fraction field of $\mathbb{Z}_p$ comes from the fact that elements of norm greater than one are elements of norm lower or equal to one multiplied by p to a certain power.

Here's another lemma :

Proposition : $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$

The injection $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ induces an isomorphism $\mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p$.

Proof : the homomorphism $\mathbb{Z} \hookrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$ is surjective, since $\mathbb{Z}$ is a dense subset of $\mathbb{Z}_p$ and thus for any element $x \in \mathbb{Z}_p$ there is an element $a \in \mathbb{Z}$ such that $|x-a| \leq \frac{1}{p^n}$, and thus $x - a \in p^n\mathbb{Z}_p$. Now its kernel is clearly exactly $p^n\mathbb{Z}$, so here we are.

This allows us to construct the isomorphisms we wanted.

Theorem : Identification of the Algebraic And the Analytic $\mathbb{Q}_p$

The rings $\varprojlim(\mathbb{Z}/p^n\mathbb{Z})$ and $\mathbb{Z}_p \subset \mathbb{Q}_p$ are isomorphic. Thus their fraction fields are too, and we may talk about the one and only obejct $\mathbb{Q}_p$ both through its algebraic and analytic construction.

Proof : to prove it, notice that the isomorphisms $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$ lift up to surjective morphisms $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$, which are easily seen to assemble into a morphism $\mathbb{Z}_p \to \varprojlim(\mathbb{Z}/p^n\mathbb{Z})$. Injectivity comes from the fact that if the image of an element is 0, this means that it is in all of the $p^n\mathbb{Z}_p$ for all n and thus that its norm is 0. Surjectivity comes from the fact that, to reach the element $(\sum_{i=0}^{n-1} a_i p^i)$, one just has to take the element $\sum_{i=0}^{\infty} a_i p^i$ in $\mathbb{Z}_p$ which can be checked to work just fine.

Exercise : The Identification is a Homeomorphism ***

Given the algebraic construction of $\mathbb{Z}_p$, which is the $\varprojlim(\mathbb{Z}/p^n\mathbb{Z})$, we give $\varprojlim(\mathbb{Z}/p^n\mathbb{Z})$ the profinite topology : it is the topology induced by the product topology on the product of the $\mathbb{Z}/p^n\mathbb{Z}$. Prove that the identification above is a homeomorphism for the two topologies (the analytic one induced by $\mathbb{Q}_p$ and the profinite topology on $\varprojlim(\mathbb{Z}/p^n\mathbb{Z})$).

Solution : prove that the profinite topology on $\varprojlim(\mathbb{Z}/p^n\mathbb{Z})$ precisely comes from the metric induced by the former bijection. To do so, notice that every open ball around $x \in \mathbb{Z}_p$ is open in $\varprojlim(\mathbb{Z}/p^n\mathbb{Z})$ (indeed, it is the intersection of $\varprojlim(\mathbb{Z}/p^n\mathbb{Z})$ and of the sequences constant equal to x and equal to $\mathbb{Z}/p^n\mathbb{Z}$ after a certain rank). Conversely, notice that a basis of open sets of $\varprojlim(\mathbb{Z}/p^n\mathbb{Z})$ are the points $\times$ the whole sets, and that this is open in $\mathbb{Z}_p$.

Exercise : Yet another presentation of $\mathbb{Z}_p$ ***

Prove that $\mathbb{Z}_p$ is isomorphic to the ring $\mathbb{Z}[[X]]/(X-p)$.

Solution : There is an obvious surjective morphism $\mathbb{Z}[[X]] \to \mathbb{Z}_p$, which to $\sum a_i X^i \mapsto (\sum_{i=1}^{n} a_i p^i \ \textbf{mod}\ p^n)_{n\in\mathbb{N}}$. Now notice that every element of $\mathbb{Z}[[X]]$ can be written as $F(X) = Q(X)(X-p) + R(X)$, where Q and R are inductively described as they should, and R has coefficients $0 \leq r_i < p$. Now notice that if the image of F is 0, this implies that $R = 0$ and thus that $F \in (X-p)$. So we have our bijection.

5.3 Interlude : Congruences and Polynomial Equations modulo p^n

In this section, we will explore a first practical application of p-adic numbers, which is that of polynomial equations. This will allow us to make many more theoretical observations about $\mathbb{Q}_p$. The main observation is that of the link between congruences of polynomial equations **mod** p and the same equations in $\mathbb{Z}_p$.

Proposition : Polynomial Equations in $\mathbb{Z}_p$ and modulo p^n

Let $F(X_1, ..., X_n)$ be a polynomial with coefficients in $\mathbb{Z}$. Then the two following statements are equivalent :

- $F(X_1, ..., X_n) = 0$ has a solution **mod** p^n for all $n \geq 1$.
- $F(X_1, ..., X_n) = 0$ has a solution in $\mathbb{Z}_p$.

Exercise : Proof of the above statement ***

1. Prove that if $F(X_1, ..., X_n) = 0$ has a solution in $\mathbb{Z}_p$, then it has a solution **mod** p^n for all $n \geq 1$.
2. Inductively construct a solution in $\mathbb{Z}_p$ if the first condition is fulfilled.

*Solution : The first point is clear, by taking the reduction modulo p^n for all n (describe $\mathbb{Z}_p$ by projective limit so that it appears clearly). For the second point, since by reduction there are infinitely solutions **mod** p^n for all n, then one might chose for $n = 1$ a solution $x_1, ..., x_n \in \mathbb{Z}/p\mathbb{Z}^n$ such that infinitely many solutions of the set reduce to $x_1, ..., x_n$. Then one might repeat the process in $\mathbb{Z}/p^2\mathbb{Z}^n$, etc. Another way to see it is that solutions form a projective system, and that a projective limit of non-empty finite sets is never empty.*

We however possess a very simple tool to check such conditions, which is a weak version of a stronger theorem called "Hensel's Lemma" which we will see appear many times in what follows.

Theorem : Hensel's Lemma, Weak Version

If $F(X) \in \mathbb{Z}_p[X]$ and $a \in \mathbb{Z}_p$ verifies :

$$F(a) = 0 \textbf{ mod } p, F'(a) \neq 0 \textbf{ mod } p$$

... then there is a unique $\alpha \in \mathbb{Z}_p$ such that $F(\alpha) = 0$ in $\mathbb{Z}_p$ and $\alpha = a$ **mod** p.

Proof : First of all, notice that in $\mathbb{Z}[X, Y]$, we have a polynomial $G(X, Y)$ such that $F(X + Y) = F(X) + YF'(X) + Y^2G(X, Y)$ (this is fairly obvious by expansion). We will use this to expand our solution. Let $\alpha_1 = a$ be the first solution. Then in $\mathbb{Z}/p\mathbb{Z}^2$, we have $F(\alpha_1 + pt_1) = F(\alpha_1) + ptF'(\alpha_1)$. Now we know that $F(\alpha_1) = k_1p$. So one may chose t_1 such that $k_1 + t_1F'(\alpha_1) = 0$ in $\mathbb{Z}/p\mathbb{Z}$, namely $t_1 = -kF'(a)^{-1}$. Write $\alpha_2 = a + pt_1$.

The induction process is similar : if the solution is found up to α_n, then we have in $\mathbb{Z}/p^{n+1}\mathbb{Z}$, $F(\alpha_n + p^nt_n) = F(\alpha_n) + p^nt_nF'(\alpha_n)$, with $F(\alpha_n) = p^nk_n$. Note that since $\alpha_n = a + p(...)$, then we have $p^nF'(\alpha_n) = p^nF'(a)$ in $\mathbb{Z}/p^{n+1}\mathbb{Z}$. Now just repeat the process of the first paragraph to construct α_{n+1}.

For uniqueness, note that in the above process, the choice of the t_i is perfectly unambiguous, we have an only choice.

This relatively easy fact has many great consequences. Notably, the following :

Exercise : Roots of Unity in $\mathbb{Q}_p$, part 1 **

Using the above observation, prove that the polynomial $X^{p-1} - 1$ has exactly $p - 1$ different roots in $\mathbb{Z}_p$, thus in $\mathbb{Q}_p$.

Proof : This polynomial has a root at every non zero element of $\mathbb{Z}/p\mathbb{Z}$, its derivative never vanishes, so Hensel's lemma determines a unique solution for each element in $\mathbb{Z}/p\mathbb{Z}$. This splits the polynomial so there can be no more roots in $\mathbb{Q}_p$.

Exercise : Roots of Unity in $\mathbb{Q}_p$, part 2 ****

Prove moreover that the roots found in the former exercise for $p > 2$ are the only roots of unity in $\mathbb{Q}_p$. Conclude that $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic as soon as $p \neq q$, and $p, q > 2$. Find the roots of unity in $\mathbb{Z}_2$. Complete this statement by proving that $\mathbb{Q}_2$ and $\mathbb{Q}_p$ are not isomorphic for all $p > 2$.

Proof : Let m be coprime to p, and ζ be an m-th root of unity. We may suppose that $p-1$ divides m. Now using uniqueness in Hensel's lemma for the polynomial $X^m - 1$ proves that there is only one root of unity for each congruence class modulo $p\mathbb{Z}_p$. However, we already found one for each class in the former exercise. Thus all roots of unity of order coprime to p are actually $p-1$ roots of unity.

We will now prove that there are no roots of unity whose order is a power of p, except 1. To do so, suppose there is a p-th root of unity, namely ζ, different from 1. Then we know that since in $\mathbb{Z}/p\mathbb{Z}$, $x^p = x$ for all x, then we know that $\zeta = 1 + pk$. Now ζ is necessarily a root of $(X^p - 1)/(X - 1) = X^{p-1} + X^{p-2} + ... + 1$, but putting this modulo p^2 proves that $p + \frac{p(p-1)}{2}pk = 0$ modulo p^2, so $p = 0$ modulo p^2. Which is impossible.

*For the last part of the proof, we will firstly seek all roots of unity in $\mathbb{Z}_2$. It is easy to see that there are no m-th roots of unity if m is odd : take the first term α in the series of such a number which is non zero. You then have $(1+2^\alpha)^m = 1$ **mod** $2^{\alpha+1}$, which reduces to $1 + m2^\alpha = 1$ **mod** $2^{\alpha+1}$, which is impossible. Now let us check for 2^n-roots of unity. We will prove that they are only 1 and -1. To do so, notice that 4-th roots of unity are only 1 and -1 : this is true because $X^4 - 1$ reduces as $(X-1)(X+1)(X^2+1)$, and -1 has no square root in $\mathbb{Z}_2$ because 3 is not a square modulo 4. Now by induction, an 8-th root of unity's square must be 1 or -1, so it is 1, etc. So all 2^n-th roots of unity are actually 2-roots of unity, namely 1 or -1.*

Finally we must check that $\mathbb{Q}_3$ and $\mathbb{Q}_2$ are not isomorphic (tough they have the same number of roots of unity). For this, just use bigger polynomials : $X^2 + X + 1$ has a root in $\mathbb{Z}/3\mathbb{Z}$ and non zero derivative at this root, so has a root in $\mathbb{Z}_3$. However $\mathbb{Z}/2\mathbb{Z}$ does not, so $\mathbb{Z}_2$ does not. Now if $x \in \mathbb{Q}_2 - \mathbb{Z}_2$, then the 2-adic valuation of x^2, x and 1 are not the same and thus $|x^2 + x + 1|_p = |x^2|_p > 0$. And thus this polynomial has no root in $\mathbb{Q}_2$.

Before moving on from this discussion about polynomials in $\mathbb{Q}_p$, here's an important difference between $\mathbb{Q}_p$ and $\mathbb{R}$.

Exercise : An Infinite Degree Algebraic Closure **

Prove that the algebraic closure of $\mathbb{Q}_p$ has infinite degree over $\mathbb{Q}_p$.

Solution : using's criterion Eisenstein, it is easy to see that the $X^n - p$ is irreducible over $\mathbb{Z}_p$ ($\mathbb{Z}_p$ is a local ring with (p) as an only prime ideal). Then using Gauss' lemma, a polynomial that is irreducible over a factorial ring is irreducible over its fraction ring. This yields extensions of $\mathbb{Q}_p$ of arbitrarily high degree, which conclude. This major comes from the fact that $\mathbb{Q}_p$ admits a description as a fraction field of a ring which is fairly easy to describe, whereas $\mathbb{R}$ hasn't got such an algebraic description.

5.4 Norms and Valuations

In this section, we will now generalize what we have done earlier to the more general setting of what we call **normed fields**.

5.4.1 Norms, Equivalent Norms

Definition : Normed Field

A **normed field** $K, ||$, is a field K with a map $K \to \mathbb{R}$ called a **norm**, which enjoys the following properties :

- Positivity : $|x| \geq 0$
- Separation : $|x - y| \geq 0 \iff x = y$
- Multiplicativity : $|xy| = |x||y|$
- Triangle Inequality : $|x + y| \leq |x| + |y|$

We exclude, in what follows, the case where the norm is simply the discrete norm.

A norm on K clearly turn K into a metric space by defining $d(x, y) = |x - y|$. Properties of d obviously turn K into a topological field. Two norms are said to be **equivalent** if they define the same topology on K. Now here's a nice characterization of equivalence, whose proof is instructive as a first exercise.

Proposition : Characterization of Equivalence of Norms

We have the following equivalences for two norms $||_1$ and $||_2$:

- $||_1 = ||_2^s$ are equivalent.
- For all $x \in K$, $|x|_1 < 1 \implies |x|_2 < 1$.
- There exists $s > 0$ such that $||_1 = ||_2^s$.

Exercise : Proof of the Above ***

1. Prove that if $||_1$ and $||_2$ are equivalent, then $|x|_1 < 1 \implies |x|_2 < 1$.
2. Suppose the second condition is fulfilled. Let $y \in K^*$ be fixed, with $|y|_1 > 1$, and take any other $x \in K$. Then there exists $\alpha \in \mathbb{R}$ such that $|x|_1^\alpha = |y|_1$. By approaching α by rationals above and below, prove that we also have $|x|_2^\alpha = |y|_2$. Use this to prove the third condition.
3. Conclude.

Solution : clearly every open ball in one topology is an open ball in the other. For the second one, use the fact that having norm stricly smaller than one is equivalent to having powers converging to 0. *Using the rationals, obtain* $|x|_1^m < |y|_1^n$ *and thus* $|\frac{x^m}{y^n}|_1 < 1$, *then so for* 2 *by last question. So* $|x|_2^\alpha \leq |y|_2$. *Then the other inequality is obtained by above. Take the logarithms and ratios, call* s *the ratio. It is positive because* $|y|_1$ *and* $|y|_2 > 1$. *It works.*

We now introduce a useful approximation theorem.

Proposition : Approximation Theorem

Let $||_1, ..., ||_n$ be pairwise inequivalent norms on K, and let $a_1, ..., a_n$ be elements of K. Then there for every $\epsilon > 0$ there is an element $x \in K$ such that $|a_i - x| < \epsilon$ for all i.

Proof : We will construct elements z_i which are very close to 1 for $||_i$ and very close to 0 for all others, and then just put $x = \sum^n z_i a_i$. Let's do this for $||_1$.

All we have to do is find an element such that $|x|_1 > 1$ and $|x|_i < 1$ for others. Then all we have to do is consider $\frac{x^n}{1+x^n}$ for n large enough.

We now need to construct such an element. For two elements, just take $|x|_1 < 1$ and $|x|_2 \geq 1$, as well as $|y|_2 < 1$ and $|y|_1 \geq 1$. Now $\alpha = y/x$ does the trick.

If we want to add $||_3$ in here, there are two cases : either $|\alpha|_3 < 1$ and there is nothing to do. Either $|\alpha|_3 \geq 1$. By changing α to $\frac{\alpha^n}{1+\alpha^n}$, you can get it as close as you want to 1 for $||_3$ and arbitrarily close to 0 for $||_2$. Now multiply it by an element not too big, known to be strictly greater than 1 for $||_1$ and strictly smaller than 1 for $||_3$. Repeat by induction.

Exercise : A Link With The Chinese Remainder Theorem

This is a thinking exercise : try to compare this theorem with the chinese remainder theorem.

5.4.2 Archimedean and non-Archimedean Norms

There are two very different types of norms called archimedean or non-archimedan norms.

Definition : Archimedean and Non-Archimedean Norms

A norm is said to be **non-archimedean** if one of the two equivalent properties is verified :

- $|n|$ is bounded.
- $|x + y| \leq \max(|x|, |y|)$ for all $|x|$ and $|y|$.

Else, it is said to be **archimedean**.

Proof : If the max property is fulfilled, then clearly n is bounded by the absolute value of 1. Now if $|n|$ is bounded, then take $|(x + y)^n|$, expand and take the $\frac{1}{n}$-th power (the binomial coefficients will stay bounded). It will be smaller than the largest.

Exercise : A Useful Property of Non-Archimedean Norms ***

Let $||$ be a non-archimedean norm on K. Prove that for $s > 0$, $||^s$ is still an archimedean valuation on K, and deduce that for all $x, y \in K$, if $|x| \neq |y|$ then $|x + y| = \max(|x|, |y|)$.

Solution : the first point is obvious. For the second one, all we need to prove is that if $|m| > 1$ then $|1 + m| = |m|$. We may change $||$ to $||^s$ so that $|m| > 2$. Now, we have $|1 + m| \leq |m|$ and $|m| \leq \max(|m + 1|, |1|)$. But since $|m| > 2$, we have $|m + 1| \geq 1$ so $|m| \leq |m + 1|$, which yields the equality.

Another much easier way to gather this is the following : if $|a| > |b|$, we have $|a + b| \leq |a|$ but also $|a| = |a + b - b| \leq \max(|a + b|, |b|)$, but since $|a| > |b|$ then we must have $|a| \leq |a + b|$.

Exercise : Norms on Function Fields **

Let $K, ||$ be a valued field with a non-archimedean valuation. Prove that $||$ can be extended to a non-archimedean norm on $K(t)$ by defnining $|a_0 + ... + a_n X^n| = \max(|a_0|, ..., |a_n|)$ and $|f/g| = |f|/|g|$.

Solution : we just have to prove that this holds for elements of $K[t]$, the norm obviously translates to the fraction field. The strong triangle inequality is obvious, and for multiplicativity, one can factor by the largest element.

We then have the following surprising fact.

Theorem : Norms on $\mathbb{Q}$

Every norm of $\mathbb{Q}$ is either equivalent to $||_p$ for a prime number p, or to the usual absolute value.

Proof : take a non-archimedean value on $\mathbb{Q}$. Then there must be a prime number p with norm strictly lower than 1, else all numbers of $\mathbb{Z}$ would have value lower than 1 by non-archimedeanity and equal to 1 by prime decomposition. So the valuation would be constant, thus discrete. The ideal of $\mathbb{Z}$ of elements with norm strictly lower than 1 contains $p\mathbb{Z}$, and thus is $p\mathbb{Z}$ since it is maximal. Now for any other element $r = p^s t$ with $t \wedge p = 1$, we have $|r| = |p|^s = |r|_p^\alpha$ for some α independent of r that I leave you to determine. Thus we have the equivalence. We leave the case of the absolute value out of consideration, though it is only a little more technical. See page 120 of Neukirch.

Non-archimedean norms of K are in bijection with **exponential valuations** of K, which are maps from $K \to \mathbb{R} \cup \{\infty\}$, which verify $v(x) = \infty \iff x = 0$, $v(xy) = v(x) + v(y)$ and $v(x + y) \geq \min\{v(x), v(y)\}$. The bijection is obtained by composing the norm with the opposite of the logarithm. Equivalent exponential valuations are defined as defining norms, so equivalently as $v = sv'$ for a given positive s.

Here's a fun exercise on norms.

Exercise : Extensions of the absolute value of $\mathbb{R}$ to $\mathbb{C}$ ***

Prove that the only extension of the absolute value of $\mathbb{R}$ to $\mathbb{C}$ is the usual norm $z \mapsto \sqrt{z\overline{z}}$.

Solution : to do so the only thing we have to prove is that for such a norm $\|z\| = \|\overline{z}\|$, then by multiplicativity we know what to do. A first easy fact is that this is true for element that can be written $re^{2\pi iq}$ where q is rational, because for any such number $\|e^{2\pi iq}\|^m = 1$ for some m and thus $\|e^{2\pi iq}\| = 1$, and so it is true for its conjugate. Now an arbitrary complex number z can be written $r + \epsilon$ where r is of the form above, and ϵ has arbitrarily small coordinates. We then have $\|\overline{z}\| = \|\overline{r} + \overline{\epsilon}\|$. Now, $|\|r\| - \|z\|| \leq \|\epsilon\|$ which is arbitrarily small by the fact that $\|i\|^2 = 1$ so $\|i\| = 1$ and triangle inequality. So by manipulating triangle inequalities we obtain that $|\|\overline{z}\| - \|z\||$ is smaller than any real number, and so the two are equal.

5.4.3 Valuation Rings, Discrete Valuation Rings

In all this section, K is a field valued by a non-archimedean norm. This situation arises in particular with the fields $\mathbb{Q}_p$, as well as all the function fields on the $\mathbb{Q}_p$ with extended norm.

Such an object can be studied through certain objects that are associated to it.

Definition : Valuation Ring Associated to a Valued Field

The subset $\mathcal{O} \subset K$ of elements of norm smaller or equal to 1, or equivalently of valuation greater than 0, is the **valuation ring** associated to K. Its group of units $\mathcal{O}^*$ is equal to the elements of norm 1 / valuation 0, and it has a unique maximal ideal $\mathfrak{p}$ consisting of the elements of norm strictly smaller than 1 / valuation strictly greater than 0.

The field $\mathcal{O}/\mathfrak{p}$ is called the **residue class field** of $\mathcal{O}$.

Verifications : the only not completely trivial thing is that the ideal is the only maximal ideal. The idea is that any other strict ideal is contained in there.

The valuation rings follows the following properties :

Proposition : Properties of Valuation Rings

- For all $x \in K$, x or $x^{-1} \in \mathcal{O}$.
- The ideals of $\mathcal{O}$ are totally ordered by inclusion.
- $\mathcal{O}$ is integrally closed.

Proof : The first property is immediate. The second property is clear, ideals are ordered by the supremum of the valuations of their elements. Integral closure is simply that if $x \notin \mathcal{O}$ but $x^n + \sum a_i x_i = 0$, then x can be expressed in terms of $x^{-1} \in \mathcal{O}$, contradiction.

All this becomes interesting when the valuation is said to be **discrete**.

Definition : Discrete Valuation and Discrete Valuation Rings

A valuation is said to be discrete if its image is discrete in $\mathbb{R}$, so is $s\mathbb{Z}$. Up to equivalence, in this case, we will always suppose that the image is $\mathbb{Z}$.

The associated ring is then said to be a **discrete valuation ring**. It is a principal ideal domain and a local ring. A generator π of the only maximal ideal is said to be **a prime element**, and the ideals of $\mathcal{O}$ are generated by the π^n. The norm on K is then re-written $||_{\mathfrak{p}}$, and the norm of an element a is given by the norm of the highest power of π that divides it.

There is a chain of multiplicative subgroups $\mathcal{O}^* \supset U^{(1)} \supset U^{(2)} \supset U^{(3)}...$ where $U^{(n)}$ is defined as :

$$1 + \mathfrak{p}^n = B(1, |\pi|_{\mathfrak{p}}^n) = \{x \in K |\ |x| \leq |\pi|_{\mathfrak{p}}^n\}$$

They are called the **higher unit groups** of $\mathcal{O}$.

Verifications : for principality, classify ideals by the elements of minimal valuation / maximal norm that it contains : they generate the ideals. For locality, this was already true for more general valuation rings. The ideals of $\mathcal{O}$ of minimal norms are all the same up to multiplication, so use the proof of maximality. Clearly the norm of an element is the norm of the highest power of π that divides it (check how invertible or not is an element, by the ideal it generates).

The presented subgroups all contain 1, are clearly stable under multiplication and also under inversion by considering the fact that if $x \in U^{(n)}$, then $|1 - x^{-1}| = |x|^{-1}|1 - x| = |1 - x|$. Alternatively, if $((1 + a\pi^n)^{-1} - 1) \times (1 + a\pi^n) = -a\pi^n$ so we're ok.

Here's an important fact presented as an exercise but that you should see as basic knowledge.

Exercise : Some Isomorphisms **

Prove the following isomorphisms of abelian groups, with the former notations :

1. $\mathfrak{p}^n/\mathfrak{p}^{n+1} \simeq \mathcal{O}/\mathfrak{p}$
2. $\mathcal{O}^*/U^{(n)} \simeq (\mathcal{O}/\mathfrak{p}^n)^*$
3. $U^{(n)}/U^{(n+1)} \simeq \mathcal{O}/\mathfrak{p}$

Solution : the first one comes from the morphism $\mathfrak{p}^n \to \mathcal{O}/\mathfrak{p}$, $\pi^n a \mapsto a$. The second one comes from the morphism $\mathcal{O}^* \to (\mathcal{O}/\mathfrak{p}^n)^*$, where an element is sent to 1 if and only if it is in $1+\mathfrak{p}^n$. The third one comes from the morphism $U^{(n)} \to \mathcal{O}/\mathfrak{p}$, $1 + a\pi^n \mapsto a$, whose kernel is indeed $U^{(n+1)}$ (check that this map does turn multiplication into addition).

5.4.4 A Conclusive Exercise

Here's a problem to sum things up and review our definitions.

Exercise : Valuations on $k(t)$ trivial on k^* ***

Let k be a field and $k(t)$ be the function field in one variable. We want to find all the valuations on $k(t)$ which are trivial on k^* (such that $v(k^*) = 0$).

1. Suppose $v(t) \geq 0$. Prove that v is equivalent to an exponential valuation associated to a prime ideal $\mathfrak{p} = (p(t))$ of $k[t]$.
2. Suppose $v(t) < 0$. Prove that v is equivalent to the degree valuation v_∞ (where $v_\infty(f/g) = \deg(g) - \deg(f)$).
3. What are the residue class fields ?
4. Find another valuation that does not satisfy the condition $v(k^*) = 0$. Notice that it is not equivalent to the former. If you can, find its residue class field.

Solution : If $v(t) \geq 0$, notice that v is positive on all of $k[t]$ by ultrametric property. Then in $k[t]$ there is at least one prime polynomial of valuation greater than 0 (else the valuation would be trivial). Then one can reproduce the proof of the case of $\mathbb{Q}$ to prove that the valuation is equivalent to the one associated to this prime ideal.

If $v(t) < 0$, then our small exercise on non-archimedean norms proved that if $|x| \neq |y|$ then $|x+y| = \max(|x|, |y|)$. Similarly, for non-archimedean valuations, we have $v(x) \neq v(y) \implies v(x+y) = \min(v(x), v(y))$. So for a polynomial $P(t)$, its valuation must be that of its term of biggest degree, namely $\deg(f)v(t)$. It is then obvious that the valuation is equivalent to the degree valuation.

Let's compute the residue class fields. In the first case, the discrete valuation ring is $k(t)_{(\mathfrak{p})}$, fractions with denominator not divisible by $\mathfrak{p}$. Then quotienting by $\mathfrak{p}k(t)_{(\mathfrak{p})}$ yields $k[t]/\mathfrak{p}$, through the morphism $k(t)_{(\mathfrak{p})} \to k[t]/\mathfrak{p}$, $\frac{f}{g} \mapsto fg^{-1}$. In the second case, the discrete valuation ring is the one of rational fractions of negative degree, and the elements of value greater than 1 generated by the fraction $\frac{1}{X}$. So quotienting by them yields k, since any fraction of degree 0 can be written in a unique way as $a + \frac{1}{X}R$, with $a \in k$ where R is a rational fraction of negative degree.

For another valuation, the extension proposed in one of the exercises above is a valid choice : choose a valuation on k, and let f's valuation be the minimal valuation of its coefficients. For example, one can do this on $\mathbb{Q}(t)$ and take the valuation $||_p$. The ring of elements with valuation greater than 0 is the subring of $\mathbb{Q}(t)$ of elements that can be written as P/Q where Q is in $\mathbb{Z}[t]$ and has content coprime to p (this is a multiplicative subset), and $P \in \mathbb{Z}_{(p)}(t)$. Its residue class field is $\mathbb{Z}/p\mathbb{Z}(t)$, as can be obtained by reduction modulo (p) of numerator and denominator (remember that $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p\mathbb{Z}$ through $\frac{a}{b} \mapsto ab^{-1}[p]$). This description is slightly involved : it would be better described through another algebraic tool called localization.

5.5 Completions

As you'd expect, a normed field is complete with respect to its norm if every Cauchy sequence converges. If a field is not complete, we can take the usual path of taking the Cauchy Sequences and quotienting by the maximal ideal of the nullsequences to obtain a larger complete topological field. For a normed

field $(K, ||)$, its completion is often denoted $(\hat{K}, \hat{||})$. We also easily obtain that the completion with respect to $||$ is unique. To turn our focus to the right things right away, we will accept the following impressive theorem (whose proof is not that enlightening for our number theoretic concerns).

Theorem : Ostrowski's Theorem

Let K be a field which is complete to an archimedean norm $||$. Then there is an isomorphism of K onto $\mathbb{R}$ or $\mathbb{C}$, such that $|a|_K = |\sigma(a)|_{\mathbb{C}}^s$ for some fixed $s \in (0; 1]$.

So, what will be working on are completions of fields for non-archimedean norms, or equivalently, exponential valuations. Note that the norm of $(\hat{K}, \hat{||})$ is defined by $|\hat{a}| = \lim |a_n|$, which exists since it is a Cauchy Sequence in $\mathbb{R}$. It is obviously still non-archimedean by continuity of the maximum, or by characterization of non-archimedean norms. The valuation, $\hat{v}$, is similarly defined by taking the opposite of the logarithm of the norm (it is infinite if and only if $a = 0$). Note that we have $v(K^*) = \hat{v}(\hat{K}^*)$, since the sequence $v(a_n)$ becomes stationary after a while ($v(a) = v(a - a_n + a_n) = \min(v(a - a_n), v(a_n))$ if they are different. However $v(a - a_n)$ becomes really big). It is thus obvious that if v is discrete and normalized, then so is $\hat{v}$. Thus, the defining features of a normed field (the field K, the valuation v, the discrete valuation ring $\mathcal{O}$, the corresponding maximal ideal $\mathfrak{p}$ and its powers $\mathfrak{p}^n$) can all be described in $\hat{K}$, and will be referred to with a hat $\hat{}$.

Also, note that in case of a discrete valuation, the maximal ideal $\hat{\mathfrak{p}}$ is still principal, and is equal to $\mathfrak{p}\mathcal{O} = \pi\mathcal{O}$, since π is defined as being an element of smallest possible valuation, that the embedding is isometric and that the span of the valuations are the same after or before completion.

We then have the following facts, which mirror the situation we encountered in $\mathbb{Q}_p$.

Proposition : Link Between Features of A Normed Field and its Completion

In a completed field with respect to a non-archimedean norm, the embedding $\mathcal{O} \hookrightarrow \hat{\mathcal{O}}$ induces isomorphisms...

$$\hat{\mathcal{O}}/\hat{\mathfrak{p}} \simeq \mathcal{O}/\mathfrak{p}$$

...and in the case of discreteness :

$$\hat{\mathcal{O}}/\hat{\mathfrak{p}}^n \simeq \mathcal{O}/\mathfrak{p}^n$$

Proof : The proof has already been seen before. The isomorphism comes from the map $\mathcal{O} \to \hat{\mathcal{O}}/\hat{\mathfrak{p}}$, which clearly has kernel $\mathfrak{p}$ since the injection $K \to \hat{K}$ is isometric, and is surjective as $\mathcal{O}$ is dense in $\hat{\mathcal{O}}$: for elements of $\hat{\mathcal{O}}$, one can find elements in $\mathcal{O}$ that are of distance less than 1, and thus so that the difference is in $\mathfrak{p}$. The exact same idea serves the second proof (you can choose the valuation of the difference to be as large as you'd like).

This isomorphism isn't just an abstract structural isomorphism between two unrelated algebraic structures : the proof gives an explicit description of this isomorphism, and proves that representatives of the classes in $\hat{\mathcal{O}}/\hat{\mathfrak{p}}$ can be taken to be classes of elements of $\mathcal{O}$.

The analogy with p-adic numbers goes further with this theorem :

Proposition : Representations of Elements as Series

Let $R \subset \mathcal{O}$ be a system of representatives of $\mathcal{O}/\mathfrak{p}$, with 0, and let π be a prime elemnt. Then every $x \neq 0$ in $\hat{K}$ admits a unique representation as a convergent series :

$$x = \pi^m \left(\sum_{i=0}^{\infty} a_i \pi^i\right)$$

... with $m \in \mathbb{Z}$, $a_i \in R$ and $a_0 \neq 0$.

Proof : such a series is always convergent, because non zero representatives in R all have norm 1, so the general term goes to 0 in terms of norms. Uniqueness is obtained through this line of reasoning : if such a non-zero series is 0, simplify by the π coefficient. Then write $\sum_{i=0}^{\infty} a_i \pi^i = a_0 + \pi y$ and quotient by $\mathfrak{p}$, to obtain an element of $\mathcal{O}/\mathfrak{p}$. It must be 0, so a_0 is the $\mathfrak{p}$ representative in R, namely 0, which proves that the whole thing must be 0.

*For existence, if $x \neq 0$, consider the valuation of x. So you can write $x = \pi^m y$ where y has valuation 0. Now modding out by $\hat{\mathfrak{p}}$, we have $y = a_0$ **mod** $\hat{\mathfrak{p}}$. Lift a_0 through R (because $\mathcal{O}/\mathfrak{p} \simeq \hat{\mathcal{O}}/\hat{\mathfrak{p}}$. Then $y - a_0$ is in $\hat{\mathfrak{p}}$. Mod by $\mathfrak{p}^2$ and find $a_1\pi$. $y - a_0 - a_1\pi$ is now in $\mathfrak{p}^2$. Keep on going and find that the series converges to y.*

These two theorems may feel like abstract theorems, but I will try and convince you that they actually are practical theorems that allow you to actually do computations. Given a field K like $\mathbb{Q}$ and $k(t)$, and a non-archimedean valuation derived from a prime ideal $\mathfrak{p}$ of $\mathbb{Z}$ or (t), it is now accessible to easily compute the Laurent series development of any element from the base field.

For example, here's a kind of calculation we already performed. Say you are working in $\mathbb{Q}_7$, and you'd like to know what $\frac{13}{5}$ looks like. You (or a computer) can simply compute :

$$13 \times 5^{-1} = 4 \textbf{ mod } 7$$

$$13 \times 5^{-1} - 4 = 4 \times 7 \textbf{ mod } 49$$

$$13 \times 5^{-1} - 4 - 4 \times 7 = 5 \times 49 \textbf{ mod } 343$$

... and so you obtain $\frac{13}{5} = 4 + 4 \times 7 + 5 \times 49$.... Our theorems above generalize this situation.

Say that you'd like to compute the expansion of $\frac{1+X}{X^2}$ in $\mathbb{Q}(X)$ completed for the valuation associated to the prime ideal $(X^2 + X + 1)$.

$$(1+X)(X^2)^{-1} = (1+X)(X) = X^2 + X = -1 \textbf{ mod } 1 + X + X^2$$

$$(1+X)(X^2)^{-1} + 1 = (1+X)(2X^3 + 3X^2 + 4X + 1) + 1 = X(1 + X + X^2) \textbf{ mod } (1 + X + X^2)^2$$

... and you may keep going as far as you want, with the right computational tools. A computer actually could.

Exercise : Putting things in Practice **

Using the former proposition, describe the completions of the following normed fields :

1. $\mathbb{C}(t)$ for the valuation associated to the prime ideal $(t-2)$.
2. $\mathbb{Q}(t)$ for the valuation associated to the prime ideal $(t^2 - 2)$.
3. Generalize the two former examples.
4. $k(t)$ where k is any field, for the valuation v_∞.

Solutions : the key of this exercise is that although one may not know what the normed field looks like, one can still compute the residue class field, since the former theorem tells us that it comes from the residue field of the discrete valuation ring. In the first one, we know that from an earlier exercise the residue class field is $\mathbb{C}[t]/(t-2) \simeq \mathbb{C}$, where representatives of classes in the discrete valuation ring $\mathbb{C}(t)_{(t-2)}$ are obtained by taking elements of $\mathbb{C} \subset \mathbb{C}(t)_{(t-2)}$. So the elements of $\hat{\mathbb{C}(t)}$ for this valuation are represented one to one by converging series $(t-2)^m \sum_{i=0}^{\infty} c_i (t-2)^i$, with $c_0 \neq 0$ and $c_i \in \mathbb{C}$.

The second one is the same, but this time the residue class field is $\mathbb{Q}[t]/(t^2-2) \simeq \mathbb{Q}[\sqrt{2}]$. *Representatives are obtained in* $\mathbb{Q}(t)_{(t^2-2)}$ *by elements of the form* $a+bt$. *Thus the elements are obtained of the form* $(t^2-a)^m \sum_{i=0}^{\infty} q_i (t^2-2)^i$, *where* q_i *is a degree* 1 *polynomial in* $\mathbb{Q}(t)$.

A generalization of this is that for a field k *with function field* $k(t)$, *and a valuation associated to an irreducible polynomial* P, *then the completion is the formal series with coefficients in* $k[t]/P$, *starting at possibly finite negative indices.*

For the last example, we found that the residue class field was k, *so a similar line of reasoning as before proves that the elements look exactly the same, with* $\pi = \frac{1}{X}$, *and the* $a_i \in k$.

Here's a great exercise to put things in perspective.

Exercise : Periodic Developments ****

1. Prove that a real number $x \in \mathbb{R}$ is in $\mathbb{Q}$ if and only if its decimal development in any base is periodic after a certain rank.
2. Prove that a p-adic number $x \in \mathbb{Q}_p$ is in $\mathbb{Q}$ if and only if its development $p^m \sum_{i=0}^{\infty} a_i \pi^i$ is periodic after a certain rank. *You may use the exercise stating that if a p-adic integer has a development which is periodic after a certain rank, then so does its opposite.*
3. Prove that an element of $\hat{\mathbb{F}_p(t)}$, the completed of $\mathbb{F}_p(t)$ for the valuation associated to a prime ideal $\mathfrak{p}$ is in $\mathbb{F}_p(t)$ if and only if its development as a Laurent series is periodic.
4. Prove that this theorem fails in $\mathbb{Q}(t)$ (for example, you may compute the development of $\frac{1}{X}$ as a Laurent series in the completed of $\mathbb{Q}(t)$ for the prime ideal $(X-a)$.

Solution : For the first case, it is easy to see that if an element $t \in \mathbb{R}$ *has a periodic development in base* $\lambda \geq 2$, $\lambda \in \mathbb{N}$, *one has* $t = r + \lambda^m \sum_{i=0}^{\infty} a_i \lambda^{-i} = r + \lambda^m u \sum_{i=0}^{\infty} \lambda^{-ni}$ *for a certain element* $u < \lambda^n$ *and* r *with a finite number of decimals, which is equal to* $r + \frac{\lambda^m u}{1-\frac{1}{\lambda^n}}$. *Now the reciprocal consists in seeing that any rational number can be written in this form. To do so, take a rational* $\frac{a}{b}$, *and start by factoring all the* λ *you can. This yields* $\lambda^m \frac{a'}{b'}$. *Now exclude* r *so that* $\lambda^m \frac{a'}{b'} = r + \lambda^m \frac{c}{b'}$ *with* $0 \leq c < b'$. *The last thing we have to show is that* $b' | \lambda^n - 1$ *for some* n. *To do so, remember that* λ *is invertible in* $\mathbb{Z}/b'\mathbb{Z}$, *it has finite order so its inverse is a power of itself. And thus there is an* n *such that* $1 - \lambda^n = 0$ ***mod*** b'. *Multiply above and under, and boom.*

For the second one, there isn't a lot more to do. One just has to see that the series $\sum_{i=0}^{\infty} p^{ni}$ *does indeed converge to* $\frac{1}{1-p^n}$. *Then it is clear that an element with a periodic development after a certain rank can be written as* $r + \frac{p^m u}{1-p^n}$ *where* r *has a finite development, and* $0 < u < p^n$. *Now conversely, if an element is rational and positive, with the same method as above, you may write it* $r + \frac{p^m u}{1-p^n}$ *where* r *is a positive integer and* $0 \leq u < p^n$ *and thus has a finite development. This has a periodic development, and so do all rational numbers by passing to the opposite.*

For the third question, one first easy check is that polynomials in $\mathbb{F}_p[t]$ *all have a finite expansion as a Laurent series (remember that the residue class field of such a field is* $\mathbb{F}_p[t]/\mathfrak{p}$ *and is represented by the elements of the vector space generated by* $1, t, t^2, ..., t^{n-1}$ *where* n *is the degree of a generator of* $\mathfrak{p}$. *Thus a development of* $P \in \mathbb{F}_p[t]$ *can be computed by doing several euclidean divisions by a generator of* $\mathfrak{p}$.

The proof that elements with periodic developments are in $\mathbb{F}_p(t)$ *is the usual proof : take out the non-periodic part, factor* $\mathfrak{p}$ *and obtain something of the form* $T + \mathfrak{p}^m \frac{u}{1-\mathfrak{p}^n}$ *where the degree of* u *is strictly smaller than that of* $\mathfrak{p}^n$. *Now what we need to do is prove that any rational fraction can be put in the following form. Once again, factor by* $\mathfrak{p}$, *take out* r, *and the situation you get is* $r + \mathfrak{p}^m \frac{a}{b}$ *where* a, b *are coprime with* $\mathfrak{p}$ *and* $\deg a < \deg b$. *You now just have to multiply* b *and* a *by* c *such that* $bc = 1 - \mathfrak{p}^n$. *But since* b *is coprime to* $\mathfrak{p}$, *then* $\mathfrak{p}$ *is invertible in the ring* $\mathbb{F}_p[t]/(b)$. *So a certain power of* $\mathfrak{p}$ *is* 1 *in here, and so here we are.*

One can easily check by induction that $\frac{1}{t} = \sum_{i=0}^{\infty} \frac{1}{a^{i+1}}(t-a)^i$ *in this field, and thus the expansion of* $\frac{1}{t}$ *is not periodic, although* $\frac{1}{t}$ *is in* $\mathbb{Q}_p(t)$.

Chapter 6

Galois Cohomology

In this new part, we introduce the basic tools for applying Group Cohomology to number theory, mainly to study Galois groups of certain extensions.

6.1 Galois modules and Cohomology

Let k be a field, and $\overline{k}$ a separable closure of k. We denote $\Gamma_k = \mathbf{Gal}(\overline{k}/k)$. It is a profinite group, which acts on different discrete Γ_k-modules: for any subextension $k \subset L \subset \overline{k}$...

1. $(L, +)$ is a discrete $\mathbf{Gal}(\overline{k}/k)$-module.
2. $(L^*, \cdot)$ is also a discrete $\mathbf{Gal}(\overline{k}/k)$-module.
3. $(\mu_n, \cdot)$, the group of n_{th}-roots of unity in L is a discrete $\mathbf{Gal}(\overline{k}/k)$-module.

In the category of discrete Γ_k-modules, we can implement the theory of cohomology we introduced in the preceding chapter : this is called **Galois Cohomology**.

The central point in our study will be the groups $H^n(\Gamma_k, \overline{k}^*)$ for k a given field.

First of all, we have to mention a few tedious but necessary lemmas, that the groups $H^n(\Gamma_k, \overline{k}^*)$ do not depend on the construction of $\overline{k}^*$, which is not canonical. We leave their proofs to the reader.

Proposition : Natural Maps in Galois Cohomology

Let k, l be a fields, $\overline{k}^*, \overline{l}^*$ be separable closures of k and l. Let $i : k \to l$ be a field homomorphism.

- This induces a non canonical map between the $\tilde{i} : \overline{k}^* \to \overline{l}^*$, where $\tilde{i}(\overline{k}^*)$ is a Galois subextension of $\overline{l}^*/i(k)$.
- $\tilde{i}$ induces by conjugation a continuous homomorphism $f : \Gamma_l = \mathbf{Gal}(\overline{l}^*/l) \to \mathbf{Gal}(\overline{k}^*/k) = \Gamma_k$.
- For any Γ_k-Module M, f induces homomorphisms between $H^n(\Gamma_k, M) \to H^n(\Gamma_l, M)$.
- The constructed map does not depend on the choices of the separable closures $\overline{k}^* \to \overline{l}^*$ or of the choice of the map $\tilde{i}$.

Proof : Left to the reader.

Proposition : Naturality of Galois Cohomology

If K and K' are two separable closures of k, then for any Galois module M the groups $H^n(\mathbf{Gal}(K/k), M)$ and $H^n(\mathbf{Gal}(K'/k), M)$ are canonically isomorphic.

Proof : Left to the reader.

6.2 Cohomology of the Additive Group

The cohomology of the additive group of a field does not hold much information.

Proposition : Cohomology of the Additive Group

Let L/k be a Galois, finite extension. Then $H^n(\mathbf{Gal}(L/k), (L, +)) = 0$ for all $n > 0$. Hence, $H^n(\mathbf{Gal}(\overline{k}/k), \overline{k}) = 0$.

Proof : thanks to the primitive element theorem, L is isomorphic (although not naturally) to $I_{\boldsymbol{Gal}(L/k)}(\mathbb{Z})$, by choosing an element α such that $(\sigma(\alpha))$, $\sigma \in \boldsymbol{Gal}(L/k)$ is base of L, and sending $\sum_{i=1}^{n} a_i\sigma_i(\alpha)$ to the right function. The rest follows by construction of the homology group.

Exercise : The Artin Schreier Theorem **

Let k be a field of characteristic p. Let $\phi : \overline{k} \to \overline{k}$ defined by $\phi(x) = x^p - x$.

1. Prove ϕ is surjective.
2. What is the kernel of ϕ ?
3. Deduce that $H^1(k, \mathbb{Z}/p) = k/\phi(k)$ and $H^q(k, \mathbb{Z}/p) = 0$ for $q > 1$.

Solution : first question is separability of $X^p - X - a$, second is $\mathbb{Z}/p$ and third question is long cohomology sequence ($\overline{k}^{\boldsymbol{Gal}(\overline{k}/k)} = k$) on $0 \to \mathbb{Z}/p \to \overline{k} \to \overline{k} \to 0$ and use of the latter theorem.

6.3 Cohomology of the Multiplicative Group

The cohomology of the multiplicative group $H^n(\mathbf{Gal}(\overline{k}/k), \overline{k}^*)$ is more interesting. This classic theorem tells us that this cohomology starts in degree 2.

Proposition : The Hilbert 90 Theorem

Let L/k be a Galois, finite extension. Then $H^1(\mathbf{Gal}(L/k), L^*) = 0$ for all $n > 0$. Hence, $H^1(\mathbf{Gal}(\overline{k}/k), \overline{k}^*) = 0$.

This can be proven easily enough through the definition with cochains: let $s \mapsto a_s$ a cocycle in Z^1 (which are essentially elements $a_s \in L^*$ for each $s \in \boldsymbol{Gal}(L/k)$ such that $a_{st} = s(a_t) \cdot a_s$). By linear independence of characters, there is an element $c \in L^*$ such that $b = \sum a_t t(c) \neq 0$. Then use the cochain relationship to prove that $a_s = s(b^{-1})/b^{-1}$.

This theorem doesn't take much to prove, but its cohomological consequences are absolutely major. Here is an example of application (we will see many others).

Proposition : The First Cohomology Group of the Roots of Unity

We have $H^1(\mathbf{Gal}(\overline{k}/k), \mu_n) \simeq k^*/(k^*)^n$.

Exercise : Kummer Theorem **

Using the long exact sequence and the Hilbert 90 theorem, prove that $k^*/(k^*)^n \simeq H^1(\mathbf{Gal}(\overline{k}/k), \mu_n)$.

Solution : use $1 \to \mu_n \to k^* \to (k^*)^n \to 1$.

6.4 Brauer Group

So, the cohomology of the multiplicative group of a field only starts at $n = 2$. This group is of central importance : so much that it has a name.

Definition : Brauer Group of a Field

Let k be a field. The **Brauer Group** of k is the group $H^2(\mathbf{Gal}(\overline{k}/k), \overline{k}^*)$. It is denoted $\mathbf{Br}\ k$.

Short exact sequences allow us to retrieve some information about these groups. Here's an example.

Exercise : The n-torsion of Brauer Groups **

Let n be coprime with the characteristic of a field k. Using the latter theorem and a well chosen exact sequence, prove that $H^2(k, \mu_n) \simeq (\mathbf{Br}\ k)[n]$.

Solution : For the first question, use $1 \to \mu_n \to k^* \to k^* \to 1$. *Notice that via the choice of a root of unity, this is essentially saying that if* $\mu_n \subset k$, *then* $H^2(k, \mathbb{Z}/n) \simeq (\boldsymbol{Br}\ k)[n]$ *(*$\mathbb{Z}/n$ *with trivial action this time).*

6.5 Cohomological Dimension of a Field

The cohomological dimension (strict, p-dimension...) of a field is simply the cohomological dimension (strict, p-dimension...) of $\mathbf{Gal}(\overline{k}/k)$. In this section we will describe some properties of the cohomollogical dimension of certain fields.

Proposition : p-cohomological dimension of a Field of Characteristic p

Let k be a field of characteristic p. Then $\mathbf{cd}_p(\mathbf{Gal}(\overline{k}/k)) \leq 1$.

Proof : Prove that a p-Sylow of a profinite group is closed (it is compact as a limit of p-groups), then take a p-Sylow of $\boldsymbol{Gal}(\overline{k}/k)$, *take the corresponding extension* K/k *and note that you now only need to prove that* $H^2(\boldsymbol{Gal}(\overline{k}/K), \mathbb{Z}/p) = 0$. *This is a simple consequence of Artin-Schreier, and ultimately a consequence of the sequence* $0 \to \mathbb{Z}/p \to \overline{k} \to \overline{k} \to 0$ *and noting that the cohomology of the additive group of a Galois field extension is trivial.*

For prime numbers different from the characteristic, much of the information about cohomological dimension is inside the Brauer group.

Proposition : The Brauer Group and Cohomological Dimension

Let p be a prime number coprime to the characteristic of k. Then the following conditions are equivalent :

- $\mathbf{cd}_p(\mathbf{Gal}(\overline{k}/k)) \leq 1$.
- For all algebraic separable extension K of k, $(\mathbf{Br}\ K)[p] = 0$.
- For all finite separable extensions K of k, $(\mathbf{Br}\ K)[p] = 0$.

Solution : For the first one, see that $\boldsymbol{Gal}(\overline{k}/K)$ *is a closed subgroup of* $\boldsymbol{Gal}(\overline{k}/k)$ *so it has lower p-cohomological dimension. Notice then that* $(\boldsymbol{Br}\ K)[p] = 0$ *can be described as* $H^2(\boldsymbol{Gal}(\overline{k}, K), \mu_p)$ *since p is coprime with the characteristic of k.* $2 \implies 3$ *is trivial.* $3 \implies 1$ *has a very elegant proof : what we want to show is that if* $\boldsymbol{Gal}(\overline{k}/K_p)$ *is a p-Sylow of* $\boldsymbol{Gal}(\overline{k}/k)$ *then* $H^2(\boldsymbol{Gal}(\overline{k}/K_p), \mathbb{Z}/p) = 0$*. The way to do this is firstly to notice that* K_p *contains the roots of unity since* $[K_p(\mu_p) : K_p]$ *is divisible by* $p-1$ *(because* μ_p*) and by p (since* $\boldsymbol{Gal}(\overline{k}/K_p)$ *is pro-p). Take the finite extension* K' *over k by the roots of unity. Then* $H^2(\boldsymbol{Gal}(\overline{k}/K_j), \mathbb{Z}/p) = 0$ *by hypothesis (note that we cannot use Artin-Schreier since we are not in characteristic p anymore). Then do a projective limit on the open subgroups* $\boldsymbol{Gal}(\overline{k}/K_j)$ *where* K_j/k *is finite and Galois, contained in* K_p*, to obtain* $\boldsymbol{Gal}(\overline{k}/K_p)$*. Since all sequences become zero eventually, so this yields* $H^2(\boldsymbol{Gal}(\overline{k}/K_p), \mu_p) = 0$*. See that since* $\mu_p \subset K_p$*, the action is trivial so this essentially means* $H^2(\boldsymbol{Gal}(\overline{k}/K_p), \mathbb{Z}_p) = 0$ *which finishes the proof.*

Exercise : An Extension of the Theorem if k is Perfect **

Prove if k is perfect of characteristic p, then for any algebraic separable extension K of k, $(\mathbf{Br}\ K)[p] = 0$.

Solution : K is again perfect (it is easy to prove from the definitions that an algebraic extension of a perfect field is still perfect). $x \mapsto x^p$ *is thus an isomorphism and so since multiplication is universal, multiplication by p is also an isomorphism in* $\boldsymbol{Br}\ K$*.*

This implies in particular that fields of characteristic 0, or perfect fields with cohomological dimension 1 have a zero Brauer group. And this is extremely useful, because this allows us to put zero groups in cohomology at the level of the H^2, which gives meaning to exact sequences.

Bibliography

[1] David Harari. *Galois cohomology and class field theory*. Springer, 2020.

[2] Luis Ribes and Pavel Zalesskii. "Profinite groups". In: *Profinite Groups*. Springer, 2000, pp. 19–77.

[3] Emily Riehl. *Category theory in context*. Courier Dover Publications, 2017.

[4] Ravi Vakil. *Spectral Sequences: Friend or Foe?* 2008.

[5] Charles A Weibel. *An introduction to homological algebra*. 38. Cambridge university press, 1995.