For which (n, p) can $\mathfrak{S}_n$ arise as the Galois group of an extension of $\mathbf{Q}_p$?

Théo Untrau

Internship carried out at the Universität Duisburg-Essen under the supervision of Prof. Dr. Vytautas Paškūnas

Abstract

This document is my report of an internship of two months and a half at the University of Duisburg-Essen, at the end of my first year of Master.

The first aim was to answer the question that constitutes the title of this work. $\mathbf{Q}_p$ denotes the field of p-adic numbers, which are introduced quite briefly in this text, so I refer to [Ro] for a better presentation. $\mathfrak{S}_n$ denotes the group of permutations of $\{1, \dots, n\}$, while $\mathfrak{A}_n$ will denote the subgroup of even permutations in $\mathfrak{S}_n$. The answer for the existence of extensions appears in section 5.5.

Before this, we prove some general results on fields K that are complete with respect to a discrete valuation, $\mathbf{Q}_p$ and its extensions being the main example of such fields in this document. For instance, their ring of integers is a discrete valuation ring, we have a very powerful analog of Newton's algorithm to approximate roots of a polynomial, and if L/K is a finite extension, then the valuation on K extends uniquely to a valuation on L.

This naturally leads to the notion of ramification, and this is the point of section 3. At the end of this section, ramification groups will allow us to make a great step in our way to answer the main question. Indeed, we prove that a finite Galois extension $L/\mathbf{Q}_p$ has a solvable Galois group ! Since $\mathfrak{S}_n$ is not solvable as soon as $n \geqslant 5$, we can already exclude many cases.

After a brief discussion on Galois groups of polynomials, we can complete our first aim. But once we know for which (n, p) there exist extensions, a natural question one may ask is : How many extensions are there in a fixed algebraic closure with the prescribed Galois group ? What do they look like ? This is the second aim of this internship : Classify the extensions when they exist. In section 6, the cases where I found an answer are presented, while appendix 7.6 contains my state of advancement for the remaining cases.

Acknowledgements

First, I would like to thank my ALGB (Algèbre de base) teacher, Prof. Tobias Schmidt, for teaching me with great clarity all the notions I needed to start this internship. I also thank him for contacting his acquaintances at the University in Essen, because this is how I had the chance to exchange with my supervisor in the first place. I am grateful to Prof. Jochen Heinloth, for welcoming me in his class on class field theory, patiently bridging some of my gaps, and taking an interest in my studies in France. Finally, many thanks to Prof. Vytautas Paškūnas, for giving me this problem, which I really envoyed working on. I also thank him for solving all the problems I did not manage to solve by myself, this work would not exist without his help.

Contents

1 p-adic numbers

We define the ring of p-adic integers as the projective limits of the rings $\mathbf{Z}/p^n\mathbf{Z}$:

$$\mathbf{Z}_p := \varprojlim_{n \geqslant 1} \mathbf{Z}/p^n\mathbf{Z}$$

See appendix 7.2 for more details. It is easy to prove that $\mathbf{Z}_p$ is an integral domain, and this justifies the following definition :

Definition 1.1. *The field of fractions of $\mathbf{Z}_p$ is called the field of p-adic numbers, and is denoted by $\mathbf{Q}_p$.*

Remark : We will give another way to define the field $\mathbf{Q}_p$ in the section about valued fields. These definitions come a bit quickly, and lack some motivations and examples, but a more detailed and illustrated introduction to p-adics can be found in [Ro] for instance.

2 Valued fields

2.1 First definitions and examples

Let K be a field. An absolute value over K is a map $|.| : K \to \mathbf{R}_+$ such that :

$$\forall (x,y) \in K^2,\ |xy| = |x|.|y|$$

$$\forall (x,y) \in K^2,\ |x+y| \leqslant |x| + |y|$$

$$\forall x \in K,\ x = 0 \iff |x| = 0$$

A field with an absolute value on it is called a *valued field.*

The absolute value $|.|$ is called *nonarchimedean* if $|n|$ stays bouded for all $n \in \mathbf{N}$. Otherwise it is called *archimedean.*

Proposition 2.1. *The absolute value $|.|$ is nonarchimedean if and only if for all $x, y \in K$ one has :*

$$|x+y| \leqslant \max(|x|, |y|)$$

Proof. See [Ne], Proposition (3.6) □

If $(K, |.|)$ is a field together with an absolute value, then K can be made a metric space by setting that the distance between x and y is $|x-y|$. If the absolute value is nonarchimedean, then it satisfies the strong triangle inequality above, and so K becomes an ultrametric space for the distance induced by $|.|$.

If $|.|$ is a nonarchimedean absolute value on K, then for any $q > 1$, putting

$$\nu(x) = -\log_q |x| \text{ for } x \in K^\times, \text{ and } \nu(0) = +\infty$$

one gets a map $\nu : K \to \mathbf{R} \cup \{+\infty\}$ such that :

$$\forall (x,y) \in K^2,\ \nu(xy) = \nu(x) + \nu(y)$$

$\forall (x,y) \in K^2,\ \nu(x+y) \geqslant \min(\nu(x), \nu(y))$

$\forall x \in K,\ \nu(x) = +\infty \iff x = 0$

A function on K satisfying these properties is called a nonarchimedean *valuation* on K. It follows from the axioms that $\nu(1) = 0$, and it is easy to prove that $\nu(-1) = 1$ too. In characteristic 2, $1 = -1$, so there is nothing to prove, and otherwise, it suffices to write $\nu(1) = \nu((-1) \times (-1)) = 2\nu(-1)$ to get the conclusion. From this, one can easily deduce that for all $y \in K$, $\nu(-y) = \nu(y)$. Note the following important fact :

$$\text{if } \nu(x) \neq \nu(y) \text{ then } \nu(x+y) = \min(\nu(x), \nu(y))$$

Indeed, assume for instance that $\nu(x) < \nu(y)$, then :

$$\nu(x) = \nu(x+y-y) \geqslant \min(\nu(x+y), \nu(y)) \geqslant \underbrace{\min(\min(\nu(x), \nu(y)), \nu(y))}_{=\min(\nu(x),\nu(y))=\nu(x)}$$

hence $\min(\nu(x+y), \nu(y)) = \nu(x)$ and so $\nu(x+y) = \nu(x) = \min(\nu(x), \nu(y))$

Remark : In the nonarchimedean case, one could also introduce the notions of absolute value and valuation in the other order, because if ν is a nonarchimedean valuation on K, then for any $q > 1$, the function

$$|.| := q^{-\nu(.)}$$

defines a nonarchimedean absolute value on K. Therefore, the datum of one of the two is really equivalent to the datum of the other one.

Example : (Absolute values on $\mathbf{Q}$)

- The usual absolute value $|.|$ on $\mathbf{R}$ defines an archimedean absolute value on $\mathbf{Q}$.
- If $r \in \mathbf{Q}^\times$ and p is a prime number, then there exists a unique $k \in \mathbf{Z}$ such that :

  $$r = p^k \ \frac{a}{b}$$

  with $a, b \in \mathbf{Z} \setminus \{0\}$ and p dividing neither a nor b. This k is called the p-adic valuation of r, and will be denoted by $\nu_p(r)$. If we set $\nu_p(0) = +\infty$, then one can check that ν_p defines a nonarchimedean valuation on $\mathbf{Q}$. Therefore, for any $q > 1$, we can obtain a nonarchimedean absolute value associated with ν_p. We make a choice and decide that $q = p$ defines the p-adic absolute value on $\mathbf{Q}$, namely :

  $$|.|_p := p^{-\nu_p(.)}$$

This example shows that $\mathbf{Q}$ can be equiped with many different absolute values, that induce different metric (or ultrametric) structures. We can wonder whether or not $\mathbf{Q}$ is complete with respect to these absolute values. We already know that for the usual absolute value, it is not the case, and one way to construct the field of real numbers is to say that it is the completion of $\mathbf{Q}$, seen as a metric space with $|.|$. For the other absolute values we have seen in the example, we have the following result.

Proposition 2.2. *Let p be a prime number. Then the completion of $(\mathbf{Q}, |.|_p)$ is the field $\mathbf{Q}_p$.*

Remark : In definition 1.1 we give another definition of $\mathbf{Q}_p$ as the fraction field of $\mathbf{Z}_p$. As for the different constructions of $\mathbf{R}$, each construction has advantages and drawbacks. If we say that $\mathbf{Q}_p$ is the completion of $\mathbf{Q}$ with respect to $|.|_p$, then it is complete by definition, but it is not clearly a field, and we do not know how to compute with the elements of $\mathbf{Q}_p$. On the other hand, if $\mathbf{Q}_p$ is defined as the field of fractions of $\mathbf{Z}_p$ then it is a field by definition, and since the computation with the elements of $\mathbf{Z}_p$ is very explicit, we know how to compute with p-adic integers. But the fact that it is complete is now less straightforward.

Theorem 2.3. *(Ostrowski) Let K be a complete field with respect to an archimedean valuation. Then there exists an isomorphism $\sigma : K \to \mathbf{R}$ or $\mathbf{C}$, and $s \in]0,1]$ such that for all $x \in K$, $|x| = |\sigma(x)|^s$*

Proof. See [Ne], Theorem (4.2) □

This theorem tells us that a complete field with respect ot an archimedean valuation "looks like" the real or the complex numbers. That is why from now on we will only consider nonarchimedean valuations, and refer to them simply as valuations.

Proposition 2.4. *Let (K, ν) be a valued field (ν being non archimedean). Then the subset $\mathcal{O}_K := \{x \in K \mid \nu(x) \geqslant 0\}$ is a subring of K, called the ring of integers. It is a local ring, with unique maximal ideal $\mathfrak{p}_K := \{x \in \mathcal{O}_K \mid \nu(x) > 0\}$ (and group of units $\mathcal{O}_K^\times = \mathcal{O}_K \setminus \mathfrak{p}_K$)*

Proof. Simple verifications. Note that $\mathcal{O}_K$ satisfies that for all x in K, either x or x^{-1} is in $\mathcal{O}_K$. This implies that $K = \mathrm{Frac}(\mathcal{O}_K)$ and that $\mathcal{O}_K$ is integrally closed in K. Indeed, let $x \in K$ be integral over $\mathcal{O}_K$. This means that x satisfies some monic polynomial equation with coefficients in $\mathcal{O}_K$:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

If we assume for a contradiction that $x \notin \mathcal{O}_K$, then $x^{-1} \in \mathcal{O}_K$ and the equation leads to

$$x = -a_{n-1} - a_{n-2}x^{-1} - \cdots - a_0(x^{-1})^{n-1} \in \mathcal{O}_K : \text{ Contradiction.}$$

Thus $\{x \in K \mid x \text{ is integral over } \mathcal{O}_K\} = \mathcal{O}_K$, this is exactly what it means for $\mathcal{O}_K$ to be integrally closed in K. □

Definition 2.5. *With the notations above, we define the residue field of K as the quotient ring $\mathcal{O}_K/\mathfrak{p}_K$. It is often denoted by κ_K, or simply κ when the context is clear.*

Definition 2.6. *A valuation ν is called discrete if there exists $s \in \mathbf{R}_+^*$ such that*

$$\nu(K^\times) = s\mathbf{Z}$$

Any element in K having valuation s is called a *local parameter* or a *uniformizer* or a *prime element*. It is often denoted by π_K or simply π when there is no possible doubt. If $s = 1$, ν is said to be normalized. Note that it is easy to get a normalized valuation from a discrete valuation, and that this does not change $\mathcal{O}_K, \mathfrak{p}_K$ and the residue field.

Suppose that ν is normalized, so that $\nu(K^\times) = \mathbf{Z}$. Let π be a uniformizer (i.e. an element of valuation 1). Take any element $x \in K^\times$ and let m be $\nu(x)$. Then

$$\nu(\pi^{-m}x) = -m\nu(\pi) + \nu(x) = -m + m = 0$$

hence $\pi^{-m}x \in \mathcal{O}_K^\times$. Therefore, any element $x \in K^\times$ can be written uniquely as a product of a power of the fixed uniformizer and a unit :

$$\forall x \in K^\times,\ \exists!(m,u) \in \mathbf{Z} \times \mathcal{O}_K^\times,\ x = \pi^m u$$

Proposition 2.7. *If ν is a discrete valuation on K, then $\mathcal{O}_K$ is a discrete valuation ring, that is : a principal ideal domain that has a unique non-zero prime ideal.*

Proof. More precisely, we are going to prove that the non-zero ideals of $\mathcal{O}_K$ are the powers of $\mathfrak{p}_K$. Let π be a local parameter in $\mathcal{O}_K$. Let $I \subset \mathcal{O}_K$ be a non-zero ideal in $\mathcal{O}_K$. Take an element $x \in I$ with minimal valuation, say n. If $n = 0$, then I contains a unit, hence $I = \mathcal{O}_K = \mathfrak{p}_K^0$. Otherwise, $n \geqslant 1$, and there exists $u \in \mathcal{O}_K^\times$ such that $x = \pi^n u$. Thus, $\pi^n \mathcal{O}_K \subset I$. Conversely, if $y \in I$, then $m := \nu(y) \geqslant n$, so there exists $v \in \mathcal{O}_K^\times$ such that

$$y = \pi^m v = \pi^n(\pi^{m-n}v) \in \pi^n \mathcal{O}_K$$

So $I = \pi^n \mathcal{O}_K = \mathfrak{p}_K^n = \{x \in \mathcal{O}_K \mid \nu(x) \geqslant n\}$. Therefore, the non-zero ideals of $\mathcal{O}_K$ are the (π^n), for $n \geqslant 0$. □

Remark : The homomorphism $\begin{array}{ccc} \mathfrak{p}_K^n & \to & \mathcal{O}_K/\mathfrak{p}_K \\ \pi^n a & \mapsto & a \bmod \mathfrak{p}_K \end{array}$ induces an isomorphism

$$\mathfrak{p}_K^n/\mathfrak{p}_K^{n+1} \simeq \mathcal{O}_K/\mathfrak{p}_K = \kappa$$

for all $n \geqslant 0$.

Definition 2.8. *A local field is a complete field K with respect to a discrete valuation ν, such that its residue field κ is a finite field.*

Example : If p is a prime number, then $\mathbf{Q}_p$ is a local field, with ring of integers $\mathbf{Z}_p$, and residue field $\mathbf{Z}_p/p\mathbf{Z}_p \simeq \mathbf{Z}/p\mathbf{Z}$.

2.2 Hensel's lemmas

When our valued field is complete with respect to a discrete valuation, we have a very strong result that allows us to lift roots of a polynomial in $\mathcal{O}_K[X]$ from roots modulo $\mathfrak{p}_K$. As we will see in the proof, this result is to be related with Newton's method to approximate zeros of a function. This is very nice, because when the residue field is finite, it is easy to find roots of a polynomial modulo $\mathfrak{p}_K$, because there are only finitely many candidates. Besides the undeniable usefulness of finding roots of polynomials, Hensel's lemma will also allow us to extend valuations uniquely to some field extensions, ans that is a very important result of the next section. First, we state the two following lemmas :

Lemma 2.9. *Let A be a commutative ring, and $f \in A[X]$. Let $a \in A$. Then there exists a unique $g \in A[X]$ such that*

$$f(X) = f(a) + f'(a)(X-a) + g(X)(X-a)^2$$

Lemma 2.10. *Let K be a field, together with a non archimedean absolute value $|.|$. A sequence $(a_n)_{n\in\mathbf{N}}$ is Cauchy if and only if $|a_{n+1} - a_n| \underset{n\infty}{\longrightarrow} 0$*

Corollary 2.11. *If $(K, |.|)$ is complete, with $|.|$ non archimedean, then a power series $\sum_{n\geqslant 0} a_n$ with coefficients in K converges if and only if $a_n \underset{n\infty}{\longrightarrow} 0$*

Theorem 2.12. *(Hensel's lemma I)*
Let (K, ν) be complete with respect to a discrete valuation. Let $q > 1$ and $|.| = q^{-\nu(.)}$. Consider $f \in \mathcal{O}_K[X]$ and $a_0 \in \mathcal{O}_K$ such that :

$$|f(a_0)| < |f'(a_0)|^2$$

For $n \geqslant 0$ we define :

$$a_{n+1} := a_n - \frac{f(a_n)}{f'(a_n)}$$

Then $(a_n)_{n\in\mathbf{N}}$ is well defined, and converges to the unique root a of f such that :

$$|a - a_0| \leqslant \varepsilon |f'(a_0)| \quad (< |f'(a_0)|\ ) \text{ where } \varepsilon \text{ is defined below}$$

Proof. (Largely inspired by [Su] and a document on this lemma in the section *Expository papers* of [Co]) Let

$$\varepsilon := \frac{|f(a_0)|}{|f'(a_0)|^2}$$

We prove by induction on n that :

(i) $|a_n| \leqslant 1$ (i.e. $a_n \in \mathcal{O}_K$)

(ii) $|a_n - a_0| \leqslant \varepsilon < 1$ ($\implies a_n \equiv a_0 \bmod \mathfrak{p}_K$)

(iii) $|f'(a_n)| = |f'(a_0)| \neq 0$ ($\implies a_{n+1}$ is well defined)

(iv) $|f(a_n)| \leqslant \varepsilon^{2^n} |f'(a_0)|^2$

For $n = 0$, all the point are clearly satisfied. Now take $n \geqslant 0$ and assume that a_n satisfies the points (i) to (iv). Let us prove that this is still the case for a_{n+1}.

(i)

$$|a_{n+1} - a_n| = \frac{|f(a_n)|}{|f'(a_n)|} \leqslant \frac{\varepsilon^{2^n}|f'(a_0)|^2}{|f'(a_0)|} = \varepsilon^{2^n}|f'(a_0)| \leqslant \varepsilon^{2^n}$$

because $|f'(a_0)| \leqslant 1$ for $f'(a_0)$ is an integer ($a_0 \in \mathcal{O}_K$ and $f \in \mathcal{O}_K[X]$). Thus :

$$|a_{n+1}| \leqslant \max(|a_{n+1} - a_n|, |a_n|) \leqslant 1$$

(ii)

$$|a_{n+1} - a_0| \leqslant \max(|a_{n+1} - a_n|, |a_n - a_0|) \leqslant \max(\varepsilon^{2^n}, \varepsilon) = \varepsilon$$

(iii) Let us consider the Taylor expansion of f' at a_n :

$$f'(a_{n+1}) = f'\left(a_n - \frac{f(a_n)}{f'(a_n)}\right) = f'(a_n) - \frac{f(a_n)}{f'(a_n)} f''(a_n) + \alpha \left(\frac{f(a_n)}{f'(a_n)}\right)^2 \tag{1}$$

for some $\alpha \in \mathcal{O}_K$ thanks to lemma 2.9. Now,

$$\left|\frac{f(a_n)}{f'(a_n)}\right| \leqslant \varepsilon^{2^n}|f'(a_0)| < |f'(a_0)| = |f'(a_n)|$$

So the term $f'(a_n)$ has strictly minimal valuation among the terms of the right hand side of (1). Therefore, $|f'(a_{n+1})| = |f'(a_n)|$

(iv) Applying lemma 2.9 to f this time, one has :

$$\begin{aligned} f(a_{n+1}) &= f(a_n) - \frac{f(a_n)}{f'(a_n)} f'(a_n) + \beta \left(\frac{f(a_n)}{f'(a_n)} \right)^2 \\ &= \beta \left(\frac{f(a_n)}{f'(a_n)} \right)^2 \quad \text{, for some } \beta \in \mathcal{O}_K. \end{aligned}$$

Since $\beta \in \mathcal{O}_K$, $|\beta| \leqslant 1$, hence

$$|f(a_{n+1})| \leqslant \left| \frac{f(a_n)}{f'(a_n)} \right|^2 = \frac{|f(a_n)|^2}{|f'(a_0)|^2} \leqslant \frac{(\varepsilon^{2^n} |f'(a_0)|^2)^2}{|f'(a_0)|^2} \leqslant \varepsilon^{2^{n+1}} |f'(a_0)|^2$$

This concludes the induction step. We have proved that $|a_{n+1} - a_n| \leqslant \varepsilon^{2^n}$, and $\varepsilon < 1$ by assumption, hence $|a_{n+1} - a_n| \underset{n\infty}{\longrightarrow} 0$. By lemma 2.10, $(a_n)_{n \in \mathbf{N}}$ is Cauchy, so it converges to an element $a \in \mathcal{O}_K$, because $\mathcal{O}_K$ is complete as a closed subset of the complete field K. Besides, $|a - a_0| = \lim_{n\infty} |a_n - a_0| \leqslant \varepsilon < 1$, so $a \equiv a_0 \mod \mathfrak{p}_K$ (i.e. a is a lift of our first root modulo $\mathfrak{p}_K$). Moreover,

$$\begin{cases} |f(a_n)| \leqslant \varepsilon^{2^n} |f'(a_0)|^2 \underset{n\infty}{\longrightarrow} 0 \\ f(a_n) \underset{n\infty}{\longrightarrow} f(a) \text{ because polynomials are continuous} \end{cases}$$

This implies that a is a root of f in $\mathcal{O}_K$.

We now need to show that a is the unique root of f such that $|a - a_0| \leqslant \varepsilon |f'(a_0)|$. For all $n \geqslant 1$,

$$|a_{n+1} - a_n| \leqslant \varepsilon^{2^n} |f'(a_0)| < \varepsilon |f'(a_0)| = \frac{|f(a_0)|}{|f'(a_0)|}$$

Moreover $|a_1 - a_0| = |f(a_0)|/|f'(a_0)|$ by definition. Therefore,

$$\forall n \in \mathbf{N}, \ |a_n - a_0| \leqslant \frac{|f(a_0)|}{|f'(a_0)|} = \varepsilon |f'(a_0)|$$

(using the ultrametric triangle inequality). When $n \longrightarrow \infty$ we get $|a - a_0| \leqslant \varepsilon |f'(a_0)|$. Thus, a is a root of f, that reduces to a_0 modulo $\mathfrak{p}_K$, and such that $|a - a_0| \leqslant \varepsilon |f'(a_0)|$.

Now if b is another root satisfying these two properties, then : we write $b = a + (b - a)$ and we apply lemma 2.9 once again :

$$f(b) = f(a) + (b - a) f'(a) + c(b - a)^2, \text{ for some } c \in \mathcal{O}_K$$

But a and b are both roots of f, so this lead to $(b - a) f'(a) + c(b - a)^2 = 0$. Assuming $a \neq b$ one has $f'(a) = c(a - b)$. Thus $|f'(a)| \leqslant |a - b|$ because $c \in \mathcal{O}_K$. Now the strong triangle inequality gives :

$$|a - b| \leqslant |a - a_0 + a_0 - b| \leqslant \max(|a - a_0|, |b - a_0|) < |f'(a_0)|$$

However, we know that $|f'(a)| = |f'(a_0)|$ (by passing to the limit in (iii)). Thus :

$$|f'(a_0)| = |f'(a)| \leqslant |a - b| < |f'(a_0)| \ : \text{Contradiction.}$$

□

Corollary 2.13. *In particular, if a_0 is a simple root of f modulo $\mathfrak{p}_K$, then it lifts uniquely to a root of f in $\mathcal{O}_K$, i.e. there exists a unique $a \in \mathcal{O}_K$ such that $a \equiv a_0$ mod $\mathfrak{p}_K$ and $f(a) = 0$.*

Proof. Let $a_0 \in \mathcal{O}_K$ such that $\begin{cases} f(a_0) \equiv 0 \bmod \mathfrak{p}_K \\ f'(a_0) \not\equiv 0 \bmod \mathfrak{p}_K \end{cases}$

Then $\nu(f(a_0)) \geqslant 1$ (ν being normalized) and $\nu(f'(a_0)) = 0$. Equivalently,

$$|f(a_0)| < 1 \quad \text{and} \quad |f'(a_0)| = 1$$

Therefore, a_0 satisfies the conditions of the theorem above, so there exists a unique $a \in \mathcal{O}_K$ such that

$$\begin{cases} f(a) = 0 \\ |a - a_0| < 1 \text{ (i.e. } a \equiv a_0 \bmod \mathfrak{p}_K) \end{cases}$$

□

The two preceding results are very useful in the study of the squares in $\mathbf{Z}_p$ and of the structure of $\mathbf{Z}_p^\times$ (the group of units).

Proposition 2.14. *Let $p \neq 2$ be a prime, and let $b \in \mathbf{Z}_p^\times = \mathbf{Z}_p \setminus p\mathbf{Z}_p$. Then b is a square in $\mathbf{Z}_p$ if and only if b is a square modulo $p\mathbf{Z}_p$.*

Proof. The direct implication is easy, and for the converse, it suffices to apply corollary 2.13 to $f = X^2 - b \in \mathbf{Z}_p[X]$. □

However, if $p = 2$, then the polynomial f above is no longer separable, so we can't apply the corollary and we need to use theorem 2.12. Namely, we have the following :

Proposition 2.15. *Let $b \in \mathbf{Z}_2^\times = \mathbf{Z}_2 \setminus 2\mathbf{Z}_2$. b is a square in $\mathbf{Z}_2$ if and only if $b \equiv 1(8\mathbf{Z}_2)$.*

Proof. If b is a square in $\mathbf{Z}_2$, then let $a \in \mathbf{Z}_2$ be such that $b = a^2$. Write $b = (b_n)_{n \in N^*}$ and $a = (a_n)_{n \in \mathbf{N}^*}$ (considering $\mathbf{Z}_2$ as the projective limit of the rings $(\mathbf{Z}/2^n\mathbf{Z})$. Then

$$b_3 = a_3^2 \in \mathbf{Z}/8\mathbf{Z}$$

Since $b \notin 2\mathbf{Z}_2$, $a_3 \notin 2.(\mathbf{Z}/8\mathbf{Z})$, hence $b_3 = (1 \bmod 8)$ by a quick study of what values can a square have modulo 8. Since $b \in \mathbf{Z}_2$, this implies that $b_1 = (1 \bmod 2)$ and $b_2 = (1 \bmod 4)$. Thus $b \equiv 1(8\mathbf{Z}_2)$.

Conversely, suppose that $b \equiv 1(8\mathbf{Z}_2)$. Let us consider $f = X^2 - b \in \mathbf{Z}_2[X]$. Then our assumption implies that $|f(1)|_2 \leqslant 1/8$. On the other hand $f'(1) = 2$ so that $|f'(1)|_2^2 = 1/4$. Thus :

$$|f(1)|_2 < |f'(1)|_2^2$$

and we can apply Hensel's lemma to find a square root of b in $\mathbf{Z}_2$. □

Proposition 2.16. *Let $p \neq 2$ be a prime. The group of p-adic units has the following structure :*

$$\mathbf{Z}_p^\times \simeq \underbrace{\mathbf{F}_p^\times \times (1 + p\mathbf{Z}_p)}_{\text{as multiplicative groups}} \simeq \underbrace{\mathbf{Z}/(p-1)\mathbf{Z} \times \mathbf{Z}_p}_{\text{as additive groups}}$$

Proof. Considering the natural inclusion $i : 1 + p\mathbf{Z}_p \to \mathbf{Z}_p^\times$ and

$$\begin{array}{rccc} \rho & : & \mathbf{Z}_p^\times & \to & \mathbf{F}_p^\times \\ & & (a_n)_{n\geqslant 1} & \mapsto & a_1 \end{array}$$

we get an exact sequence of abelian groups :

$$1 \to 1 + p\mathbf{Z}_p \overset{i}{\hookrightarrow} \mathbf{Z}_p^\times \overset{\rho}{\twoheadrightarrow} \mathbf{F}_p^\times \to 1$$

By the splitting lemma in homological algebra, it suffices to prove that there exists a group homomorphism $\sigma : \mathbf{F}_p^\times \to \mathbf{Z}_p^\times$ such that $\rho \circ \sigma = id$ to conclude that $\mathbf{Z}_p^\times$ is isomorphic to the direct product of the terms on its right and left sides. Consider $f = X^{p-1} - 1$: it has $p-1$ distinct simple roots in $\mathbf{F}_p$, which are exactly the elements of $\mathbf{F}_p^\times$: $\bar{1}, \dots, \overline{p-1}$. By corollary 2.13, each of them lifts uniquely to an element $\alpha_i = (\bar{i}, a_2, a_3, \dots) \in \mathbf{Z}_p^\times$. Then $\sigma : \bar{i} \to \alpha_i$ is a group homomorphism satisfying $\rho \circ \sigma = id$.

Now, $\mathbf{F}_p^\times$ is a cyclic group of order $(p-1)$, hence isomorphic to the additive group $\mathbf{Z}/(p-1)\mathbf{Z}$. To prove that $(1 + p\mathbf{Z}_p, .) \simeq (\mathbf{Z}_p, +)$, one can consider the logarithm :

$$\begin{array}{rccc} \ln & : & 1 + p\mathbf{Z}_p & \to & p\mathbf{Z}_p \\ & & 1 + x & \mapsto & \sum_{n=1}^{+\infty} (-1)^{n-1} \frac{x^n}{n} \end{array}$$

The series considered converge because their general term tends to zero as $n \longrightarrow +\infty$. It remains to check that ln is a group isomorphism between $(1 + p\mathbf{Z}_p, .)$ and $(p\mathbf{Z}_p, +)$ and that the latter is isomorphic to $(\mathbf{Z}_p, +)$ □

Proposition 2.17.

$$\mathbf{Z}_2^\times \simeq \{\pm 1\} \times (1 + 4\mathbf{Z}_2)$$

Proof. First, $\mathbf{Z}_2^\times = \mathbf{Z}_2 \setminus 2\mathbf{Z}_2$, so an element in $\mathbf{Z}_2^\times$ is just a sequence $(a_n)_{n\geqslant 1}$ such that :

$$\begin{cases} \forall n \geqslant 1,\ a_n \in \mathbf{Z}/2^n\mathbf{Z} \\ a_1 = 1 \in \mathbf{Z}/2\mathbf{Z} \end{cases}$$

Thus, $\mathbf{Z}_2^\times = 1 + 2\mathbf{Z}_2$. Now consider :

$$1 \longrightarrow 1 + 4\mathbf{Z}_2 \overset{i}{\hookrightarrow} 1 + 2\mathbf{Z}_2 \overset{\rho}{\longrightarrow} (\mathbf{Z}/4\mathbf{Z})^\times \longrightarrow 1 \tag{2}$$

where i is the natural inclusion, and :

$$\begin{array}{rccc} \rho & : & 1 + 2\mathbf{Z}_2 & \longrightarrow & (\mathbf{Z}/4\mathbf{Z})^\times = \{\pm 1\} \\ & & (1 \bmod 2, 1 + 2b \bmod 4, \dots) & \mapsto & 1 + 2b \bmod 4 \end{array}$$

The sequence (2) is exact, so to obtain the conclusion, we just need to find a group homomorphism $s : (\mathbf{Z}/4\mathbf{Z})^\times \longrightarrow 1 + 2\mathbf{Z}_2$ such that $\rho \circ s = id$. It suffices to take $s : \overline{-1} \mapsto -1 \in \mathbf{Z} \subset 1 + 2\mathbf{Z}_2$, hence the conclusion. □

Hensel's lemma is sometimes stated in an other version, which says that from a factorization af a polynomial modulo $\mathfrak{p}_K$, we can lift a factorization in $\mathcal{O}_K[X]$. The idea is the same, starting from our factorization in $\frac{\mathcal{O}_K}{\mathfrak{p}_K}[X]$, we try to find a factorization modulo $\mathfrak{p}_K^2$ by adjoining only terms that are zero modulo $\mathfrak{p}_K$, and so on, by induction. The precise statement is the following :

Theorem 2.18. *(Hensel's lemma II)*
Let (K, ν) be as in theorem 2.12, with residue field denoted by κ. Let $f \in \mathcal{O}_K[X]$ be a primitive polynomial (this means that at least one of its coefficients lies in $\mathcal{O}_K^\times$). If f admits a factorization modulo $\mathfrak{p}_K$ into two relatively prime polynomials :

$$f \ mod \ \mathfrak{p}_K = \bar{g}.\bar{h} \in \kappa[X], \quad \bar{g} \wedge \bar{h} = 1$$

Then f admits a factorization in $\mathcal{O}_K[X]$:

$$f = g.h$$

with $deg(g) = deg(\bar{g})$, $(g \ mod \ \mathfrak{p}_K) = \bar{g}$, and $(h \ mod \ \mathfrak{p}_K) = \bar{h}$.

Proof. See [Ne], (4.6) "Hensel's Lemma"

We can observe that the condition "f primitive" is just there to ensure that $f \bmod \mathfrak{p}_K$ is not zero in $\kappa[X]$. The proof is similar to the proof of the other version of Hensel's lemma : We construct factorization modulo $\mathfrak{p}_K^n$ inductively, but there are some subtleties, because the degree of the polynomials must stay bouded, so that we do not end up with a factorization into power series instead of polynomials. An euclidean division solves the problem. □

Corollary 2.19. *For every irreducible polynomial $f = \sum_{i=0}^{d} a_i X^i \in K[X]$, one has :*

$$\max_{i=0\ldots d} |a_i| = \max\left(|a_0|, |a_d|\right)$$

In particular, if f is monic, irreducible, and $a_0 \in \mathcal{O}_K$, then $f \in \mathcal{O}_K[X]$

Proof. Let us set $|f| := \max_{i=0\ldots d} |a_i|$

After multiplying by an appropriate power of a uniformizer, we may assume that $f \in \mathcal{O}_K[X]$ and that $|f| = 1$. Our aim is to prove that $m := \max(|a_0|, |a_d|) = 1$. Of course $m \leqslant 1$. Assume that $m < 1$.

Let r be $\min\{i \in [\![0, d]\!]; |a_i| = 1\}$. Then $0 < r < d$ because $m < 1$ and :

$$f = X^r(a_r + a_{r+1}X + \cdots + a_d X^{d-r}) \bmod \mathfrak{p}_K$$

By theorem 2.18, this factorization lifts to a factorization of f in $\mathcal{O}_K[X] \subset K[X]$. This contradicts the irreducibility of f. Thus, $m = 1$ and this concludes the proof. □

2.3 Extension of valuations

The aim of this section is to prove theorem 2.21. We start with a short recall on norms in field theory. Let L/K be a finite field extension of degree n (in particular, L is a n-dimensional vector space over K). Then for any $\alpha \in L$ the map :

$$\begin{array}{rccc} \mu(\alpha) & : & L & \to & L \\ & & x & \mapsto & \alpha x \end{array}$$

is K linear. Thus, it is an endomorphism of a n dimensional vector space over K, so it makes sense to consider its determinant.

Definition 2.20. *The norm of the element $\alpha \in L$ over K is the determinant of the multiplication by α, namely :*

$$Nm_{L/K}(\alpha) := det(\mu(\alpha)) \quad (\in K)$$

It follows immediately that $Nm_{L/K}(.)$ is multiplicative.

Theorem 2.21. *If (K,ν) is complete with respect to a discrete valuation and L/K is a finite field extension, then ν extends uniquely to L. Moreover, the unique valuation ν_L extending ν can be written explicitly :*

$$\forall \alpha \in L,\ \nu_L(\alpha) = \frac{1}{[L:K]}\nu(Nm_{L/K}(\alpha))$$

To prove this theorem, we will need a few lemmas. Recall that if $A \subset B$ are two rings, an element $b \in B$ is said to be integral over A if there exists a monic polynomial $P \in A[X]$ such that $P(b) = 0$.

Lemma 2.22. *Let A be an integral domain, integrally closed in $K := Frac(A)$. Let L/K be a finite extension. Then, for all $\alpha \in L$, α is integral over A if and only if the minimal polynomial of α over K has its coefficients in A.*

Proof. Let $x \in L$. Let f be the minimal polynomial of x over K. If $f \in A[X]$, then x is a root of a monic polynomial with coefficients in A, so by definition, x is integral over A.

Conversely, assume that x is integral over A. Let $P \in A[X]$ be a monic polynomial such that $P(x) = 0$. Then f divides P, so every root of f is a root of P, hence is integral over A. Moreover we know that sums and products of integral elements are still integral. More precisely, given an algebraic closure $\bar{K}$ of K containing L, the following set

$$\{z \in \bar{K} \mid z \text{ is integral over } A\}$$

is a subring of $\bar{K}$. This is not obvious, but it is very standard, see for instance Milne's lecture notes in algebraic number theory ([Mi]), where he gives two proofs of this statement. Now, we also know that the coefficients of f are just sums and products of the roots, so they are all integral over A, and they lie in K (recall that f is the minimal polynomial of x over K). Since A is assumed to be integrally closed in K, $f \in A[X]$. □

Lemma 2.23. *If L/K is a finite extension, $\alpha \in L$, and a_0 is the constant term of the minimal polynomial of α over K, then*

$$Nm_{L/K}(\alpha) = \pm a_0^m,\ \textit{for some } m \in \mathbf{N}^*$$

Proof. In fact, the statement can be made way more precise, but we actually just need to know this. A proof can be found in [Go] Chapter IX. □

Lemma 2.24. *Let L be a field, and $|.|_1, |.|_2$ two absolute values on L. Assume that $\forall x \in L,\ |x|_1 \leqslant 1 \implies |x|_2 \leqslant 1$. Then there exists $s > 0$ such that $|.|_1 = |.|_2^s$*

Proof. Let $y \in L$ such that $|y|_1 > 1$. Take any $x \in L^\times$. Then $|x|_1 > 0$, so $\ln(|x|_1)$ is well-defined. Set $\alpha := \ln(|x|_1)/\ln(|y|_1)$, so that $|x|_1 = |y|_1^\alpha$. Let $(m_i/n_i)_{i\in\mathbf{N}}$ be a decreasing sequence of rational numbers converging to α. Then :

$$|x|_1 = |y|_1^\alpha \leqslant |y|_1^{\frac{m_i}{n_i}} \implies \frac{|x|_1}{|y|_1^{m_i/n_i}} \leqslant 1$$

this leads to :

$$\left|\frac{x^{n_i}}{y^{m_i}}\right|_1 \leqslant 1 \underset{\text{by assumption}}{\implies} \left|\frac{x^{n_i}}{y^{m_i}}\right|_2 \leqslant 1$$

Hence :

$$|x|_2 \leqslant |y|_2^{m_i/n_i} \underset{n\infty}{\longrightarrow} |y|_2^\alpha$$

Taking an increasing sequence of rational numbers converging to α would lead to $|y|_2^\alpha \leqslant |x|_2$, so $|x|_2 = |y|_2^\alpha$. Therefore, for all $x \in L^\times$,

$$\frac{\ln(|x|_1)}{\ln(|x|_2)} = \frac{\ln(|y|_1^\alpha)}{\ln(|y|_2^\alpha)} := s > 0 \quad \text{(independent of } x\text{)}$$

Therefore, $|.|_1 = |.|_2^s$. □

Remark : In particular, two such absolute values give rise to the same topology on L.

We can now start the proof of theorem 2.21.

Proof. *Step 1 :* *Let us set* $\mathcal{O} := \{x \in L \mid Nm_{L/K}(x) \in \mathcal{O}_K\}$. *We prove that* $\mathcal{O}$ *is exactly the integral closure of* $\mathcal{O}_K$ *in* L.

If $x \in L$ is integral over $\mathcal{O}_K$, then the minimal polynomial f of x over K has coefficients in $\mathcal{O}_K$. In particular its constant term lies in $\mathcal{O}_K$, so by lemma 2.23, $Nm_{L/K}(x) \in \mathcal{O}_K$.

Conversely, suppose x is an element of L such that $Nm_{L/K}(x) \in \mathcal{O}_K$. Let f be its minimal polynomial over K, say :

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

Again, by lemma 2.23, $Nm_{L/K}(x) = \pm a_0^m$ for some $m \in \mathbf{N}^*$. Therefore $m\nu(a_0) = \nu(Nm_{L/K}(x)) \geqslant 0$ by assumption, so $a_0 \in \mathcal{O}_K$. To sum it up : f is a monic irreducible polynomial in $K[X]$ with $a_0 \in \mathcal{O}_K$, hence (by corollary 2.19) $f \in \mathcal{O}_K[X]$. This implies that x is integral over $\mathcal{O}_K$

Step 2 : ν_L *is a valuation on* L *that extends* ν.

All the points are clear except the ultrametric inequality, namely :

$$\forall (x,y) \in L^2,\ \nu_L(x+y) \geqslant \min(\nu_L(x), \nu_L(y)) \tag{3}$$

First, since $\mathcal{O}$ is the integral closure of $\mathcal{O}_K$ in L, it is a ring, so that :

$$\forall x \in L,\ x \in \mathcal{O} \implies 1 + x \in \mathcal{O}$$

Now, let $x, y \in L$. If x or y is zero, then (3) is clearly satisfied, so we can assume that none of them is zero. Then $\nu_L(x+y) = \nu_L(x(1+x^{-1}y)) = \nu_L(x) + \nu_L(1+x^{-1}y)$

- *If* $x^{-1}y \in \mathcal{O}$: Then $1 + x^{-1}y \in \mathcal{O}$, so $\nu_L(1+x^{-1}y) \geqslant 0$, hence

$$\nu_L(x+y) \geqslant \nu_L(x) \geqslant \min(\nu_L(x), \nu_L(y))$$

- *If* $x^{-1}y \notin \mathcal{O}$: Then we write $\nu_L(x+y) = \nu_L(y(y^{-1}x+1)) = \nu_L(y) + \nu_L(y^{-1}x+1)$ Since $x^{-1}y \notin \mathcal{O}$, it is not hard to see that its inverse $y^{-1}x \in \mathcal{O}$. Indeed,

$$\forall \alpha \in L,\ Nm_{L/K}(\alpha) \notin \mathcal{O}_K \implies \underbrace{Nm_{L/K}(\alpha)^{-1}}_{=Nm_{L/K}(\alpha^{-1})} \in \mathcal{O}_K$$

  Thus, $\nu_L(y^{-1}x+1) \geqslant 0$, hence :

$$\nu_L(x+y) \geqslant \nu_L(y) \geqslant \min(\nu_L(x), \nu_L(y))$$

  So ν_L is a valutation on L that extends ν, and moreover, the ring of integers in L with respect to this valuation, namely $\mathcal{O}_L = \{x \in L \mid \nu_L(x) \geqslant 0\}$, is nothing else than $\mathcal{O}$, the integral closure of $\mathcal{O}_K$ in L.

Step 3 : *Uniqueness.*

Let ν' be a valuation on L extending ν. We denote by $\mathcal{O}'$ the ring of integers in L for this valuation, namely : $\mathcal{O}' = \{x \in L \mid \nu'(x) \geqslant 0\}$, and by $\mathfrak{p}'$ the unique maximal ideal in $\mathcal{O}'$: $\mathfrak{p}' = \{x \in L \mid \nu'(x) > 0\}$. The corresponding sets in (L, ν_L) are denoted by $\mathcal{O}_L, \mathfrak{p}_L$.

Let us prove that $\mathcal{O}_L \subset \mathcal{O}'$. Assume for a contradiction that there exists $x \in L$ such that $x \in \mathcal{O}_L$ but $x \notin \mathcal{O}'$. Since $x \in \mathcal{O}_L$, which is the integral closure of $\mathcal{O}_K$ in L (as we have seen in *Step 1*), there are integers $a_0, \dots a_{n-1} \in \mathcal{O}_K$ such that :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

Dividing by x^n gives the following :

$$1 = -a_{n-1}x^{-1} - \cdots - a_0 x^{-n}$$

However, since $x \notin \mathcal{O}'$, $\nu'(x) < 0$ and ν' extends ν, so :

$$\forall i \in \{0, \dots, n-1\},\ \nu'(a_i x^{i-n}) = \underbrace{\nu(a_i)}_{\geqslant 0} + \underbrace{(i-n)\nu'(x)}_{>0}$$

Thus, $\nu'(1) \geqslant \min_i \nu'(a_i x^{i-n}) > 0$, so $1 \in \mathfrak{p}'$: Contradiction.

Therefore, $\mathcal{O}_L \subset \mathcal{O}'$, which we can rewrite as $\forall x \in L,\ \nu_L(x) \geqslant 0 \implies \nu'(x) \geqslant 0$. Setting

$$|.|_L := \exp(-\nu_L(.)) \quad \text{and} \quad |.|' := \exp(-\nu'(.))$$

we get two absolute values on L satisfying the assumption of lemma 2.24, so there exists $s > 0$ such that $|.|_L = |.|'^s$. But these two must agree on K, hence $s = 1$ (it suffices to take an element in K with absolute value different from 1). Thus, $|.|_L = |.|'$ and $\nu_L = \nu'$. □

Moreover, this unique extension of valuation gives a valued field (L, ν_L) which is still complete ! Indeed, let us set $|.| = \exp(-\nu(.))$. Then, $|.|_L := \exp(-\nu_L(.))$ is a norm on L seen as a K-vector space. Indeed, it satisfies the triangle inequality and the separability condition. Moreover, if $\lambda \in K$ and $x \in L$, then

$$|\lambda x|_L = \exp(-\nu_L(\lambda x)) = \exp(-\nu(\lambda))\exp(-\nu_L(x)) = |\lambda||x|_L$$

Since L is a finite dimensional vector space over K, and $(K, |.|)$ is complete, the fact that $(L, |.|_L)$ is complete follows from this general result :

Proposition 2.25. *Let K be complete with respect to an absolute value $|.|$. Let V be any n-dimensional normed vector space over K. Then for any basis $(e_1, \dots, e_n)$ of V, the maximum norm :*

$$\left\| \sum_{i=1}^{n} x_i e_i \right\|_\infty = \max(|x_1|, \dots, |x_n|)$$

is equivalent to the given norm on V. In particular V is complete.

Remark: This theorem is just a more general version of the equivalence of all norms over a finite dimensional ($\mathbf{R}$ or $\mathbf{C}$) vector space. We see that the key ingredient is that the ground field K has to be complete for its absolute value.

Proof. Let $\|.\|$ be a norm on V. We want to prove that there exist $\rho, \rho' > 0$ such that :

$$\forall x \in V,\ \rho\|x\|_\infty \leqslant \|x\| \leqslant \rho'\|x\|_\infty$$

- Let $x \in V$ and write $x = \sum x_i e_i$. Then :

$$\|x\| = \left\|\sum_{i=1}^n x_i e_i\right\| \leqslant \sum_{i=1}^n |x_i|\|e_i\| \leqslant \underbrace{\left(\sum_{i=1}^n \|e_i\|\right)}_{:=\rho'} \|x\|_\infty$$

- In order to prove the existence of a ρ, we proceed by induction on the dimension of V.

  If $n = \dim(V) = 1$, then for all $x \in V$, $\|x\| = \|x_1 e_1\| = |x_1|\|e_1\| = \|e_1\|\|x\|_\infty$, so one can take ρ to be $\|e_1\|$.

  Now, let $n \geqslant 1$, and assume that the result holds for any $(n-1)$ dimensional normed vector space over K. Set $V_i = \mathrm{Span}(e_j, j \neq i)$, for all $i \in \{1, \dots, n\}$. Then by the induction assumption, V_i is complete with respect to the restricted norm $\|.\|$. In particular, it is closed in $(V, \|.\|)$. This implies that for all i, $V_i + \{e_i\}$ is closed, hence

$$\bigcup_{i=1}^n V_i + \{e_i\} \text{ is a closed subset of } V$$

  Moreover, it does not contain 0. Therefore, there exists $\rho > 0$ such that for all $i \in \{1, \dots, n\}$, if $w_i \in V_i$, then $\|w_i + e_i\| \geqslant \rho$.
  Now, let $x = \sum x_i e_i \in V \setminus \{0\}$ and let r be the index such that $|x_r| = \|x\|_\infty$. Then, one has :

$$\left\|\frac{x}{x_r}\right\| = \left\|e_r + \sum_{i \neq r} \frac{x_i}{x_r} e_i\right\| \geqslant \rho$$

  So $\|x\| \geqslant \rho|x_r| = \rho\|x\|_\infty$ This holds for all non zero $x \in V$, and it is also satisfied at zero, hence the result.

□

3 Ramification

3.1 Ramification index, inertia degree and dimension formula

Again, let K be complete with respect to a discrete valuation ν, and let L/K be a finite extension. In the preceding section, we proved that ν extends uniquely to a valuation ν_L on L, and that (L, ν_L) is also complete. Now, our aim is to study the same objects in L that we studied in K, such that the subgroup $\nu_L(L^\times)$ of $(\mathbf{R}, +)$, or the residue field $\kappa_L = \mathcal{O}_L/\mathfrak{p}_L$. We will try to study the different relations that can arise between these objects and κ_K, $\nu(K^\times)$ ...

Since $K^\times$ is a multiplicative subgroup of $L^\times$, one has that $\nu(K^\times) = \nu_L(K^\times)$ is a subgroup of $\nu_L(L^\times)$. We denote by e its index, that is :

$$e := \#\left(\frac{\nu_L(L^\times)}{\nu(K^\times)}\right)$$

e is called the *ramification index* of the extension L/K.

Moreover, we have a natural ring homomorphism $\phi : \mathcal{O}_K \to \mathcal{O}_L/\mathfrak{p}_L = \kappa_L$ obtained by composing the natural inclusion $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ and the surjection $\mathcal{O}_L \twoheadrightarrow \kappa_L$ (reduction modulo $\mathfrak{p}_L$). But $\mathfrak{p}_K \subset \ker\phi$, so ϕ factors to a ring homomorphism :

$$\begin{array}{ccccc} \varphi & : & \kappa & \to & \kappa_L \\ & & x \bmod \mathfrak{p}_K & \mapsto & x \bmod \mathfrak{p}_L \end{array}$$

and φ is injective because κ is a field. Thus, κ_L/κ is a field extension, we denote by f its degree, namely :

$$f := [\kappa_L : \kappa]$$

f is called the *inertia degree* of L/K. When the context is clear, we stick to the notations e and f, but sometimes we will write $e(L/K)$ and $f(L/K)$ in order to specify explicitly to which extension correspond e and f.

Remark : If π_L is a uniformizer in L and π a uniformizer in K, then $\pi \in \mathcal{O}_L$, so it can be written $\pi_L^m.u$ with $u \in \mathcal{O}_L^\times$ and $m \in \mathbf{Z}$, unique. But $\nu_L(\pi) = \nu(\pi) = e.\nu_L(\pi_L)$, hence $e = m$. Therefore $\mathfrak{p}_K\mathcal{O}_L = \pi\mathcal{O}_L = \pi_L^e\mathcal{O}_L = \mathfrak{p}_L^e$. This is a particular case of Hilbert's ramification theory, which consists in studying how a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ factors in $\mathcal{O}_L$ when we look at the ideal it generates in $\mathcal{O}_L$. Here we have :

$$\mathfrak{p}_K\mathcal{O}_L = \mathfrak{p}_L^e$$

and this justifies the name *ramification index* for e. If K were a number field, the decomposition of a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ could be more complicated :

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=0}^{m} \mathfrak{P}_i^{e_i}$$

where the $\mathfrak{P}_i$ are prime ideals in $\mathcal{O}_L$. Then e_i is a relative ramification index (because it is relative to one of the prime ideals in the decomposition).

Proposition 3.1. *If (K, ν) is a complete discrete valued field, and L/K is a finite extension, then with the notations above, one has :*

$$[L : K] = e.f$$

Proof. Since $f = [\kappa_L : \kappa]$, let $w_1, \ldots, w_f \in \mathcal{O}_L$ such that $(\bar{w}_1, \ldots, \bar{w}_f)$ is a basis of κ_L as a κ vector space ($\bar{w}_i = w_i \bmod \mathfrak{p}_L$). Let π_L be a uniformizer in L. Then $\pi_L^0, \ldots, \pi_L^{e-1}$ are representatives of $\nu_L(L^\times)/\nu(K^\times)$

Let us prove that $(\pi_L^i w_j)_{0 \leqslant i \leqslant e-1,\ 1 \leqslant j \leqslant f}$ is an integral basis of $\mathcal{O}_L$ over $\mathcal{O}_K$. This implies that it is a basis of L/K and the dimension formula follows.

- *Linear independance* : Let us assume, for a contradiction, that there exist $a_{i,j} \in K$ not all of them equal to zero, such that :

$$\sum_{i=0}^{e-1} \sum_{j=1}^{f} a_{i,j} w_j \pi_L^i = 0 \tag{4}$$

For all $i \in \{0, \ldots, e-1\}$, let us denote :

$$s_i := \sum_{j=1}^{f} a_{i,j} w_j$$

If $s_i = 0$ and $a_{i,j} \neq 0$ for some j, then multiplying by an appropriate power of π_K, we obtain :

$$\sum_{j=1}^{f} b_{i,j} w_j = 0$$

with $b_{i,j} \in \mathcal{O}_K$ and at least one of them lies in $\mathcal{O}_K^\times$. But if one reduces this equality modulo $\mathfrak{p}_L$, one gets a non-trivial linear combination of the $\bar{w}_j$'s which is equal to zero, hence a contradiction, because $\bar{w}_1, \ldots, \bar{w}_f$ is a basis of κ_L/κ. Thus :

$$s_i = 0 \implies \forall j \in \{1, \ldots, f\},\ a_{i,j} = 0$$

Since some of the $a_{i,j}$'s are assumed to be non-zero, some of the s_i's must be non-zero. Let us denote by I^* the set of all indices i such that $s_i \neq 0$. Then (4) becomes :

$$\sum_{i \in I^*} s_i \pi_L^i = 0$$

Now, let us show that for all $i \in I^*$, $\nu_L(s_i) \in \nu(K^\times)$. As above, one can find $m \in \mathbf{Z}$ such that :

$$s_i = \sum_{j=1}^{f} a_{i,j} w_j = \pi_K^m \sum_{j=1}^{f} b_{i,j} w_j$$

with $b_{i,j} \in \mathcal{O}_K$ and at least one of them in $\mathcal{O}_K^\times$. Thus

$$\nu_L(s_i) = \nu(\pi_K^m) + \nu_L\left(\sum_{j=1}^{f} b_{i,j} w_j\right)$$

However, since some of the $b_{i,j}$'s lie in $\mathcal{O}_K^\times$, they are non-zero modulo $\mathfrak{p}_K$. Using the fact that $\bar{w}_1, \ldots, \bar{w}_f$ are linearly independant over κ, we get that $\sum_j b_{i,j} w_j$ cannot lie in $\mathfrak{p}_L$, and hence is invertible in $\mathcal{O}_L$. Therefore, it has valuation 0 and so

$$\nu_L(s_i) = \nu(\pi_K^m) \in \nu(K^\times)$$

Now if $i \neq j \in I^*$ then $\nu_L(s_i \pi_L^i)$ and $\nu_L(s_j \pi_L^j)$ must be different because $\nu_L(\pi_L^i)$ and $\nu_L(\pi_L^j)$ are different modulo $\nu(K^\times)$. Thus :

$$\nu_L\left(\sum_{i \in I^*} s_i \pi_L^i\right) = \nu_L(0) = \infty = \min_{i \in I^*} \nu_L(s_i \pi_L^i)$$

This implies that for all $i \in I^*, s_i = 0$. Contradiction.

- *$\mathcal{O}_L$ is generated by $(\pi_L^i w_j)$ over $\mathcal{O}_K$* : Let us denote by M the $\mathcal{O}_K$-module

$$M := \sum_{i=0}^{e-1} \sum_{j=1}^{f} \mathcal{O}_K \pi_L^i w_j$$

and by N the following :

$$N := \sum_{j=1}^{f} \mathcal{O}_K w_j$$

so that

$$M = \sum_{i=0}^{e-1} \pi_L^i N$$

It is not hard to prove that $\mathcal{O}_L = N + \pi_L \mathcal{O}_L$, and iterating this

$$\mathcal{O}_L = N + \pi_L(N + \pi_L(N + \pi_L \dots))$$

until we get :

$$\mathcal{O}_L = M + \pi_L^e \mathcal{O}_L \quad \text{i.e.} \quad \mathcal{O}_L = M + \mathfrak{p}_K \mathcal{O}_L$$

Iterating this last formula, one has $\mathcal{O}_L = M + \mathfrak{p}_K(M + \mathfrak{p}_K \mathcal{O}_L) = M + \mathfrak{p}_K M + \mathfrak{p}_K^2 \mathcal{O}_L$ But clearly, $\mathfrak{p}_K M \subset M$, hence $\mathcal{O}_L = M + \mathfrak{p}_K^2 \mathcal{O}_L$, and we would prove the same way that for all $i \geqslant 1$,

$$\mathcal{O}_L = M + \mathfrak{p}_K^i \mathcal{O}_L$$

It is easy to prove that this implies that M is dense $\mathcal{O}_L$ (with respect to the topology induced by ν_L of course). We just have to show that M is closed in $\mathcal{O}_L$ to conclude. This follows from the fact that (K, ν) is complete, and $\mathcal{O}_K$ is closed in (K, ν), see the proof of Proposition 2.25.

□

From the proof we can deduce the following useful result :

Corollary 3.2. *Under the assumptions of the proposition above, if one further assumes that κ_L/κ is separable, then there exists $x \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[x]$*

Proof. We denote by ν_L the unique extension of ν to L, and by w_L the normalization of ν_L, so that a local parameter $\pi_L \in \mathcal{O}_L$ satisfies $w_L(\pi_L) = 1$ (with the notations of the preceding proposition one has $w_L = e.\nu_L$).

Since κ_L/κ is finite and separable, one can find $\gamma \in \kappa_L$ such that $\kappa_L = \kappa(\gamma)$ (a primitive element). Then $1, \gamma, \dots, \gamma^{f-1}$ form a basis of κ_L/κ. Let us denote by $\bar{g}$ the minimal polynomial of γ over κ, and let us take g to be any lift of $\bar{g}$ to $\mathcal{O}_K[X]$ (i.e. g is a polynomial in $\mathcal{O}_K[X]$ which reduction modulo $\mathfrak{p}_K$ is $\bar{g} \in \kappa[X]$). Then we claim that there exists a representative $x \in \mathcal{O}_L$ of γ, such that $g(x)$ is a local parameter for $\mathcal{O}_L$. Indeed, take any x in $\mathcal{O}_L$ such that $x \bmod \mathfrak{p}_L = \gamma$. Then $g(x) \bmod \mathfrak{p}_L = \bar{g}(\gamma) = 0$, so $w_L(g(x)) \geqslant 1$. If it is equal to one, then we are done. Otherwise, take π_L any uniformizer in $\mathcal{O}_L$. Then by lemma 2.9 :

$$g(x + \pi_L) = g(x) + \pi_L g'(x) + \pi_L^2 y \quad \text{for some } y \in \mathcal{O}_L$$

As κ_L/κ is separable, $\bar{g}$ is a separable polynomial, so $g'(x) \bmod \mathfrak{p}_L = \bar{g}'(x \bmod \mathfrak{p}_L) = \bar{g}'(\gamma) \neq 0$. Thus, $g'(x)$ is in $\mathcal{O}_L^\times = \mathcal{O}_L \setminus \mathfrak{p}_L$. In particular, the term $\pi_L g'(x)$ satifies $w_L(\pi_L g'(x)) = w_L(\pi_L) + w_L(g'(x)) = 1 + 0 = 1$. Since the two other terms have valuation greater than two, $w_L(g(x + \pi_L)) = 1$, hence $g(x + \pi_L)$ is a uniformizer. It suffices to take $x + \pi_L$ instead of x to get a representative of γ such that $g(x)$ is a local parameter in $\mathcal{O}_L$.

To sum it up, we have found $x \in \mathcal{O}_L$ such that $\gamma = (x \bmod \mathfrak{p}_L)$ satisfies that $1, \gamma, \dots, \gamma^{f-1}$ is a basis of κ_L over κ, and $g(x)$ is a local parameter in $\mathcal{O}_L$. The proof of proposition 3.1 shows that $(x^i g(x)^j) \;\; 0 \leqslant i \leqslant f-1, \; 0 \leqslant j \leqslant e-1$, is a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$, hence $\mathcal{O}_L = \mathcal{O}_K[x]$. □

3.2 Unramified and totally ramified extensions

Definition 3.3. *Let K be a complete field with respect to a discrete valuation ν.*

- *A finite extension L/K is called unramified if κ_L/κ is separable and $[L:K] = [\kappa_L : \kappa]$*
- *A finite extension L/K is said to be totally ramified if the residue field extension κ_L/κ is separable and $[L:K] = e(L/K)$ in the degree formula of proposition 3.1.*

Remarks:

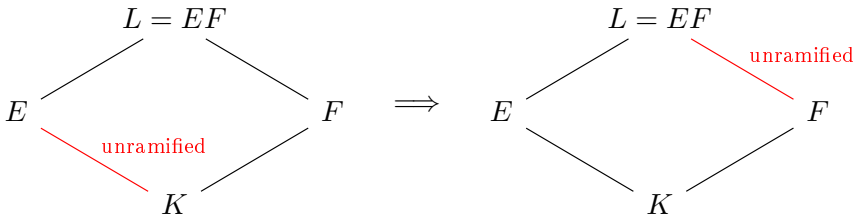
- According to proposition 3.1, L/K is unramified if and only if $\nu_L(L^\times) = \nu(K^\times)$, or equivalently : every local parameter in K is still a local parameter in L.
- With the notations of proposition 3.1, saying that L/K is unramified is just saying that $[L:K] = f$
- Note that if K is a local field, then the separability condition is automatically verified, because κ is a finite field, hence a perfect field.
- The proof of proposition 3.1 shows that if a finite extension L/K is totally ramified of degree n, then $(1, \pi_L, \dots, \pi_L^{n-1})$ is an integral basis of $\mathcal{O}_L$ over $\mathcal{O}_K$. In particular,

$$\mathcal{O}_L = \mathcal{O}_K[\pi_L]$$

- L/K is totally ramified if and only if :

$$\mathfrak{p}_K \mathcal{O}_L = \mathfrak{p}_L^{[L:K]}$$

Proposition 3.4. *Let E/K and F/K be two extensions inside an algebraic closure $\bar{K}/K$, and let $L = EF$. Then one has : E/K unramified $\implies$ L/F unramified. In particular, each subextension of an unramified extension is unramified.*



Proof. First, let us prove the *"in particular"* part. Let $K \subset F \subset E$, and suppose E/K is unramified. Then $L := EF = E$, and the proposition shows that E/F is unramified. Therefore, $[F:K] = [L:K]/[L:F] = [\kappa_L : \kappa]/[\kappa_L : \kappa_F]$. But on the other hand, $[\kappa_L : \kappa] = [\kappa_L : \kappa_F][\kappa_F : \kappa]$. Hence $[F:K] = [\kappa_F : \kappa]$ i.e. F/K is unramified. Less formally, if the extension E/K does not create new possible values for the extended valuation, any subextension cannot create new values, and so is also unramified.

We now prove the main statement. E/K is finite unramified, so κ_E/κ is finite and separable. Let us take $\alpha \in \kappa_E$ such that $\kappa_E = \kappa(\alpha)$ (this is possible by the primitive element theorem). Let $\gamma \in \mathcal{O}_E$ be a representative of α. Let f be the minimal polynomial of γ over K and g be the minimal polynomial of α over κ. Since $\gamma \in \mathcal{O}_E$, f lies in $\mathcal{O}_K[X]$. We denote by $\bar{f}$ its reduction modulo $\mathfrak{p}_K$. Then $\bar{f}(\alpha) = 0$ hence $g | \bar{f}$. So $\deg(\bar{f}) \geqslant [\kappa_E : \kappa]$. Therefore :

$$[\kappa_E : \kappa] \leqslant \deg(\bar{f}) \underset{f \text{ monic}}{=} \deg(f) = [K(\gamma) : K] \leqslant [E:K] = [\kappa_E : \kappa]$$

So there must be equalities all along, and this proves that $E = K(\gamma)$, since $K(\gamma) \subset E$ and they have the same dimension as K vector spaces. Thus,

$$L = EF = K(\gamma)F \underset{K \subset F}{=} F(\gamma)$$

Moreover, $\deg(\bar{f}) = [\kappa_E : \kappa] = \deg(g)$ and so $\bar{f} = g$, the minimal polynomial of α over κ.

Now, let us prove that L/F is unramified. Let h be the minimal polynomial of γ over F (it has coefficients in $\mathcal{O}_F$ because γ is in $\mathcal{O}_E$, hence in $\mathcal{O}_L$). Let $\bar{h}$ be its reduction modulo $\mathfrak{p}_F$. Since $f(\gamma) = 0$ and $f \in K[X] \subset F[X]$, one has $h|f$. But when we compute the euclidean division of f by h in $F[X]$, we are doing it in the ring $\mathcal{O}_F[X]$, and so $h|f$ not only in $F[X]$, but also in $\mathcal{O}_F[X]$. Reducing modulo $\mathfrak{p}_F$ gives us that $\bar{h}|\bar{f}$. The latter is separable because it is the minimal polynomial of α over κ, and κ_E/κ is separable. So $\bar{h}$ is separable. Thus, if $\bar{h}$ factors in $\kappa_F[X]$, then the two factors are relatively prime, and $\bar{h}$ is primitive because it is monic. By theorem 2.18, h would factor in $\mathcal{O}_F[X]$, which is absurd because h is the minimal polynomial of γ over F. Thus, $\bar{h}$ is irreducible in $\kappa_F[X]$, so :

$$[\kappa_L : \kappa_F] \leqslant [L : F] = \deg(h) = \deg(\bar{h}) = [\kappa_F(\gamma \bmod \mathfrak{p}_L) : \kappa_F] \leqslant [\kappa_L : \kappa_F]$$

Thus, $\kappa_L = \kappa_F(\gamma \bmod \mathfrak{p}_L)$, so κ_L/κ_F is separable because $(\gamma \bmod \mathfrak{p}_L)$ has $\bar{h}$ as minimal polynomial, and $\bar{h}$ is separable. We also have $[L : F] = [\kappa_L : \kappa_F]$, hence the conclusion : L/F is unramified. □

Corollary 3.5. *The compositum of two unramified extensions of K is again unramified.*

Proof. Suppose E/K and F/K are two unramified extension, then by the preceding proposition E/K unramified $\implies$ EF/F unramified. Hence F/K is unramified and EF/F is unramified. This implies that EF/K is unramified because separability is transitive and the degree in field extensions is multiplicative. □

Proposition 3.6. *If K is complete with respect to a discrete valuation, then for any finite extension L/K such that κ_L/κ is separable, there exists a unique extension F of K contained in L such that F/K is unramified and L/F is totally ramified. This field F is called the inertial subfield of the extension L/K.*

Proof. Since κ_L/κ is finite and separable, one can find a primitive element α for this extension, i.e. there exists $\alpha \in \kappa_L^\times$ such that $\kappa_L = \kappa(\alpha)$. Let $g \in \kappa[X]$ be the minimal polynomial of α over κ. Let $h \in \mathcal{O}_K[X]$ be a monic polynomial which reduction modulo $\mathfrak{p}_K$ gives g :

$$\bar{h} := h \bmod \mathfrak{p}_K = g \in \kappa[X]$$

Then h is irreducible in $K[X]$. Indeed, g is irreducible in $\kappa[X]$, and h is monic, so h is irreducible in $\mathcal{O}_K[X]$ (it is easy to see this by contrapositive, write a factorization of h in $\mathcal{O}_K[X]$ and reduce it modulo $\mathfrak{p}_K$, this leads to a non trivial facorization of g in $\kappa[X]$). But this implies the irreducibility of h in $K[X]$ (in general, if A is a UFD, the irreducible polynomials in $A[X]$ are the ones that are irreducible in $\mathrm{Frac}(A)[X]$ and *primitive* (meaning that the gcd of their coefficients is equal to one). One example that one can have in mind to remember which implication is true is the following : the polynomial $2X \in \mathbf{Z}[X]$ is irreducible over $\mathbf{Q}$, but it is not irreducible in $\mathbf{Z}[X]$ because 2 is not a unit in $\mathbf{Z}$. Thus, being irreducible in $\mathbf{Z}[X]$ is a stronger condition than being irreducible in $\mathbf{Q}[X]$).

Now, let $\gamma \in \mathcal{O}_L$ such that $\gamma \bmod \mathfrak{p}_L = \alpha \in \kappa_L$. Then :

$$\begin{cases} h(\gamma) \bmod \mathfrak{p}_L = g(\alpha) = 0 \\ h'(\gamma) \bmod \mathfrak{p}_L = g'(\alpha) \neq 0 \text{ because } (\kappa_L/\kappa \text{ separable } \implies g \text{ separable}) \end{cases}$$

By Hensel's lemma (see corollary 2.13), there exists $\beta \in \mathcal{O}_L$ such that $h(\beta) = 0$ and $\beta \bmod \mathfrak{p}_L = \gamma \bmod \mathfrak{p}_L = \alpha$. We define :

$$F := K(\beta) \subset L$$

Composing $\mathcal{O}_F \hookrightarrow \mathcal{O}_L$ and $\mathcal{O}_L \twoheadrightarrow \kappa_L$ gives a ring homomorphism :

$$\begin{array}{rccc} \varphi & : & \mathcal{O}_F & \to & \kappa_L \\ & & a & \mapsto & a \bmod \mathfrak{p}_L \end{array}$$

$\mathfrak{p}_F$ is clearly included in $\ker(\varphi)$, hence φ factors to a ring homomorphism :

$$\begin{array}{rccc} \overline{\varphi} & : & \kappa_F & \to & \kappa_L \\ & & a \bmod \mathfrak{p}_F & \mapsto & a \bmod \mathfrak{p}_L \end{array}$$

Since κ_F is a field, it is injective, but it is also surjective, becasuse $\beta \in \mathcal{O}_F$, and $\overline{\varphi}(\beta) = \alpha$ and $\kappa_L = \kappa(\alpha)$. Therefore, the residue field extension κ_L/κ_F has degree 1, hence L/F is totally ramified.
On the other hand, since h is irreducible, it is the minimal polynomial of β over K, hence :

$$[F : K] = [K(\beta) : K] = \deg(h) = \deg(g) = [\kappa(\alpha) : \kappa] = [\kappa_L : \kappa] = [\kappa_F : \kappa]$$

because κ_F and κ_L are isomorphic as fields, and as κ-vector spaces via $\overline{\varphi}$. This shows that F/K is unramified and concludes the proof of the existence of a subextension F such that :

$$\begin{array}{c} L \\ \big) \text{ totally ramified} \\ F \\ \big) \text{ unramified} \\ K \end{array}$$

It remains to prove that F is unique with these properties. Suppose F' also satisfies $K \subset F' \subset L$, F'/K is unramified and L/F' is totally ramified. Then the compositum FF' is again unramified by corollary 3.5. From the inclusions :

$$F \subset FF' \subset L$$

we can deduces the following for the inertia degrees :

$$f(F/K) \leqslant f(FF'/K) \leqslant f(L/K)$$

But as we have just seen, $\kappa_F \simeq \kappa_L$ as κ-vector spaces, hence :

$$f(L/K) = [\kappa_L : \kappa] = [\kappa_F : \kappa] = f(F/K)$$

Therefore, one must have :

$$f(F/K) = f(FF'/K)$$

But since the two extensions are both unramified, this implies :

$$[F : K] = [FF' : K]$$

But $F \subset FF'$, so we can deduce that $F = FF'$, and this implies that $F' \subset F$. The same method can be repeated to show the converse inclusion, hence $F = F'$. □

Remark : If one further assumes that κ_L/κ is Galois, then in the proposition above, F/K is Galois. Indeed, if we assume κ_L/κ to be Galois, then since g is irreducible in $\kappa[X]$ and has a root in κ_L, it has all its roots in κ_L. g being separable, its roots are all distinct, so κ_L contains the $f(L/K)$ distinct roots of g. Let us denote f instead of $f(L/K)$ for the inertia degree of the extension L/K (recall that $f = [\kappa_L : \kappa]$ by definition). We denote by $\alpha_1, \alpha_2, \ldots, \alpha_f$ the roots of g, α_1 being the α of the proof of the proposition.

By what we saw in the proof, there exist $\gamma_1, \gamma_2, \ldots, \gamma_f \in \mathcal{O}_F$, unique modulo $\mathfrak{p}_F$, such that :

$$\forall 1 \leqslant i \leqslant f,\ \alpha_i = \gamma_i \bmod \mathfrak{p}_L$$

Then :

$$\forall 1 \leqslant i \leqslant f,\ \begin{cases} h(\gamma_i) \bmod \mathfrak{p}_L = g(\alpha_i) = 0 \\ h'(\gamma_i) \bmod \mathfrak{p}_L = g'(\alpha_i) \neq 0 \end{cases}$$

Via the isomorphism $\overline{\varphi}$, the same holds if we replace $\mathfrak{p}_L$ by $\mathfrak{p}_F$. Thus, by Hensel's lemma, for all $1 \leqslant i \leqslant f$, there exists a unique $\beta_i \in \mathcal{O}_F$ such that $h(\beta_i) = 0$ and $\beta_i \bmod \mathfrak{p}_F = \gamma_i \bmod \mathfrak{p}_F$. Suppose that $\beta_i = \beta_j$ for some $i \neq j$: Then $\gamma_i - \gamma_j = 0 \bmod \mathfrak{p}_F$. But $\mathfrak{p}_F \subset \mathfrak{p}_L$, hence $\gamma_i \bmod \mathfrak{p}_L = \gamma_i \bmod \mathfrak{p}_L$, i.e. $\alpha_i = \alpha_j$: Contradiction. Therefore, $\beta_1, \ldots, \beta_f$ are all distinct, so we found f roots of h, which is of degree f : we have all of them. Thus, $\mathcal{O}_F$ contains all the roots of h, and F is generated over K by one of them, so F is the splitting field of h over K. Since h is irreducible in $K[X]$ and separable, F/K is Galois.

Theorem 3.7. *Let K be complete with respect to a discrete valuation, and let L/K be a finite Galois extension. Assume that κ_L/κ is separable. Then κ_L/κ is Galois and there is a surjective group homomorphism :*

$$Gal(L/K) \twoheadrightarrow Gal(\kappa_L/\kappa)$$

whose kernel, denoted by $I_{L/K}$, is called the inertia subgroup of $Gal(L/K)$.
Moreover, $I_{L/K} = Gal(L/F)$ where F is the inertial subfield of L/K.

Proof. With the notations of the proof of proposition 3.6, since h is irreducible in $K[X]$ and has a root in L (namely β), it must split into linear factors in $L[X]$ because L/K is Galois. Therefore, there exist $\beta_1, \ldots, \beta_f \in L$ such that $\beta_1 = \beta$ and :

$$h(X) = \prod_{i=1}^{f} (X - \beta_i) \in L[X]$$

Besides, we have seen in the proof of proposition 3.6 that all the roots of h have valuation zero, hence :

$$\forall 1 \leqslant i \leqslant f,\ \beta_i \in \mathcal{O}_L$$

Reducing modulo $\mathfrak{p}_L$ leads to :

$$\bar{h} = \prod_{i=1}^{f} \left(X - \underbrace{(\beta_i \bmod \mathfrak{p}_L)}_{:=\alpha_i} \right) = g$$

Thus, the roots of g are all in κ_L, and we know that $\kappa_L = \kappa(\beta_1 \bmod \mathfrak{p}_L) = \kappa(\alpha)$, so that κ_L is the splitting field of the separable polynomial g over κ, hence κ_L/κ is Galois.

Now, let us prove that there is a surjective group homomorphism from $Gal(L/K)$ to $Gal(\kappa_L/\kappa)$. Let $\sigma \in Gal(L/K)$. We want explain how σ induces a field automorphism of the residue field κ_L. First, take

$x \in \mathcal{O}_L$. Since $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L, x satisfies a monic polynomial equation over $\mathcal{O}_K$, namely :

$$x^n + \sum_{i=0}^{n-1} a_i x^i = 0, \quad \text{with } a_0, \ldots, a_{n-1} \in \mathcal{O}_K$$

Applying σ, we get

$$\sigma(x)^n + \sum_{i=0}^{n-1} a_i \sigma(x)^i = 0$$

since σ fixes K, hence $\mathcal{O}_K$. Therefore, $\sigma(x)$ is integral over $\mathcal{O}_K$, so it is in $\mathcal{O}_L$. We have proved that $\sigma(\mathcal{O}_L) \subset \mathcal{O}_L$. But the same proof shows that $\sigma^{-1}(\mathcal{O}_L) \subset \mathcal{O}_L$, for σ^{-1} is also in $Gal(L/K)$. Thus, $\sigma\sigma^{-1}(\mathcal{O}_L) \subset \sigma(\mathcal{O}_L)$, hence $\sigma(\mathcal{O}_L) = \mathcal{O}_L$. That is why σ induces a surjective (and injective) ring homomorphism :

$$\sigma_{|\mathcal{O}_L} : \mathcal{O}_L \twoheadrightarrow \mathcal{O}_L$$

Therefore we have a natural ring homomorphism given by :

$$\begin{array}{rccc} \tilde{\sigma} & : & \mathcal{O}_L & \twoheadrightarrow & \kappa_L \\ & & x & \mapsto & \sigma(x) \bmod \mathfrak{p}_L \end{array}$$

Let us show that $\mathfrak{p}_L \subset \ker(\tilde{\sigma})$. It is easy to see that $\nu_L \circ \sigma$ is a valuation on L extending the valuation ν defined on K. Thus, it must be equal to ν_L. This implies that if $\nu_L(x) > 0$, then $\nu_L(\sigma(x)) = \nu_L(x) > 0$ (i.e. if x is zero modulo $\mathfrak{p}_L$, then $\sigma(x)$ is also zero modulo $\mathfrak{p}_L$). So $\tilde{\sigma}$ factors to $\bar{\sigma}$:

$$\begin{array}{rccc} \bar{\sigma} & : & \kappa_L & \twoheadrightarrow & \kappa_L \\ & & x \bmod \mathfrak{p}_L & \mapsto & \sigma(x) \bmod \mathfrak{p}_L \end{array}$$

Now, $\bar{\sigma}$ is injective because κ_L is a field, and so it is a field automorphism. Moreover, $\bar{\sigma}$ fixes κ, for σ fixes K. This explains how any element $\sigma \in Gal(L/K)$ induces $\bar{\sigma} \in Gal(\kappa_L/\kappa)$. Now it is easy to check that $\sigma \mapsto \bar{\sigma}$ is a group homomorphism. Let us prove that is is surjective. Let $\sigma^* \in Gal(\kappa_L/\kappa)$. Since $\kappa_L = \kappa(\alpha_1)$, σ^* is uniquely determined by the image of α_1, which is necessarily a root of g, i.e. one of the α_i's. Suppose that $\sigma^*(\alpha_1) = \alpha_i$. Since h is irreducible and separable, if we denote by H its splitting field over K (such that $K \subset H \subset L$), then $Gal(H/K)$ acts transitively on the roots of h (see proposition 4.2). So there exists $\tau \in Gal(H/K)$ such that $\tau(\beta_1) = \beta_i$. Now, H/K is Galois, so :

$$\begin{array}{ccc} Gal(L/K) & \to & Gal(H/K) \\ \sigma & \mapsto & \sigma_{|H} \end{array} \quad \text{is surjective}$$

Therefore, we can find $\sigma \in Gal(L/K)$ such that $\sigma_{|H} = \tau$, hence $\sigma(\beta_1) = \beta_i$. Then it is clear that $\bar{\sigma} = \sigma^*$, hence the surjectivity we wanted.

Finally, let us prove that $I_{L/K}$, the kernel of :

$$\begin{array}{ccc} Gal(L/K) & \to & Gal(\kappa_L/\kappa) \\ \sigma & \mapsto & \bar{\sigma} \end{array}$$

is actually $Gal(L/F)$. If $\sigma \in Gal(L/F)$, then $\sigma(\beta) = \beta$ because $\beta \in F = K(\beta)$. Therefore,

$$\bar{\sigma}(\alpha) = \bar{\sigma}(\beta \bmod \mathfrak{p}_L) = \sigma(\beta) \bmod \mathfrak{p}_L = \beta \bmod \mathfrak{p}_L = \alpha$$

Since $\kappa_L = \kappa(\alpha)$, this implies that $\bar{\sigma} = id$. Thus, $Gal(L/F) \subset I_{L/K}$. Conversely, if $\sigma \in I_{L/K}$, then $\bar{\sigma} = id$, i.e. $\bar{\sigma}(\alpha) = \alpha$, i.e. $\sigma(\beta) \equiv \beta \bmod \mathfrak{p}_L$. But the roots of h are all representatives of distinct classes modulo

$\mathfrak{p}_L$ because g is separable. Since $\sigma(\beta)$ is also a root of h, it must be equal to β. Therefore, σ fixes β, so it fixes $K(\beta) = F$: $\sigma \in Gal(L/F)$. Thus :

$$I_{L/K} = Gal(L/F)$$

□

Corollary 3.8. *Under the assumptions of theorem 3.7,*

$$Gal(F/K) \simeq Gal(\kappa_L/\kappa)$$

Proof. The preceding theorem shows that :

$$Gal(L/K)/Gal(L/F) \simeq Gal(\kappa_L/\kappa)$$

Besides, in a remark above we proved that when κ_L/κ is Galois, so is F/K. Then Galois theory tells us that :

$$Gal(F/K) \simeq Gal(L/K)/Gal(L/F)$$

hence the result. □

Remark : In particular, if K is a local field, and L/K is finite unramified, then κ_L/κ is Galois because κ is a finite field. This implies that F/K is Galois by a preceding remark, but $F = L$ because L/K is unramified. Therefore, a finite unramified extensions of a local field is always Galois. Moreover, we can apply the corollary, and deduce :

$$Gal(L/K) \simeq Gal(\kappa_L/\kappa)$$

We are now interested in the subextensions of L/F in the preceding theorems. That is why we concentrate on the subextensions of a totally ramified extension.

Let us restate the context. Let K be a complete field with respect to a discrete valuation, with residue field κ of characteristic $p > 0$. Suppose L/K is a finite totally ramified extension of degree n. Proposition 3.1 tells us that :

$$\mathcal{O}_L = \mathcal{O}_K[\pi_L] = \mathcal{O}_K + \pi_L\mathcal{O}_K + \cdots + \pi_L^{e-1}\mathcal{O}_K$$

where π_L is a uniformizer in L and e the ramification index of L/K. Since we assume that the extension is totally ramified, $e = n$. We write $n = n_0 p^l$ with n_0 prime to p. Then we have the following lemma :

Lemma 3.9. *If $z \in L$ satisfies $z^{n_0} = 1$, then $z \in K$*

Proof. Let $f(X) := X^{n_0} - 1$, and let $z \in L$ be a root of f. We denote by ν (respectively $|.|$) the valuation (respectively absolute value) on L extending the one on K. Since $z^{n_0} = 1$, one has $n_0\nu(z) = \nu(1) = 0$, hence $\nu(z) = 0$. In particular, $z \in \mathcal{O}_L$ and so there exist $x_0, x_1, \ldots, x_{e-1} \in \mathcal{O}_K$ such that :

$$z = x_0 + \pi_L x_1 + \cdots + \pi_L^{e-1} x_{e-1}$$

Therefore, it suffices to take $y := x_0$ to get $y \in \mathcal{O}_K$ such that $|y - z| < 1$. Then :

$$f(y) = y^{n_0} - 1 = y^{n_0} - z^{n_0} = (y - z)\underbrace{\left(\sum_{i=0}^{n_0-1} y^i z^{n_0-1-i}\right)}_{:=S}$$

with $S \in \mathcal{O}_L$. So $\nu(f(y)) = \nu(y-z) + \nu(S) \geqslant \nu(y-z)$, hence :

$$|f(y)| \leqslant |y-z| < 1 \tag{5}$$

Besides,

$$|y| \leqslant \max(|y-z|, |z|)$$

But $1 = |z| \neq |y-z|$ so we have an equality, and $|y| = \max(|y-z|, |z|) = |z| = 1$. Thus, $y \in \mathcal{O}_K^\times$.

Now $|f'(y)| = |n_0 y^{n_0-1}|$. But since n_0 is prime to p, $(n_0 \bmod \mathfrak{p}_K) \neq 0$ in κ, so $n_0 \in \mathcal{O}_K^\times$, as well as y^{n_0-1}, so that :

$$|f'(y)| = |\underbrace{n_0 y^{n_0-1}}_{\in \mathcal{O}_K^\times}| = 1 \tag{6}$$

By (5), (6) and Hensel's lemma applied in the field K, there exists a unique $y_0 \in K$ such that $f(y_0) = 0$ and $|y - y_0| < 1$. But if we apply Hensel's lemma in L, we also find that there exists a unique $z_0 \in L$ such that $f(z_0) = 0$ and $|z_0 - y| < 1$. Both conditions are satisfied by y_0 and z, so by the uniqueness, $z = y_0 \in K$. □

From this we can deduce the following theorem, that will be a key tool to answer our main question.

Theorem 3.10. *With the notations introduced above, there exists a unique extension V of K with $K \subset V \subset L$ such that $[V : K] = n_0$. Moreover, there exists π a uniformizer in K, and $\omega \in V$ such that $\omega^{n_0} = \pi$ and $V = K(\omega)$*

Proof. Let π_K be a uniformizer in K. If π_L still denotes a local parameter in L, then we know that $\nu_L(\pi_L^e) = e.\nu_L(\pi_L) = \nu(\pi_K)$. Therefore :

$$\frac{\pi_L^e}{\pi_K} \in \mathcal{O}_L^\times$$

Let $U \in \mathcal{O}_L^\times$ such that $\pi_L^e = U\pi_K$. One can find $x_0, \ldots, x_{e-1} \in \mathcal{O}_K$ such that :

$$U = x_0 + \cdots + \pi_L^{e-1} x_{e-1}$$

and since $U \in \mathcal{O}_L^\times$, $x_0 \in \mathcal{O}_K^\times$. Factorizing by x_0 leads to :

$$U = x_0 Z, \quad \text{where } Z \in \mathcal{O}_L \text{ and } \nu_L(Z-1) > 0$$

Hence :

$$\pi_L^e = x_0 Z \pi_K$$

Recall that since the L/K is totally ramified, $e = n = n_0 p^l$. So the equality above is :

$$\left(\pi_L^{p^l}\right)^{n_0} = Z \underbrace{(x_0 \pi_K)}_{:=\pi}$$

and π is still a uniformizer in K because $x_0 \in \mathcal{O}_K^\times$. We would like to find a n_0-th root of Z, that is why we introduce the polynomial $f := X^{n_0} - Z$. We have seen that $\nu_L(Z-1) > 0$ and this implies :

$$|f(1)| = |1 - Z| < 1$$

Besides,

$$|f'(1)| = |n_0| = 1 \text{ because } n_0 \text{ is prime to } p$$

Therefore, by Hensel's lemma, one finds $v \in L$ such that $f(v) = 0$. Thus :

$$\left(\frac{\pi_L^{p^l}}{v}\right)^{n_0} = \pi$$

We set

$$\omega := \frac{\pi_L^{p^l}}{v} \text{ and } V = K(\omega)$$

It remains to prove that $[V : K] = n_0$, and that it is unique with this degree. Since ω is a zero of $X^{n_0} - \pi$, which is a polynomial with coefficients in K,

$$[V : K] = [K(\omega) : K] \leqslant n_0$$

But since $\omega^{n_0} = \pi$: a uniformizer in K, $n_0 \nu_L(\omega) = \nu(\pi) = 1$, so V contains an element of valuation $1/n_0$, which means that the ramification index $e(V/K)$ is at least n_0. This implies $n_0 \leqslant [V : K]$ because the ramification index is less than the degree of the extension. Therefore :

$$[V : K] = n_0$$

Now, suppose $K \subset W \subset L$ is another extension such that $[W : K] = n_0$. Then since L/K is totally ramified, W/K is also totally ramified, and so by proposition 3.1, $W = K(\pi_W)$ if π_W denotes a uniformizer in W. Then $\pi_W^{n_0}$ is a uniformizer in K, and so there exists $u \in \mathcal{O}_K^\times$ such that :

$$\frac{\pi_W^{n_0}}{\pi} = \left(\frac{\pi_W}{\omega}\right)^{n_0} = u$$

Let us introduce $g = X^{n_0} - u \in K[X]$. Denote by a the fraction π_W/ω. $\nu_L(a) = 0$, so $a \in \mathcal{O}_L^\times$. By the same arguments as earlier in the proof, one can find $z \in \mathcal{O}_K^\times$ such that $|z - a| < 1$. Then :

$$|g(z)| = |z^{n_0} - a^{n_0}| = |z - a| \underbrace{|\dots|}_{\leqslant 1} < 1$$

and :

$$|g'(z)| = |n_0| = 1$$

Hensel's lemma gives us an element $z_0 \in K$ such that $g(z_0) = 0$. Therefore :

$$\left(\frac{\pi_W}{\omega}\right)^{n_0} = u = z_0^{n_0} \implies \left(\frac{\pi_W}{\omega z_0}\right)^{n_0} = 1$$

Using lemma 3.9, we get that $\pi_W/(\omega z_0) \in K$, and since $z_0 \in K$, this tells us that $\pi_W/\omega \in K$, hence :

$$V = K(\omega) = W = K(\pi_W)$$

This concludes the proof.

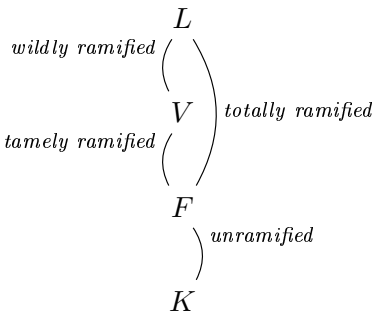
□

3.3 Tamely ramified extensions

Definition 3.11. *Let K be complete with respect to a discrete valuation. Suppose that the residue field κ has characteristic $p > 0$. A finite extension L/K is said to be tamely ramified if the residue field extension κ_L/κ is separable and the ramification index $e(L/K)$ is prime to p. Otherwise, i.e. if $p \mid e(L/K)$, then the extension is said to be wildly ramified.*

Combining the results we have already proved, we can state the following structure theorem :

Theorem 3.12. *Let K be a field complete with respect to a discrete valuation, and let L/K be a finite extension. Suppose that the residue field κ has characteristic $p > 0$ and that κ_L/κ is separable. Then there exist unique fields F and V such that :*



Proof. This follows immediately from proposition 3.6 and theorem 3.10. □

3.4 Ramification groups

Let (K, ν) be a local field, and let L/K be a finite Galois extension, with Galois group denoted by G. ν extends uniquely to a discrete valuation on L, say ω_L. We denote by ν_L the normalization of ω_L, so that a uniformizer in L has valuation 1 for the valuation ν_L. Note that ν_L no longer extends ν, but this way it takes values in $\mathbf{Z}$.

Definition 3.13. *Let $i \in \mathbf{Z}, i \geqslant -1$. We define the i-th ramification group G_i of the extension L/K as follows :*

$$G_i := \{\sigma \in G \mid \forall a \in \mathcal{O}_L,\ \nu_L(\sigma(a) - a) \geqslant i + 1\}$$

Remarks: We know that any $\sigma \in G$ preserves $\mathcal{O}_L$, so G_{-1} is just G. Moreover, by looking at the surjective homomorphism of theorem 3.7, it is clear that G_0 is the inertia subgroup of G, i.e. $G_0 = I_{L/K}$.

If σ belongs to a high ramification group, it means that σ does not move $\mathcal{O}_L$ to much, i.e. every element in $\mathcal{O}_L$ is sent by σ to an element in $\mathcal{O}_L$ that is close to it with respect to the absolute value associated to ν_L.

Proposition 3.14. *$(G_i)_{i \geqslant -1}$ form a decreasing sequence of normal subgroups of G, and they eventually become trivial.*

Proof. The first statement can be easily checked just by writing down what this means. For the second part, recall (see corollary 3.2) that there exists $x \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[x]$. Then one can prove that :

$$G_i = \{\sigma \in G \mid \nu_L(\sigma(x) - x) \geqslant i + 1\}$$

Set :

$$n := \max_{\sigma \in G \setminus \{id\}} \nu_L(\sigma(x) - x)$$

Then $n < +\infty$, for if $\sigma(x) = x$ then $\sigma_{|\mathcal{O}_L} = id$, and this implies that σ is trivial on $L = Frac(\mathcal{O}_L)$. Now for all $i \geqslant n$, $G_i = \{id\}$. □

To sum it up, we have a sequence of normal subgroups of the Galois group :

$$\cdots \subset \underbrace{G_{n+1}}_{=\{id\}} \subset \underbrace{G_n}_{=\{id\}} \subset \cdots \subset G_{i+1} \subset G_i \subset \cdots \subset G_1 \subset \underbrace{G_0}_{=I_{L/K}} \subset \underbrace{G_{-1}}_{=G}$$

Since they are all normal in G, they are in particular normal subgroups of their preceding term :

$$\cdots \lhd \cdots \lhd G_{i+1} \lhd G_i \lhd \cdots \lhd G_1 \lhd G_0 \lhd G_{-1}$$

Now our aim is to study the quotients G_i/G_{i+1}. We already know from theorem 3.7 and the preceding remark that G_{-1}/G_0 is isomorphic to the Galois group of the residue field extension :

$$G_{-1}/G_0 \simeq Gal(\kappa_L/\kappa)$$

We will need the following lemma to simplify the study of the higher order quotients.

Lemma 3.15. *Let π be a uniformizer in L, and $\sigma \in G_0$.*

$$\forall i \geqslant 1,\ \sigma \in G_i \iff \frac{\sigma(\pi)}{\pi} \equiv 1 \ mod\ \pi^i$$

Proof. Let $i \geqslant 1$ and $\sigma \in G_0$.
If $\sigma \in G_i$, then for all $a \in \mathcal{O}_L$, $\nu_L(\sigma(a) - a) \geqslant i + 1$, hence $\sigma(a) - a \equiv 0 \bmod \pi^{i+1}$. In particular, for $a = \pi$, we get :

$$\frac{\sigma(\pi)}{\pi} \equiv 1 \bmod \pi^i \tag{7}$$

Conversely, suppose that (7) is satisfied. Let F be the unique maximal unramified extension such that $K \subset F \subset L$ (see proposition 3.6 and theorem 3.7). Then since L/F is totally ramified, one has $\mathcal{O}_L = \mathcal{O}_F[\pi]$. Therefore for any $\tau \in Gal(L/F)$,

$$(\forall a \in \mathcal{O}_L,\ \nu_L(\tau(a) - a) \geqslant i + 1) \iff \nu_L(\tau(\pi) - \pi) \geqslant i + 1$$

But $Gal(L/F) = I_{L/K} = G_0$, so $\sigma \in Gal(L/F)$. Moreover (7) tells us that σ satisfies the right hand side of the above equivalence, hence : $\forall a \in \mathcal{O}_L,\ \nu_L(\sigma(a) - a) \geqslant i + 1$ i.e. $\sigma \in G_i$ □

We introduce the following notations :

$$\forall i \geqslant 1,\ U_L^{(i)} := 1 + \mathfrak{p}_L^i = 1 + \pi^i \mathcal{O}_L \ \text{ and } \ U_L^{(0)} := \mathcal{O}_L^\times \tag{8}$$

Proposition 3.16. *For all $i \in \mathbf{N}$, there is an injective group homomorphism*

$$\overline{\theta_i} : G_i/G_{i+1} \hookrightarrow U_L^{(i)}/U_L^{(i+1)}$$

Proof. First of all, we shall explain why $U_L^{(i)}$ is a group when $i \geqslant 1$! Let us try to prove that it is a subgroup of $\mathcal{O}_L^\times$. It is clearly stable under product and contains the 1 element, but does any element have an inverse in $U_L^{(i)}$? This is due to the fact that L is complete. Indeed, for any element $x \in \mathfrak{p}_L^i$, the power series $\sum(-1)^n x^n$ converges because its general term tends to zero, and a simple computation shows that this is a multiplicative inverse for $1+x$, and that it is also in $1+\mathfrak{p}_L^i$. Thus, $U_L^{(i)}$ is a subgroup of $\mathcal{O}_L^\times$ (in particular, it is commutative). Morover, one has $U_L^{(i+1)} \subset U_L^{(i)}$ for all $i \in \mathbf{N}$.

Now, let $i \in \mathbf{N}^*$, and let π still denote a uniformizer in L. If $\sigma \in G_i$ then :

$$\frac{\sigma(\pi)}{\pi} \equiv 1 \bmod \pi^i$$

so $\sigma(\pi)/\pi \in U_L^{(i)}$. Therefore, the map :

$$\begin{array}{ccc} G_i & \to & U_L^{(i)} \\ \sigma & \mapsto & \frac{\sigma(\pi)}{\pi} \end{array}$$

is well defined. We can then compose it with the natural surjection :

$$U_L^{(i)} \twoheadrightarrow U_L^{(i)}/U_L^{(i+1)}$$

We obtain the following map :

$$\begin{array}{ccccc} \theta_i & : & G_i & \to & U_L^{(i)}/U_L^{(i+1)} \\ & & \sigma & \mapsto & \frac{\sigma(\pi)}{\pi} U_L^{(i+1)} \end{array}$$

Besides, for $i = 0$, since $\nu_L \circ \sigma = \nu_L$, one has :

$$\nu_L\left(\frac{\sigma(\pi)}{\pi}\right) = 0$$

hence $\sigma(\pi)/\pi \in \mathcal{O}_L^\times = U_L^{(0)}$. So we can define $\theta_0 : G_0 \to U_L^{(0)}/U_L^{(1)}$ by the same formula as for θ_i when $i \geqslant 1$.
Now that we have defined maps θ_i for all $i \in \mathbf{N}$, let us check that these are group homomorphisms with kernel G_{i+1}. Let $i \in \mathbf{N}$ and $\sigma, \tau \in G_i$. Setting $u = \tau(\pi)/\pi$, one has :

$$\frac{(\sigma \circ \tau)(\pi)}{\pi} = \frac{\sigma(\pi)}{\pi}\frac{\tau(\pi)}{\pi}\frac{\sigma(u)}{u} \tag{9}$$

Since $\sigma \in G_i$, $\sigma(u) \equiv u \bmod \pi^{i+1}$ But $u = \tau(\pi)/\pi \in \mathcal{O}_L^\times$ by the same arguments as above, because $\nu_L \circ \tau = \nu_L$. Therefore,

$$\frac{\sigma(u)}{u} \equiv 1 \bmod \pi^{i+1} \quad \text{i.e.} \quad \frac{\sigma(u)}{u} \in U_L^{(i+1)} \tag{10}$$

(9) and (10) yield $\theta_i(\sigma \circ \tau) = \theta_i(\sigma)\theta_i(\tau)$.

Let us determine the kernel of θ_i. If $\sigma \in G_i$,

$$\sigma \in \ker(\theta_i) \iff \frac{\sigma(\pi)}{\pi} \in U_L^{(i+1)} \iff \frac{\sigma(\pi)}{\pi} \equiv 1 \mod \pi^{i+1} \underset{\text{lemma 3.15}}{\iff} \sigma \in G_{i+1}$$

Thus, $\ker(\theta_i) = G_{i+1}$ and so we get injective group homomorphisms :

$$\begin{array}{ccccc} \overline{\theta_i} & : & G_i/G_{i+1} & \hookrightarrow & U_L^{(i)}/U_L^{(i+1)} \\ & & \sigma \mod G_{i+1} & \mapsto & \frac{\sigma(\pi)}{\pi} U_L^{(i+1)} \end{array}$$

□

Now that we know that the successive quotients G_i/G_{i+1} can be identified with subgroups of $U_L^{(i)}/U_L^{(i+1)}$, we need to understand these groups.

Proposition 3.17.

$$U_L^{(0)}/U_L^{(1)} \simeq \left(\kappa_L^\times, .\right) \text{ and for all } i \geqslant 1,\ U_L^{(i)}/U_L^{(i+1)} \simeq \left(\mathfrak{p}_L^i/\mathfrak{p}_L^{i+1}, +\right) \simeq (\kappa_L, +)$$

Proof. Let

$$\begin{array}{rccccc} \varphi & : & \mathcal{O}_L^\times = U_L^{(0)} & \twoheadrightarrow & & \kappa_L^\times \\ & & a & \mapsto & a & \mod \pi \end{array}$$

It is a well-defined, surjective, group homomorphism. Moreover,

$$a \in \ker(\varphi) \iff a \in 1 + (\pi) = U_L^{(1)}$$

Hence $U_L^{(0)}/U_L^{(1)}$ is isomorphic to the multiplicative group of the residue field of the extension.

Now , let $i \geqslant 1$. Consider the following map :

$$\begin{array}{ccccc} U_L^{(i)} & \twoheadrightarrow & & & \mathfrak{p}_L^i/\mathfrak{p}_L^{i+1} \\ 1+x & \mapsto & x & \mod & \mathfrak{p}_L^{i+1} \end{array}$$

One checks easily that this is a surjective group homomorphism with kernel $U_L^{(i+1)}$ hence :

$$U_L^{(i)}/U_L^{(i+1)} \simeq \left(\mathfrak{p}_L^i/\mathfrak{p}_L^{i+1}, +\right)$$

But the latter is isomorphic to $(\kappa_L, +)$ via :

$$\begin{array}{ccccc} \mathcal{O}_L & \twoheadrightarrow & & & \mathfrak{p}_L^i/\mathfrak{p}_L^{i+1} \\ a & \mapsto & a\pi^i & \mod & \mathfrak{p}_L^{i+1} \end{array}$$

which factors through $\mathfrak{p}_L = (\pi)$. □

Summary : We have proved that there are embeddings :

$$G_0/G_1 \hookrightarrow (\kappa_L^\times, .)$$

and

$$\forall i \geqslant 1,\ G_i/G_{i+1} \hookrightarrow (\kappa_L, +)$$

This allows us to deduce many consequences about the structure of G_0. Indeed, the first embedding tells us that G_0/G_1 can be seen as a finite subgroup of $(\kappa_L^\times, .)$, and therefore G_0/G_1 is a cyclic group. In particular it is abelian. Morever, as subgroups of $(\kappa_L, +)$, the quotients G_i/G_{i+1} for $i \geqslant 1$ are abelian. Therefore, we have a sequence of normal subgroups of G_0 :

$$\cdots \lhd \cdots \lhd G_{i+1} \lhd G_i \lhd \cdots \lhd G_1 \lhd G_0$$

such that they eventually become trivial and all the successive quotients are abelian groups. This means (by definition) that G_0 is solvable ! But we can be more precise concerning the structure of the groups G_i/G_{i+1}.

Suppose κ_L has characteristic zero. Then $(\kappa_L, +)$ has only $\{0\}$ as a finite subgroup, hence for all $i \geqslant 1$, G_i/G_{i+1} is the trivial group, i.e. $G_i = G_{i+1}$. But G_k is trivial for k sufficiently large, so for all $i \geqslant 1$, $G_i = \{id\}$. Then $G_0/G_1 = G_0$ and this implies that G_0 is a cyclic group.

Now, suppose κ_L has characteristic $p > 0$. Then finite subgroups of $(\kappa_L, +)$ are finite dimensional $\mathbf{F}_p$ vector spaces, hence isomorphic to $(\mathbf{F}_p^{n_i}, +)$ for some $n_i \in \mathbf{N}$. Thus, we obtain :

$$\forall i \geqslant 1, \exists n_i \in \mathbf{N},\ G_i/G_{i+1} \simeq \left(\mathbf{Z}/p\mathbf{Z}\right)^{n_i}$$

Let us prove that G_1 is a p-group, that is : a group of order p^m for some $m \in \mathbf{N}$.
For all $i \geqslant 1$ we have $\#G_i = \#\left(G_{i+1}\right)\#\left(G_i/G_{i+1}\right)$. Besides, for N sufficiently large, $G_N = \{id\}$. Therefore,

$$\begin{aligned} \#G_{N-1} &= \#\left(G_{N-1}/G_N\right) = p^{n_{N-1}} \\ \#G_{N-2} &= \#(G_{N-1})\#(G_{N-2}/G_{N-1}) = p^{n_{N-1}}p^{n_{N-2}} \\ &\vdots \\ \#G_1 &= \textstyle\prod_{i=1}^{N-1} p^{n_i} \quad \text{is a power of } p \end{aligned}$$

Finally, assume that the residue field of K, namely κ, is a finite field. Then κ_L/κ is a finite extension of a finite field, so it has a cyclic Galois group. Since :

$$G/G_0 \simeq Gal(\kappa_L/\kappa)$$

we deduce that G/G_0 is cyclic, hence solvable. Now, we have the following standard result :

Lemma 3.18. *Let G be a group. If $H \triangleleft G$,*

$$\begin{cases} H \text{ solvable} \\ G/H \text{ solvable} \end{cases} \implies G \text{ solvable}$$

Proof. See [Go] theorem XIII.16 □

Using lemma 3.18 with $G = Gal(L/K)$ and $H = G_0$, we obtain that when κ is finite, $Gal(L/K)$ is solvable.

Let us summarize all these results in the following proposition :

Proposition 3.19. *Let L/K be a finite Galois extension of a complete field with respect to a discrete valuation. Denoting by G_i the ramification groups as in definition 3.13. We have the following properties :*

- *G_0/G_1 is cyclic*
- *G_0 is solvable*
- *If κ_L has characteristic 0, then for all $i \geqslant 1$, $G_i = \{id\}$ and G_0 is a cyclic group*
- *If κ_L has characteristic $p > 0$, then for all $i \geqslant 1$, there exists $n_i \in \mathbf{N}$ such that*

$$G_i/G_{i+1} \simeq \left(\mathbf{Z}/p\mathbf{Z}\right)^{n_i}$$

and G_1 is a p-group

- *If κ (the residue field of K) is finite, then $G = G_{-1}$ is solvable*

In particular, the last point tells us that if $K = \mathbf{Q}_p$, then for any finite Galois extension $L/\mathbf{Q}_p$, the Galois group $Gal(L/\mathbf{Q}_p)$ will be solvable. Now, it is well known that $\mathfrak{S}_n$ is not solvable as soon as $n \geqslant 5$, and that is is solvable for $n \leqslant 4$ (it is, in my opinion, very nicely done in chapter XIII of [Go]. It starts from the definition of solvability, and the proof of this result is then very detailed). Therefore, if $n \geqslant 5$, $\mathfrak{S}_n$ cannot be the Galois group of a finite extension of $\mathbf{Q}_p$! This is a great first step in our way to answer the main question, because now we are reduced to study the possibility of $\mathfrak{S}_n$-extensions for $n \in \{2, 3, 4\}$, and these groups are not too large. However, as we will see, this is not so easy to work out the remaining cases.

4 The Galois group of a polynomial

In this section, we forget a little about local fields, and state some general results from Galois theory.

4.1 Definition and first properties

Let K be a field, and $\bar{K}$ a fixed algebraic closure of K. Let us take f to be a separable monic polynomial of degree $n \geqslant 1$ in $K[X]$. This means that it has only simple roots in $\bar{K}$ i.e. there exist $\alpha_1, \ldots, \alpha_n \in \bar{K}$, all distinct, such that :

$$f = (X - \alpha_1) \ldots (X - \alpha_n) \text{ in } \bar{K}[X]$$

Let us denote by L the splitting field of f over K :

$$L := K(\alpha_1, \ldots, \alpha_n) \subset \bar{K}$$

Then since f is separable, L/K is Galois, and we define the Galois group of the polynomial f to be the Galois group of the extension L/K.

Now, consider a fixed index $i \in \{1, \ldots, n\}$, and $\sigma \in Gal(L/K)$. Applying σ to the equation $f(\alpha_i) = 0$ leads to $f(\sigma(\alpha_i)) = 0$, because f has coefficients in K. Therefore, there exists a unique index j such that $\sigma(\alpha_i) = \alpha_j$. So we can define the following map :

$$\begin{array}{rccc} \varphi_\sigma & : & \{1, \ldots, n\} & \to & \{1, \ldots, n\} \\ & & i & \mapsto & \text{the unique } j \text{ such that } \sigma(\alpha_i) = \alpha_j \end{array}$$

If $\varphi_\sigma(i) = \varphi_\sigma(i')$ then this means that $\sigma(\alpha_i) = \sigma(\alpha_{i'})$. Since σ is injective, one has $\alpha_i = \alpha_{i'}$, hence $i = i'$. Therefore, φ_σ is injective, and since it goes from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$, it is bijective. That is why we can define the following map from the Galois group of a polynomial into the set of permutations of the indices of the roots :

$$\begin{array}{rccc} \varphi & : & Gal(L/K) & \to & \mathfrak{S}_n \\ & & \sigma & \mapsto & \varphi_\sigma \end{array}$$

One proves easily the following :

Proposition 4.1. *The map φ from the discussion above is an injective group homomorphism.*

This tells us that there is an embedding :

$$Gal(L/K) \hookrightarrow \mathfrak{S}_n$$

One important think to notice is that this embedding is not canonical, since it depends one the choice of the numbering of the roots. So we cannot canonically identify the Galois group of f with a subgroup of $\mathfrak{S}_n$, but only with a subgroup "up to conjugation".

Remark : Seeing the Galois group of a separable polynomial of degree n as a subgroup of $\mathfrak{S}_n$ is the original point of view of Galois. The modern way to introduce Galois groups as groups of automorphisms of field extensions is due to Dedekind.

Proposition 4.2. *Let $f \in K[X]$ be separable of degree n, with Galois group G.*

(i) If f is irreducible in $K[X]$, then $n \mid \#G$

(ii) f is irreducible in $K[X]$ if and only if G (as a subgroup of $\mathfrak{S}_n$) acts transitively on $\{1, \dots, n\}$

Proof. See appendix 7.3 □

This proposition is very useful for our main purpose. Indeed, if one wants to find an extension $K/\mathbf{Q}_p$ with Galois group $\mathfrak{S}_3$, it can be a good idea to look for an irreducible polynomial of degree 3 in $\mathbf{Q}_p[X]$. Since $\mathbf{Q}_p$ has characteristic zero, such a polynomial would also be separable. The splitting field of this polynomial over $\mathbf{Q}_p$ will give an extension $K/\mathbf{Q}_p$ with Galois group G, and this group will be a transitive subgroup of $\mathfrak{S}_3$. Now, it is easy to verify that the only transitive subgroups of $\mathfrak{S}_3$ are $\mathfrak{S}_3$ and $\mathfrak{A}_3$. Therefore, we just need a tool to be able to say whether the extension will have Galois group $\mathfrak{S}_3$ or $\mathfrak{A}_3$ when we pick an irreducible polynomial of degree 3 in $\mathbf{Q}_p[X]$. This is the point of the following theorem.

Theorem 4.3. *Let K be a field of characteristic $\neq 2$. Let $P \in K[X]$ be a separable polynomial, monic of degree $n \geqslant 2$, i.e. :*

$$P = (X - \alpha_1) \dots (X - \alpha_n)$$

in some fixed algebraic closure of K. We still denote by L the splitting field of P over K, namely $L = K(\alpha_1, \dots, \alpha_n)$ and by φ the natural embedding $Gal(L/K) := G \hookrightarrow \mathfrak{S}_n$. Let us introduce

$$d(P) := \prod_{i<j} (\alpha_i - \alpha_j)$$

Then :

- $\forall g \in G,\ g(d(P)) = \varepsilon(\varphi(g))d(P)$
- *Under the Galois correspondence, the subgroup $\varphi^{-1}(\mathfrak{A}_n) \subset G$ corresponds to the subfield $K(d(P)) \subset L$*

Proof. See [Go] theorem XI.32 □

Corollary 4.4. *$\varphi(G) \subset \mathfrak{A}_n$ if and only if $disc(P)$ is a square in $K^\times$ (denoted by $disc(P) \in (K^\times)^2$)*

Proof. By the theorem above, one has :

$$\varphi(G) \subset \mathfrak{A}_n \iff \varphi^{-1}(\mathfrak{A}_n) = G \iff K(d(P)) = K \iff d(P) \in K$$

But since $disc(P) = d(P)^2$, the last condition is equivalent to $disc(P) \in (K^\times)^2$, hence the result. □

4.2 Galois groups of cubics and quartics

The discussion in the last section tells us how to proceed to find polynomials with Galois group $\mathfrak{S}_3$. Indeed, let us say that P is a polynomial of degree 3, with coefficients in a field K with characteristic different from 2. Suppose that P is irreducible over K, and separable. Then the Galois group G of this polynomial can be identified with $\varphi(G)$ which is a transitive subgroup of $\mathfrak{S}_3$. Therefore, $\varphi(G)$ can only be $\mathfrak{A}_3$ or $\mathfrak{S}_3$. Besides, the distinction can be done using the discriminant of P, by corollary 4.4. We get the following proposition :

Proposition 4.5. *Let K be a field of characteristic $\neq 2$, and $P \in K[X]$ an irreducible, separable, monic, cubic. If $disc(P) \in (K^\times)^2$, then $G \simeq \mathfrak{A}_3$. Otherwise, $G \simeq \mathfrak{S}_3$*

Remark : If K has characteristic zero, then irreducible implies separable, so we do not need to check this condition. This fact follows from the following proposition :

Proposition 4.6. *Let K be a field, and $P \in K[X]$ an irreducible polynomial. Then : P is inseparable if and only if $P' = 0$.*

Proof. $\boxed{\Rightarrow}$ Suppose $P \in K[X]$ is irreducible and inseparable. Then there exists $a \in \bar{K}$ such that :

$$(X-a)^2 \mid P \text{ in } \bar{K}[X]$$

This implies that $(X-a)$ divides both P and P' in $\bar{K}[X]$. Thus, P and P' have a common factor in $\bar{K}[X]$, so that they are not coprime in $\bar{K}[X]$. Therefore, when one computes Euclid's algorithm for P and P', the last non-zero remainder has degree $\geqslant 1$. But since P and P' are ine $K[X]$, all the polynomials that appear in the successive euclidean divisions are in $K[X]$, and the computation of the last non-zero remainder gives the GCD of P and P' in $K[X]$. Therefore, the GCD of P and P' in $K[X]$ has degree $\geqslant 1$, so P and P' share a common irreducible factor in $K[X]$. Since P is irreducible, this implies that P divides P'. However, $\deg(P') < \deg(P)$, so P' must be zero.

Alternative proof : Since a is a root of P and P', the minimal polynomial of a over K, say f, is a common irreducible factor of P and P'. Since P and f are irreducible and $f \mid P$, there exists $\lambda \in K^\times$ such that $P = \lambda f$, and so :

$$f \mid P' \implies P \mid P'$$

Afterward, the proof is the same.

$\boxed{\Leftarrow}$ If $P' = 0$ then P and P' certainly have a common root in $\bar{K}$, hence : P is inseparable. □

In particular, if we assume that K has characteristic zero and P is irreducible, then $P' = 0$ implies $P \in K$. This gives a contradiction because P is irreducible. Therefore, $P' \neq 0$ and P is also separable.

Now, let us study the case of quartic polynomials. The problem is that there are more transitive subgroups in $\mathfrak{S}_4$ than there are in $\mathfrak{S}_3$, so it is more complicated to distinguish which irreducible polynomial gives which subgroup. The discriminant is not sufficient to make the distinction. The idea is to associate to a quartic a cubic polynomial, called its cubic resolvent. The Galois group of our quartic P will now depend on the behaviour of P, but also of its cubic resolvent. The motivation to the definition of the cubic resolvent is detailed in [Co] : *Galois groups of cubics and quartics (not in characteristic 2)*, as well as many examples of quartics over $\mathbf{Q}$ with all the possible Galois groups. The following definition and theorem can be found in this reference, but also in chapter XVII, §5, in [Go].

Definition 4.7. *Let K be a field with characteristic $\neq 2$, and let $P \in K[X]$ be an irreducible monic polynomial of degree 4 :*

$$P(X) = X^4 - a_1X^3 + a_2X^2 - a_3X + a_4$$

The cubic resolvent of P is :

$$R_3(P) := X^3 - a_2X^2 + (a_1a_3 - 4a_4)\,X - \left(a_1^2a_4 + a_3^2 - 4a_2a_4\right)$$

Remark : In fact, if we denote the roots of P by $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, one has :

$$R_3(P) = (X - (\alpha_1\alpha_2 + \alpha_3\alpha_4))\,(X - (\alpha_1\alpha_3 + \alpha_2\alpha_4))\,(X - (\alpha_1\alpha_4 + \alpha_2\alpha_3))$$

(See Keith Conrad's expository paper for the motivation of this definition and the computation of the coefficients). Then it is easy to see that P and $R_3(P)$ have the same discriminant. We denote by Δ this common discriminant, and by G the Galois group of P over K. Then we have the following :

Theorem 4.8. *We denote by K^2 the set $\{x^2, x \in K\}$.*

(i) $G \simeq \mathfrak{S}_4 \iff R_3(P)$ *is irreducible and* $\Delta \notin K^2$

(ii) $G \simeq \mathfrak{A}_4 \iff R_3(P)$ *is irreducible and* $\Delta \in K^2$

(iii) $G \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \iff R_3(P)$ *splits completely over* K

(iv) $G \simeq \mathbf{Z}/4\mathbf{Z} \iff R_3(P)$ *has exactly one root in* K *and* P *is reducible over* $K(\sqrt{\Delta})$

(v) $G \simeq D_4 \iff R_3(P)$ *has exactly one root in* K *and* P *is irreducible over* $K(\sqrt{\Delta})$

Proof. See [Go] theorem XVII.22, or Keith Conrad's expository paper *Galois groups of cubics and quartics (not in characteristic 2)* ([Co]) □

Now, we have all the tools we need to answer completely our question, at least for the question of the existence of extensions, this is the aim of the next section. Then, we will try to work out the question of the classification of the extensions when we know there are some.

5 Answer to our main question

Recall : We are trying to find out for which (n, p) there exist $\mathfrak{S}_n$-extensions of $\mathbf{Q}_p$, that is : finite Galois extensions of $\mathbf{Q}_p$ with Galois group $\mathfrak{S}_n$.

5.1 Quadratic extensions of $\mathbf{Q}_p$

If one takes any $\alpha \in \mathbf{Q}_p$ such that α is not a square in $\mathbf{Q}_p$, then $\mathbf{Q}_p(\sqrt{\alpha})/\mathbf{Q}_p$ is a finite Galois extension with Galois group of order 2, i.e. a $\mathfrak{S}_2$-extension. The existence of elements in $\mathbf{Q}_p \setminus (\mathbf{Q}_p)^2$ is given by propositions 2.14 and 2.15, and so quadratic extensions of $\mathbf{Q}_p$ can certainly occur. The interesting question is to classify these extensions, and we will do this in section 6.1.

5.2 The cases $(n \geqslant 5)$ and $(n = 4 \ \& \ p \geqslant 3)$

Let $p \geqslant 2$ be a prime number. Then $\mathbf{Q}_p$ is complete with respect to a discrete valuation, with finite residue field (isomorphic to $\mathbf{F}_p$). As we have seen in proposition 3.19, any finite Galois extension $L/\mathbf{Q}_p$ has a solvable Galois group, hence $Gal(L/\mathbf{Q}_p)$ cannot be isomorphic to $\mathfrak{S}_n$, if $n \geqslant 5$.

n \ p	2	3	5	7	11	... ...
2						
3						
4						
5						
⋮						
⋮						

Now, let us try to understand the case $n = 4$: *For which p can $\mathfrak{S}_4$ occur as the Galois group of an extension of $\mathbf{Q}_p$?*

- First, let us assume $p \geqslant 5$.

  Suppose that there exists a Galois extension $L/\mathbf{Q}_p$ with Galois group $G \simeq \mathfrak{S}_4$. By proposition 3.19, we know that G_1 is a p-group. But $\#G_1 \mid \#\mathfrak{S}_4 = 24 = 2^3 \times 3$. Since $\#G_1$ is a power of p, the only way that it divides 24 is that G_1 is trivial. Thus, G_0/G_1 is isomorphic to G_0. Besides, proposition 3.19 tells us that G_0/G_1 is cyclic, hence G_0 is cyclic. However, it is easy to check that $\mathfrak{S}_4$ has no normal cyclic subgroup, except $\{id\}$. This implies that $G_0 = \{id\}$ and $G/G_0 \simeq G = Gal(L/\mathbf{Q}_p)$. Now, G/G_0 is isomorphic to the Galois group of the residue field extension, which is a cyclic group (Galois group of a finite extension of finite field). So G is a cyclic group, whereas we assumed $G \simeq \mathfrak{S}_4$: This is a contradiction.

- Now, let us consider the case $p = 3$.

  Once again, we assume that there exists an extension $L/\mathbf{Q}_p$ with Galois group $G \simeq \mathfrak{S}_4$. The difference with the last point is that this time $\#G_1$ is a power of 3 dividing 24, so it could be 3. However, if $\#G_1 = 3$, then denoting by $\varphi : G \to \mathfrak{S}_4$ an isomorphism between the two groups, $\varphi(G_1)$ is a normal subgroup of $\mathfrak{S}_4$ which contains a 3-cycle, and this implies that $\mathfrak{A}_4 \subset \varphi(G_1)$. Therefore :

  $$12 = \#\mathfrak{A}_4 \leqslant \#\varphi(G_1) = \#G_1 = 3 \implies \text{Contradiction.}$$

  Thus, $\#G_1 = 1$, and we can repeat the same proof as when $p \geqslant 5$ to show that $\mathfrak{S}_4$-extensions of $\mathbf{Q}_3$ do not occur.

Summary table :

n \ p	2	3	5	7	11	... ...
2						
3						
4						
5						
⋮						
⋮						

All the the gray cells in this table correspond to tuples (n, p) for which there is no finite Galois extension $L/\mathbf{Q}_p$ with Galois group $\mathfrak{S}_n$.

5.3 The case $n = 3$

5.3.1 If $p \neq 3$

First, let us assume $p \geqslant 5$.

Suppose there exists a finite Galois extension $L/\mathbf{Q}_p$ with Galois group $G := Gal(L/\mathbf{Q}_p)$ isomorphic to $\mathfrak{S}_3$. Then by proposition 3.19, G_1 is a p-group and its order divides the order of G, namely 6. Therefore, $G_1 = \{id\}$. So $G_0/G_1 \simeq G_0$, and we know that G_0/G_1 is a cyclic group, hence G_0 is a cyclic group.

Now, if $L/\mathbf{Q}_p$ is totally ramified, then $G = G_0$, and so G is cyclic. Since $\mathfrak{S}_3$ is not cyclic, this cannot happen : $L/\mathbf{Q}_p$ cannot be totally ramified.

On the other hand, if $L/\mathbf{Q}_p$ is unramified, then $G_0 = \{id\}$, hence $G/G_0 \simeq G$. But we know that G/G_0 is cyclic, so G is cyclic. Once again, since $\mathfrak{S}_3$ is not cyclic, this cannot happen : $L/\mathbf{Q}_p$ cannot be unramified.

Therefore, in the formula $[L : \mathbf{Q}_p] = e(L/\mathbf{Q}_p)f(L/\mathbf{Q}_p) = e.f$, we cannot have $e(L/\mathbf{Q}_p) = 1$ or $e(L/\mathbf{Q}_p) = 6$. Either $e = 2$ and $f = 3$ or $e = 3$ and $f = 2$. But if we consider $F = L^{G_0}$ the maximal unramified subextension of the extension $L/\mathbf{Q}_p$ (as in proposition 3.6 and theorem 3.7), we have $Gal(L/F) \lhd Gal(L/\mathbf{Q}_p)$. Since $\mathfrak{S}_3$ has no normal subgroup of order 2, $\#Gal(L/F) = 3 = [L : F]$. This implies that $[F : \mathbf{Q}_p] = 2 = f$.

To sum it up, if $L/\mathbf{Q}_p$ is a $\mathfrak{S}_3$-extension, then we are in the following situation :

$$\begin{array}{c} L \\ \big) \text{ totally ramified of degree 3} \\ F \\ \big) \text{ unramified of degree 2} \\ \mathbf{Q}_p \end{array}$$

Now, let H be any subgroup of G of order 2. Let L^H be the corresponding subfield of L under the Galois correspondence. Then L^H has degree 3 over $\mathbf{Q}_p$. Since 3 is prime, the extension $L^H/\mathbf{Q}_p$ is either unramified or totally ramified. But it cannot be unramified because it is of degree 3, and the inertia degree of $L/\mathbf{Q}_p$ is 2. Therefore, $L^H/\mathbf{Q}_p$ is totally ramified of degree 3, which is prime to p : the characteristic of the residue field of $\mathbf{Q}_p$ (this is where the assumption $p \neq 3$ is important). This tells us that $L^H/\mathbf{Q}_p$ is

tamely ramified, so we can apply theorem 3.10 !

By this theorem, one can find π a uniformizer in $\mathbf{Q}_p$, and an element $\omega \in L^H$ such that $\omega^3 = \pi$ and $L^H = \mathbf{Q}_p(\omega)$. Now, suppose that $\mu_3 := \{\zeta \in \overline{\mathbf{Q}_p} \mid \zeta^3 = 1\} \subset \mathbf{Q}_p$. Then $\mathbf{Q}_p(\omega)$ is the splitting field of the Eisenstein polynomial $X^3 - \pi$ over $\mathbf{Q}_p$. This implies that $L^H/\mathbf{Q}_p$ is Galois, so H is a normal subgroup of G. But as we said before, in $\mathfrak{S}_3$, a subgroup of order 2 cannot be normal, so we have a contradiction. We have proved that if a $\mathfrak{S}_3$-extension $L/\mathbf{Q}_p$ exists, then $\mathbf{Q}_p$ cannot contain μ_3.

Besides, $\mu_3 \subset \mathbf{Q}_p \iff X^3 - 1$ splits in $\mathbf{Q}_p \iff X^2 + X + 1$ splits in $\mathbf{Q}_p \iff disc(X^2 + X + 1)$ is a square in $\mathbf{Q}_p \iff -3 \in \mathbf{Q}_p^2$

Since $-3 \in \mathbf{Z}_p^\times$, the last condition is equivalent to $-3 \in \left(\mathbf{Z}_p^\times\right)^2$, and this is (by proposition 2.14) the same as -3 being a square modulo p (because $p \neq 2$). However, the question *"For which p is -3 a square modulo p ?"* is not so easy to turn into a simple condition on p, whereas the question *"Which p is a square modulo 3 ?"* is very simple ! Gladly, the quadratic reciprocity law allows us to turn the not so easy question into the easy one. Before this, we need to introduce a notation : the Legendre symbol, to write the quadratic reciprocity law in a concise way.

Definition 5.1. *Let p be an odd prime number. We define, for all $a \in \mathbf{F}_p^\times$, the Legendre symbol :*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \iff a \in \left(\mathbf{F}_p^\times\right)^2 \\ -1 \iff a \notin \left(\mathbf{F}_p^\times\right)^2 \end{cases}$$

It satisfies the following property :

$$\forall a \in \mathbf{F}_p^\times, \ \left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$$

and :

$$\begin{array}{rccc} \mathcal{L} & : & \mathbf{F}_p^\times & \to & \{-1, 1\} \\ & & a & \mapsto & \left(\frac{a}{p}\right) \end{array}$$

is a non-trivial group homomorphism.

Proof. If $a \in \mathbf{F}_p^\times$, then :

$$a^{p-1} = 1 = \left(a^{\frac{p-1}{2}}\right)^2$$

Therefore,

$$a^{\frac{p-1}{2}} \in \{-1, 1\}$$

So the following map is well defined, and is clearly a group homorphism :

$$\begin{array}{rccc} \mathcal{L}' & : & \mathbf{F}_p^\times & \to & \{-1, 1\} \\ & & a & \mapsto & a^{\frac{p-1}{2}} \end{array}$$

We want to prove that $\mathcal{L} = \mathcal{L}'$. It suffices to show that for all $a \in \mathbf{F}_p^\times$,

$$a^{\frac{p-1}{2}} = 1 \iff a \in \left(\mathbf{F}_p^\times\right)^2$$

which amounts to prove that the kernel of $\mathcal{L}'$ is equal to the image of :

$$\begin{array}{rccc} u & : & \mathbf{F}_p^\times & \to & \mathbf{F}_p^\times \\ & & x & \mapsto & x^2 \end{array}$$

Clearly, $\mathrm{Im}(u) \subset \ker(\mathcal{L}')$, so we just need to prove that these two sets have the same number of elements. Since $\mathrm{Im}(u) \simeq \mathbf{F}_p^\times/\ker(u)$ and $\ker(u) = \{-1, 1\}$ has order 2 ($-1 \neq 1$ because p is an odd prime), one has :

$$\#\mathrm{Im}(u) = \frac{p-1}{2}$$

Now, since $\mathcal{L}'$ is a group homomorphism, we know that :

$$\#\ker(\mathcal{L}') = \frac{p-1}{\#\mathrm{Im}(\mathcal{L}')}$$

So to get the conclusion we want, we need to prove that $\#\mathrm{Im}(\mathcal{L}') = 2$ i.e. there exist elements x in $\mathbf{F}_p^\times$ such that $x^{(p-1)/2}$ is not equal to 1. But the polynomial

$$X^{\frac{p-1}{2}} - 1$$

cannot have $p-1$ distinct roots because its degree is $\frac{p-1}{2}$, so $\#\mathrm{Im}(\mathcal{L}') = 2$ and we obtain the result. □

Proposition 5.2. *(Quadratic reciprocity law)*
Let p, q be two distinct odd primes. Then :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Proof. See [Go] theorem XII.25 □

Using this, we can compute $\left(\frac{-3}{p}\right)$ as follows :

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right) = (-1)^{p-1}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$$

Therefore,

$$\mu_3 \subset \mathbf{Q}_p \iff -3 \in \mathbf{Q}_p^2 \iff -3 \in \left(\mathbf{F}_p^\times\right)^2 \iff \left(\frac{-3}{p}\right) = 1 \iff \left(\frac{p}{3}\right) = 1$$

But now, it is easy to check that p is square modulo 3 if and only of $p \equiv 1 \bmod 3$, so we have finally found a very simple condition on p for the existence of an $\mathfrak{S}_3$-extension of $\mathbf{Q}_p$. Indeed :

If such an extension $L/\mathbf{Q}_p$ exists, then $\mu_3 \not\subset \mathbf{Q}_p$, hence $p \not\equiv 1 \bmod 3$ i.e. $p \equiv 2 \bmod 3$ (because $p \geqslant 5$ is a prime, it is not congruent to zero modulo 3).

Conversely, suppose $p \equiv 2 \bmod 3$.

The polynomial $P = X^3 - p$ is irreducible in $\mathbf{Q}_p[X]$ because it is Eisenstein. Since $\mathbf{Q}_p$ has characteristic zero, it is also separable. By proposition 4.5, it suffices to compute its discriminant to tell the Galois group

of this polynomial. This can be done by computing the resultant of P and P', so this is not hard, but it can be tedious. I just take the following result as a fact :

$$disc(X^3 + aX + b) = -4a^3 - 27b^2 \tag{11}$$

Thus, $disc(P) = -27p^2 = -3(3p)^2$, so that :

$$disc(P) \in \mathbf{Q}_p^2 \iff -3 \in \mathbf{Q}_p^2 \iff \left(\frac{-3}{p}\right) = 1 \iff \left(\frac{p}{3}\right) = 1 \iff p \equiv 1 \bmod 3$$

Since we assumed $p \equiv 2 \bmod 3$, $disc(P)$ is not a square in $\mathbf{Q}_p$, so the Galois group of P over $\mathbf{Q}_p$ is isomorphic to $\mathfrak{S}_3$ by proposition 4.5. Therefore, there exists a $\mathfrak{S}_3$-extension of $\mathbf{Q}_p$.

Summary : For all primes $p \geqslant 5$, $\mathfrak{S}_3$ arises as the Galois group of an extension of $\mathbf{Q}_p$ if and only if $p \equiv 2 \bmod 3$.

Moreover, if $p = 2$ then the polynomial $X^3 - 2$ also gives a $\mathfrak{S}_3$-extension of $\mathbf{Q}_2$. Indeed, it is irreducible and separable, and its discriminant is a square in $\mathbf{Q}_2$ if and only if -3 is a square $\mathbf{Q}_2$. But $-3 \not\equiv 1 \bmod 8$, so by proposition 2.15, $disc(X^3 - 2)$ is not a square in $\mathbf{Q}_2$. Thus, the Galois group of $X^3 - 2$ over $\mathbf{Q}_2$ is isomorphic to $\mathfrak{S}_3$.

5.3.2 If $p = 3$

$X^3 - 3$ is irreducible and separable, and its discriminant is $-27(-3)^2 = -3^5$ which is not a square in $\mathbf{Q}_3$, because 5 is odd. Therefore, the splitting field of this polynomial over $\mathbf{Q}_3$ gives a $\mathfrak{S}_3$-extension of $\mathbf{Q}_3$.

5.3.3 Summary

n \ p	2	3	5	7	11	... ...
2						
3						
4						
5						
⋮						
⋮						

In the green line of this table, $\mathfrak{S}_3$ can occur as the Galois group of an extension of $\mathbf{Q}_p$ if and only if $p = 3$ or $p \equiv 2 \bmod 3$

5.4 The case ($n = 4$ & $p = 2$)

Let us consider, for instance, the polynomial $P = X^4 + 2X + 2 \in \mathbf{Q}_2[X]$. P is Eisenstein, hence irreducible. Besides, its cubic resolvent is $R_3(P) = X^3 - 8X - 4$. This polynomial is again irreducible. Indeed, its Newton polygon (see appendix 7.1) is given by the figure below :

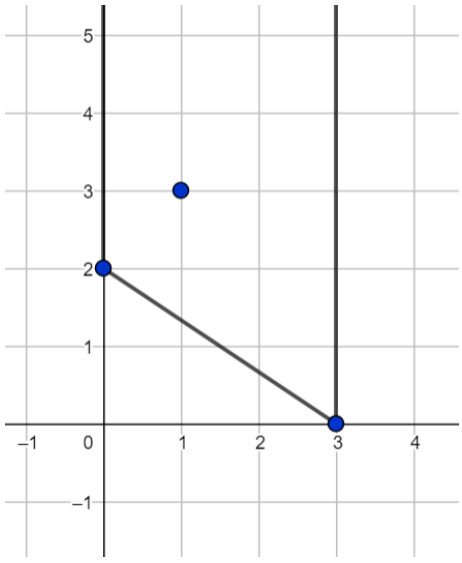


Figure 1: Newton polygon of $R_3(P) = X^3 - 8X - 4 \in \mathbf{Q}_2[X]$

The polygon has only one finite side, and the slope of this side is $-\frac{2}{3}$. Since 2 and 3 are coprime, $R_3(P)$ is irreducible in $\mathbf{Q}_2[X]$ by corollary 7.4. Moreover, a simple computation using (11) shows that

$$disc(P) = disc(R_3(P)) = disc(X^3 - 8X - 4) = -4(-8)^3 - 27 \times 4^2 = 1616 = 2^4 \times 101$$

Therefore :

$$disc(P) \in (\mathbf{Q}_2)^2 \iff 101 \in (\mathbf{Q}_2)^2 \iff 101 \equiv 1 \bmod 8 \quad \text{(by proposition 2.15)}$$

However, $101 = 96 + 5 = 8 \times 12 + 5$, hence $101 \not\equiv 1 \bmod 8$ i.e. $disc(P) \notin (\mathbf{Q}_2)^2$
To sum it up, P satisfies :

$$\begin{cases} P \text{ is irreducible (Eisenstein) in } \mathbf{Q}_2[X] \\ R_3(P) \text{ is irreducible in } \mathbf{Q}_2[X] \\ disc(P) \text{ is not a square in } \mathbf{Q}_2 \end{cases}$$

By theorem 4.8 *(i)*, the Galois group of P over $\mathbf{Q}_2$ is isomorphic to $\mathfrak{S}_4$. Thus, there exist $\mathfrak{S}_4$-extensions of $\mathbf{Q}_2$!

5.5 Conclusion

In the summary table of paragraph 5.3.3, all the white cells correspond to tuples (n, p) for which extensions exist, all the grey cells correspond to tuples for which we know there is no such extension, and finally what happens in the green line is explained under the summary table.

6 Classification of the $\mathfrak{S}_n$-extensions of $\mathbf{Q}_p$ when they exist

6.1 Classification of the quadratic extensions of $\mathbf{Q}_p$

If K is a field with characteristic $\neq 2$, then any extension L/K of degree 2 is Galois and of the form $L = K(\alpha)$ with $\alpha^2 \in K^\times \setminus (K^\times)^2$. $(1, \alpha)$ is a basis of L as a K vector space, so that every element in L

can be written uniquely $x+y\alpha$ with $x, y \in K$. Using this, it is easy to prove that two quadratic extensions of K, say $K(\alpha)$ and $K(\beta)$, are the same if and only if $\alpha/\beta \in K$.

To reformulate this, quadratic extensions of K look like $K\left(\sqrt{\Delta}\right)$ with Δ in $K^\times \setminus (K^\times)^2$ and :

$$K\left(\sqrt{\Delta}\right) = K\left(\sqrt{\Delta'}\right) \iff \frac{\Delta}{\Delta'} \in \left(K^\times\right)^2 \iff \overline{\Delta} = \overline{\Delta'} \text{ in } K^\times/(K^\times)^2$$

Therefore, to describe all the quadratic extensions of K, it suffices to find a set of representatives of $K^\times/(K^\times)^2$. If $\{1, \Delta_1, \ldots, \Delta_n\}$ is a set of representatives of $K^\times/(K^\times)^2$, then the quadratic extensions of K (inside a fixed algebraic closure) are $K(\Delta_1), \ldots, K(\Delta_n)$. So we just need to study $\mathbf{Q}_p^\times/\left(\mathbf{Q}_p^\times\right)^2$ to answer the question of the classification of the quadratic extensions of $\mathbf{Q}_p$.

First, let us assume that $p \geqslant 3$. We know that any element in $\mathbf{Q}_p^\times$ can be written uniquely as a power of p times a p-adic unit. This gives an isomorphism :

$$\mathbf{Q}_p^\times \simeq (\mathbf{Z}, +) \times (\mathbf{Z}_p^\times, .)$$

Therefore,

$$\mathbf{Q}_p^\times/\left(\mathbf{Q}_p^\times\right)^2 \simeq (\mathbf{Z}/2\mathbf{Z}) \times \left(\mathbf{Z}_p^\times/\left(\mathbf{Z}_p^\times\right)^2\right)$$

Besides, by proposition 2.16 :

$$\mathbf{Z}_p^\times \simeq \mathbf{Z}/(p-1)\mathbf{Z} \times \mathbf{Z}_p$$

Since p does not divide 2, 2 is a unit in $\mathbf{Z}_p$, so $2\mathbf{Z}_p = \mathbf{Z}_p$. This implies :

$$\mathbf{Z}_p^\times/\left(\mathbf{Z}_p^\times\right)^2 \simeq \mathbf{Z}/2\mathbf{Z}$$

Conclusion :

$$\mathbf{Q}_p^\times/\left(\mathbf{Q}_p^\times\right)^2 \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$$

So this group has 3 non trivial elements, i.e. $\mathbf{Q}_p$ has exactly 3 quadratic extensions in a fixed algebraic closure. Let us be more explicit :

Let $\varepsilon \in \mathbf{Z}_p^\times \setminus \left(\mathbf{Z}_p^\times\right)^2$. Such an ε exists by proposition 2.14. Then it is not hard to see that $\{1, p, \varepsilon, p\varepsilon\}$ is a set of representatives of $\mathbf{Q}_p^\times/\left(\mathbf{Q}_p^\times\right)^2$, just by checking that the quotients $1/p, \varepsilon/p, p\varepsilon/\varepsilon, \ldots$ are not squares in $\mathbf{Q}_p^\times$.

Thus, if $p \neq 2$ is a prime, then $\mathbf{Q}_p$ has exactly 3 quadratic extensions, namely :

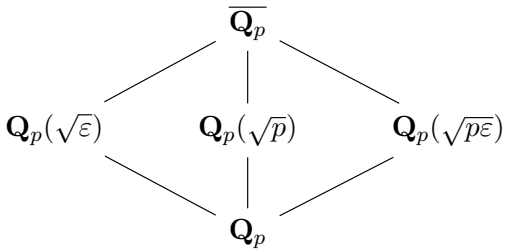


Figure 2: The three quadratic extensions of $\mathbf{Q}_p$ ($p \neq 2$)

Now, let us consider the case $p = 2$. To understand the quadratic extensions of $\mathbf{Q}_2$, we need to understand the group $\mathbf{Q}_2^\times/(\mathbf{Q}_2^\times)^2$.

First, $\mathbf{Q}_2^\times \simeq \mathbf{Z} \times \mathbf{Z}_2^\times \simeq \mathbf{Z} \times \{\pm 1\} \times (1 + 4Z_2)$ (see proposition 2.17), so :

$$\mathbf{Q}_2^\times/(\mathbf{Q}_2^\times)^2 \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times (1 + 4\mathbf{Z}_2)/(1 + 4\mathbf{Z}_2)^2$$

Claim : $(1 + 4\mathbf{Z}_2)^2 = 1 + 8\mathbf{Z}_2$.

Let us prove this statement using Newton polygons (appendix 7.1). It is clear that $(1 + 4\mathbf{Z}_2)^2 \subset 1 + 8\mathbf{Z}_2$. To prove the converse, suppose b is an element of $2\mathbf{Z}_2$. We want to prove that the polynomial

$$f(X) := (1 + 2^2X)^2 - (1 + 2^2b) \in \mathbf{Q}_2[X]$$

has a root in $\mathbf{Z}_2$. $f(X) = -2^2b + 2^3X + 2^4X^2$, so the Newton polygon of $f(X)$ looks like this :

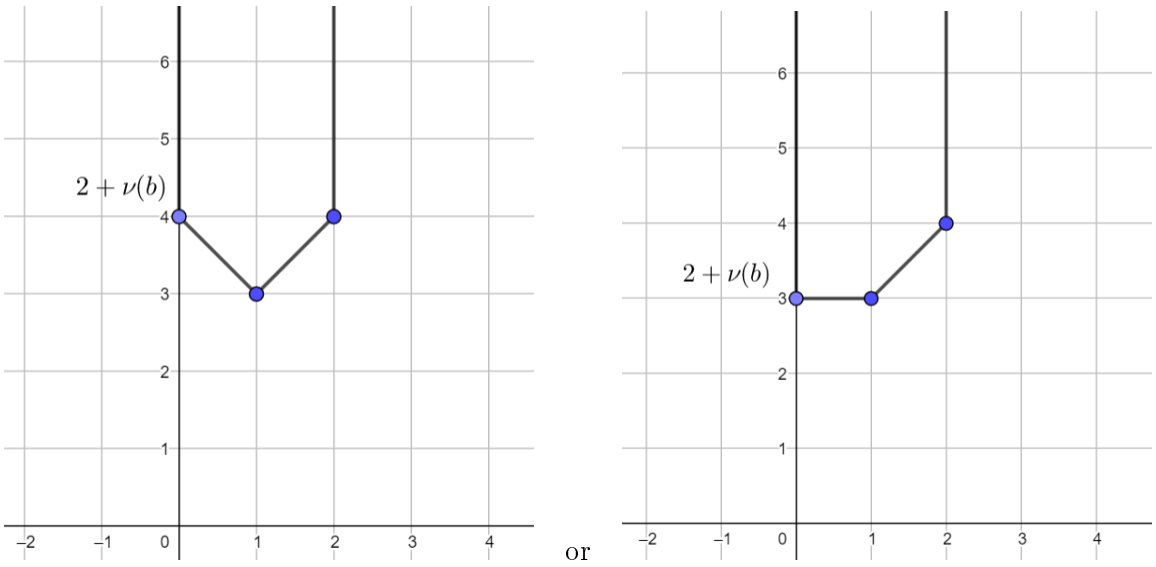


Figure 3: possible shapes of the Newton polygon of $f(X)$, depending on the value of $\nu(b)$, where ν is the usual valuation on $\mathbf{Q}_2$

In any case, the first finite side corresponds to a single root, so this root must be in $\mathbf{Q}_2$, and since the slope is $\leqslant 0$, the root must have a valuation $\geqslant 0$, which means that the root lies in $\mathbf{Z}_2$. Therefore, we get the conclusion we wanted : $f(X)$ has a root in $\mathbf{Z}_2$, hence $1 + 8\mathbf{Z}_2 \subset (1 + 4\mathbf{Z}_2)^2$.

This implies :

$$(1 + 4\mathbf{Z}_2)/(1 + 4\mathbf{Z}_2)^2 = (1 + 4\mathbf{Z}_2)/(1 + 8\mathbf{Z}_2) = U_{\mathbf{Q}_2}^{(2)}/U_{\mathbf{Q}_2}^{(3)}$$

with the notations introduced in section 3.4 equation (8). We have seen in proposition 3.17 that this last group is isomorphic to the residue field of $\mathbf{Q}_2$ for the additive law, namely $\mathbf{Z}/2\mathbf{Z}$. Therefore,

$$\mathbf{Q}_2^\times/(\mathbf{Q}_2^\times)^2 \simeq (\mathbf{Z}/2\mathbf{Z})^3 \quad (\mathbf{F}_2\text{-vector space of dimension 3})$$

Since this group contains 7 non trivial elements, $\mathbf{Q}_2$ has exactly 7 quadratic extensions. To find elements that are not squares in $\mathbf{Q}_2$, we try to find elements in $\mathbf{Z}_2^\times$ that are not congruent to 1 modulo 8.

Odd integers are in $\mathbf{Z}_2^\times$, so $3, -3, -1$ are good candidates. Now we proceed as above by multiplying these numbers by 2 we get $6, -6, -2$ which represent other classes in $\mathbf{Q}_2^\times/\left(\mathbf{Q}_2^\times\right)^2$, and finally 2 is not a square in $\mathbf{Q}_2$. It is not hard to prove that :

$$\{1, 2, -2, 3, -3, -1, 6, -6\}$$

is a set of representatives of $\mathbf{Q}_2^\times/\left(\mathbf{Q}_2^\times\right)^2$. This gives us the following classification : Inside an algebraic closure $\overline{\mathbf{Q}_2}$, there are 7 extensions of degre 2 of $\mathbf{Q}_2$, namely :

$$\mathbf{Q}_2(\sqrt{2}),\ \mathbf{Q}_2(\sqrt{-2}),\ \mathbf{Q}_2(\sqrt{3}),\ \mathbf{Q}_2(\sqrt{-3}),\ \mathbf{Q}_2(\sqrt{-1}),\ \mathbf{Q}_2(\sqrt{6}) \text{ and } \mathbf{Q}_2(\sqrt{-6})$$

6.2 The line $n = 3$ for $p \neq 3$

We have already proved (see paragraph 5.3.1) that $\mathfrak{S}_3$ can occur as a Galois group of an extension of $\mathbf{Q}_p$ if and only if $p \equiv 2 \bmod 3$. Let us show that in this case, such an extension is unique, and is given by the splitting field of the polynomial $X^3 - p$ over $\mathbf{Q}_p$.

Suppose that $p \equiv 2 \bmod 3$ and $L/\mathbf{Q}_p$ is a finite Galois extension with Galois group $G := Gal(L/\mathbf{Q}_p)$ isomorphic to $\mathfrak{S}_3$. Let H be a subgroup of G of order 2. As usual, we denote by L^H the corresponding subfield of L under the Galois correspondence.

$$\begin{array}{c} L \\ | \\ L^H \\ | \\ \mathbf{Q}_p \end{array}$$

As in paragraph 5.3.1, we have that since $[L^H : \mathbf{Q}_p] = 3$, the extension $L^H/\mathbf{Q}_p$ is totally ramified. Besides, 3 is prime to p. Therefore, by theorem 3.10, there exists $\omega \in L^H$ such that $L^H = \mathbf{Q}_p(\omega)$ and $\omega^3 = p.u$ for some $u \in \mathbf{Z}_p^\times$ (i.e. ω^3 is a uniformizer in $\mathbf{Q}_p$).

Now, let us prove that $x \mapsto x^3$ is surjective from $\mathbf{Z}_p^\times$ to $\mathbf{Z}_p^\times$.

- First, suppose $p \geqslant 5$. Then by proposition 2.16,

  $$\mathbf{Z}_p^\times \simeq \mathbf{Z}/(p-1)\mathbf{Z}\ \times \mathbf{Z}_p$$

  Since $p \equiv 2 \bmod 3$, $(p-1)$ is prime to 3, so 3 is a unit in $\mathbf{Z}/(p-1)\mathbf{Z}$. Therefore, multiplication by 3 is a bijection of $\mathbf{Z}/(p-1)\mathbf{Z}$. Moreover, p does not divide 3, so $3 \in \mathbf{Z}_p^\times$. Thus, multiplication by 3 is also a bijection of $\mathbf{Z}_p$. This proves that $x \mapsto x^3$ is surjective from $\mathbf{Z}_p^\times$ to $\mathbf{Z}_p^\times$.

- Else, if $p = 2$, proposition 2.17 tells us :

  $$\mathbf{Z}_2^\times \simeq \{\pm 1\} \times (1 + 4\mathbf{Z}_2)$$

  Since $x \mapsto x^3$ induces id on $\{\pm 1\}$, we just need to prove that $x \mapsto x^3$ is surjective from $(1 + 4\mathbf{Z}_2)$ to $(1 + 4\mathbf{Z}_2)$.

Let $1 + 2^2 a \in 1 + 4\mathbf{Z}_2$.
We want to show that the polynomial $P = \left(1 + 2^2 X\right)^3 - \left(1 + 2^2 a\right) \in \mathbf{Q}_2[X]$ has a root in $\mathbf{Z}_2$. One has :

$$P = -2^2 a + 3 \times 2^2 X + 3 \times 2^4 X^2 + 2^6 X^3$$

Therefore, the Newton polygon of P has the following shape :

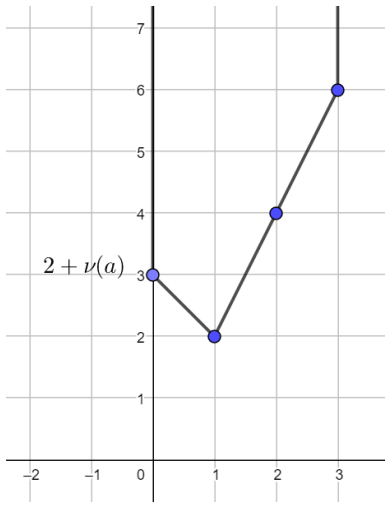


Figure 4: Newton polygon of $P = \left(1 + 2^2 X\right)^3 - \left(1 + 2^2 a\right) \in \mathbf{Q}_2[X]$

The first finite side starting from the left tells us that P has a single root with valuation the opposite of the slope of this side. This root necessarily lies in $\mathbf{Q}_2$. Moreover, the first side has a non-positive slope, so the root has a non-negative valuation, i.e. it is in $\mathbf{Z}_2$ (even if $\nu(a) = 0$). Thus, P has a root in $\mathbf{Z}_2$, and this concludes the proof that $x \mapsto x^3$ is surjective from $\mathbf{Z}_2^\times$ to $\mathbf{Z}_2^\times$.

We proved that $L^H = \mathbf{Q}_p(\omega)$ with ω such that $\omega^3 = p.u$ for some $u \in \mathbf{Z}_p^\times$. Since raising to the third power is surjective in $\mathbf{Z}_p^\times$, there exists $v \in \mathbf{Z}_p^\times$ such that $v^3 = u$. Therefore,

$$\frac{\omega}{v} \in L^H \text{ and } \left(\frac{\omega}{v}\right)^3 = p$$

This implies that L^H contains a root of $X^3 - p$, hence L contains a root of $X^3 - p$. Since this polynomial is irreducible (Eisenstein) and $L/\mathbf{Q}_p$ is Galois (hence normal), $X^3 - p$ splits in L i.e. L contains all the roots of $X^3 - p$. If we denote by F the splitting field of $X^3 - p$ over $\mathbf{Q}_p$, one has : $F \subset L$. We want to prove that this inclusion is an equality.

$L^H = \mathbf{Q}_p(\omega) = \mathbf{Q}_p\left(\frac{\omega}{v}\right)$ because $v \in \mathbf{Z}_p^\times$. Since w/v is a root of $X^3 - p$, $L^H \subset F$. However, $L^H/\mathbf{Q}_p$ is not Galois, because $\mathfrak{S}_3$ has no normal subgroup of order 2, whereas $F/\mathbf{Q}_p$ is Galois. Therefore, $L^H \subsetneq F$, so that :

$$\underbrace{[L^H : \mathbf{Q}_p]}_{=3} < \underbrace{[F : \mathbf{Q}_p]}_{\text{divides } 6}$$

This implies that $[F : \mathbf{Q}_p] = 6 = [L : \mathbf{Q}_p]$, so that the inclusion $F \subset L$ is in fact an equality : $F = L$. Conclusion : L is the splitting field of $X^3 - p$ over $\mathbf{Q}_p$.

To sum it up, in paragraph 5.3.1, we proved that there exist $\mathfrak{S}_3$-extensions of $\mathbf{Q}_p$ if and only if $p \equiv 2 \bmod 3$ or $p = 3$. The discussion above shows that in the case where $p \neq 3$, if a $\mathfrak{S}_3$-extension of $\mathbf{Q}_p$ exists, then it is unique, and it is the splitting field of $X^3 - p$ over $\mathbf{Q}_p$.

6.3 Partial conclusion

In the following table, we summarize what we proved so far. At the intersection of the row n and the column p, one reads the number of $\mathfrak{S}_n$-extensions of $\mathbf{Q}_p$, that is : the number of finite Galois extensions $K/\mathbf{Q}_p$ inside a fixed algebraic closure $\overline{\mathbf{Q}_p}$ such that $Gal(K/\mathbf{Q}_p) \simeq \mathfrak{S}_n$. The cells coloured in grey correspond to tuples (n, p) such that there is no such extension.

n \ p	2	3	5	7	11	... ...
2	7	3	3	3	3	3
3	1	$\exists$	1	0	1	$\mathbb{1}_{p\equiv 2 \bmod 3}$
4	$\exists$					
5						
⋮						
⋮						

The two cells coloured in red correspond to tuples (n, p) for which we know there exist extensions, but we have not achieved their classification yet. Indeed, there exists a $\mathfrak{S}_3$-extension of $\mathbf{Q}_3$ by paragraph 5.3.2, and there exists a $\mathfrak{S}_4$-extension of $\mathbf{Q}_2$ by subsection 5.4.

An attempt to classify $\mathfrak{S}_3$-extensions of $\mathbf{Q}_3$ is presented in the appendix, section 7.6.

7 Appendix

7.1 Newton polygons

In this section, we define the Newton polygon of a polynomial, which will give us a geometric way to tell the valuations of the roots of a polynomial from the valuations of its coefficients ! But first, we start with a classic lemma which will be useful in the proof of the main theorem of this section.

Lemma 7.1. *Let K be a field with characteristic $p > 0$. Let $f \in K[X]$ be irreducible. If f is not separable, then there exists $g \in K[X]$ irreducible and separable, and $k \in \mathbf{N}^*$, such that*

$$f(X) = g(X^{p^k})$$

Proof. Since f is irreducible and inseparable, one must have $f' = 0$ (thanks to proposition 4.6). Thus, f must be of the form :

$$f = a_0 + a_1 X^p + a_2 X^{2p} + \cdots + a_n X^{np}$$

Setting $g_1 = a_0 + \cdots + a_n X^n$, one has $f(X) = g_1(X^p)$. Now, g_1 is irreducible because f is, and if it is separable, we are done. If g_1 is not separable, we can apply the same proof to g_1 and find g_2 irreducible such that $g_1(X) = g_2(X^p)$. Then $f(X) = g_2(X^{p^2})$. Continuing in this fashion, we eventually find g_k separable, irreducible such that $f(X) = g_k(X^{p^k})$. □

Let K be a field, and ν a discrete (normalized) valuation on K. Let $f \in K[X]$, say :

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

Then for any $i \in \{1, \ldots, n\}$, define $A_i \in \mathbf{Z}^2$ to be the point with coordinates $(i, \nu(a_i))$. If $a_i = 0$, then $\nu(a_i) = +\infty$, and in this case we say that A_i is the point at infinity on the positive vertical axis : $(0, +\infty)$.

Definition 7.2. *The Newton polygon of f, is the convex hull of the set of points*

$$\{A_i, i \in \{1, \ldots, n\}\}$$

Example : Let us take $K = \mathbf{Q}_5$, with the 5-adic valuation, simply denoted by ν. Consider the polynomial $f = 5X^{10} + 5^2 X^6 + 5^{-1} X^5 + X^4 + 5^2 X + 5^7 \in \mathbf{Q}_5[X]$. Then $A_{10} = (10, 1), A_6 = (6, 2), A_5 = (5, -1), A_4 = (4, 0), A_1 = (1, 2), A_0 = (0, 7)$ and the other A_i's are all equal to the point $(0, +\infty)$. Therefore, we get the following contruction for f :

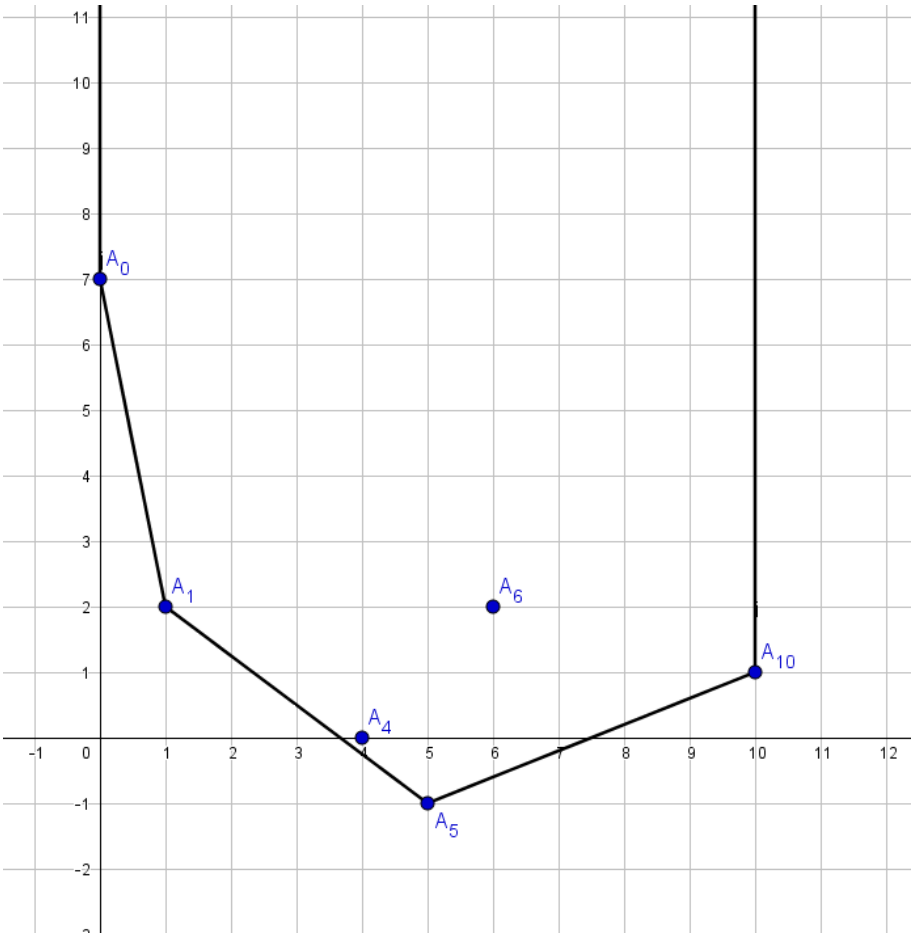


Figure 5: Newton polygon of $f = 5X^{10} + 5^2X^6 + 5^{-1}X^5 + X^4 + 5^2X + 5^7 \in \mathbf{Q}_5[X]$

Now, if the field (K, ν) is complete, we know that ν extends to any finite extension of K. In particular, if we denote by L the splitting field of f over K (in some fixed algebraic closure), then L is a finite extension, and we can wonder if there is a link between the valuations of the coefficients of f and the valuations of its roots in (L, ν_L). Newton polygons provide a very visual way to answer this question. I have learned the following theorem from [Dw].

Theorem 7.3. *Let K be a complete field with respect to a discrete valuation ν, and let $f \in K[X]$. Then to each finite side of the Newton polygon of f there corresponds at least one root of f. The number (counting multiplicities) of roots corresponding to a given side is equal to the length of the projection of that side on the x-axis, and all roots α corresponding to the same side have valuation $\nu_L(\alpha) = -\lambda$ where λ is the slope of the side. If*

$$f_\lambda = \prod_{f(\alpha)=0,\ \nu_L(\alpha)=-\lambda} (X - \alpha)$$

Then $f_\lambda \in K[X]$.

Proof. First, let us prove the last statement. Assume f has degree n, and write $\alpha_1, \ldots, \alpha_n$ its roots counted with multiplicity. Let us denote by L the splitting field of f over K, namely $L = K(\alpha_1, \ldots, \alpha_n)$.

First, we assume that L/K is Galois. Note that since L is the splitting field of f, L/K is normal, so if K is a perfect field, L/K is Galois. This holds for instance if K has characteristic zero. Then for any $\sigma \in Gal(L/K)$, we have already seen that σ preserves valuations (just because $\nu_L \circ \sigma$ is also a valuation on L extending ν, so by the uniqueness in theorem 2.21, it must be equal to ν_L). Thus, if we denote by R_λ the set of roots of f with valuation $-\lambda$, one has : $\sigma(R_\lambda) \subset R_\lambda$, and since σ is injective, and R_λ is a finite set, $\sigma(R_\lambda) = R_\lambda$. But R_λ is exactly the set of roots of f_λ, so the coefficients of f_λ are fixed by the action of $Gal(L/K)$ (because they are symmetric functions of the roots, and the set R_λ is globally fixed by σ, for any σ in $Gal(L/K)$). Therefore, they must lie in K, hence $f_\lambda \in K[X]$.

Now, if K has characteristic $p > 0$, L/K may not be Galois. However, if f is irreducible, then all the roots of f have same valuation, so that $f_\lambda = f \in K[X]$ for a unique λ. Why do they all have same valuation ? If f is separable, then L/K is Galois, and the Galois group acts transitively on the roots of f, and preserves valuations, so the roots must have the same valuation. Otherwise, f is not separable, and so it must be of the form $f = g(X^{p^k})$ with $g \in K[X]$ an irreducible separable polynomial (thanks to lemma 7.1). Thus, if we denote by $Z(g)$ and $Z(f)$ their respective sets of roots, then $Z(g) = Z(f)^{p^k}$, hence :

$$\nu_L(Z(f)) = \frac{1}{p^k}\nu_L(Z(g))$$

Since g is separable, $\nu_L(Z(g))$ consists of only one element, so $\nu_L(Z(f))$ is also reduced to one element.

Finally, if f is reducible, we proceed by induction on n. If f is reducible of degree 2, then its roots are in K, so the statement is clearly satisfied. Now let $n \geqslant 3$, and assume that the statement is true for all $k < n$. Let $h \in K[X]$ be the minimal polynomial of α_1 over K. Then $h|f$. Let $g \in K[X]$ such that $f = gh$, and set :

$$g_\lambda = \prod_{g(\alpha)=0,\ \nu_L(\alpha)=-\lambda} (X - \lambda) = -\lambda$$

Then by the induction hypothesis, g_λ lies in $K[X]$ for every λ (by convention, a product over the empty set is equal to 1). Let $\lambda_1 := -\nu_L(\alpha_1)$. By the above case, since h is irreducible, all the roots of h have valuation $-\lambda_1$. Therefore,

$$\begin{cases} \forall \lambda \neq \lambda_1,\ f_\lambda(X) = g_\lambda(X) \\ f_{\lambda_1}(X) = h(X) g_{\lambda_1}(X) \end{cases}$$

which shows that in any case $f_\lambda \in K[X]$.

Now, let us prove the first assertion of the theorem. It is not restrictive to assume that $a_0 = 1$, for multiplying f by X or a non zero constant has the effect of a translation on the Newton polygon of f. Assuming this, we write :

$$f = \prod_{i=1}^{n} (1 + \beta_i X) = 1 + a_1 X + \cdots + a_n X^n \tag{12}$$

and suppose that $\nu_L(\beta_1) \leqslant \cdots \leqslant \nu_L(\beta_n)$ where ν_L is the unique extension of ν to L : the splitting field of f over K. Suppose that $\{\nu_L(\beta_1), \ldots, \nu_L(\beta_n)\} = \{\nu_1, \ldots, \nu_l\}$ with $\nu_1 < \cdots < \nu_l$. We denote by k_i the

number of β_i's with valuation ν_i so that :

$$\begin{cases} \nu_L(\beta_1) = \cdots = \nu_L(\beta_{k_1}) = \nu_1 \\ \nu_L(\beta_{k_1+1}) = \cdots = \nu_L(\beta_{k_1+k_2}) = \nu_2 \\ \quad \vdots \\ \nu_L(\beta_{k_1+\cdots+k_{l-1}+1}) = \cdots = \nu_L(\underbrace{\beta_{k_1+\cdots+k_l}}_{=\beta_n}) = \nu_l \end{cases}$$

We want to prove that the Newton polygon of f has exactly l finite (i.e. non vertical) sides, say $P_0P_1, \ldots, P_{l-1}P_l$, such that the projection of $P_{i-1}P_i$ on the x-axis has length k_i and that the side $P_{i-1}P_i$ has slope ν_i. This is equivalent to proving that :

$$\forall 1 \leqslant p \leqslant l,\ \nu_L(a_{k_1+\ldots k_p}) = \sum_{i=1}^{p} \nu_i k_i \quad \text{and :} \tag{13}$$

$$\forall 1 \leqslant p \leqslant l,\ \forall \sum_{i=1}^{p-1} k_i < s < \sum_{i=1}^{p} k_i,\ \nu_L(a_s) \geqslant \sum_{i=1}^{p-1} \nu_i k_i + \left(s - \sum_{i=1}^{p-1} k_i \right) \nu_p \tag{14}$$

with the usual convention that a sum from 1 to 0 is equal to zero. Indeed, the first condition just tells that :

$$\begin{gathered} P_0 = (0,0) \text{ because we assumed } a_0 = 0 \\ P_1 = (k_1, \nu_1 k_1), \\ P_2 = (k_1 + k_2, \nu_1 k_1 + \nu_2 k_2) \\ \vdots \\ P_l = (\underbrace{k_1 + \cdots + k_l}_{=n}, \nu_1 k_1 + \cdots + \nu_l k_l) \end{gathered}$$

which are the necessary positions of the points P_i for the statement to hold, and the second assertion says that if s is between $k_1 + \cdots + k_{p-1}$ and $k_1 + \cdots + k_p$, then the point $(s, \nu(a_s))$ lies above the side $P_{p-1}P_p$. The formula may seem obscure, but it is just writing the equation of the line passing through P_{p-1} and P_p and expressing the fact of being above this line.
Now, from (12) it is easy to see that :

$$a_s = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_s \leqslant n} \beta_{i_1} \ldots \beta_{i_s}$$

Hence :

$$\nu(a_s) \geqslant \min_{1 \leqslant i_1 < i_2 < \cdots < i_s \leqslant n} \{\nu_L(\beta_{i_1}) + \cdots + \nu_L(\beta_{i_s})\} \tag{15}$$

Recalling the ordering of the valuations, we find that this minimum is $\nu_L(\beta_1) + \cdots + \nu_L(\beta_s)$ Thus,

$$\nu(a_s) \geqslant \nu_L(\beta_1) + \cdots + \nu_L(\beta_s)$$

which is the same as (14), just by definition of $\nu_1, \ldots, \nu_l$ and of the numbers k_i. Moreover, if $s = k_1 + \cdots + k_p$ for some $1 \leqslant p \leqslant l$, then $\nu_L(\beta_{s+1}) > \nu_L(\beta_s)$ and so (15) must be an equality, hence :

$$\nu(a_s) = \nu_L(\beta_1) + \cdots + \nu_L(\beta_s) = k_1\nu_1 + \cdots + k_p\nu_p$$

which is (13).

□

Corollary 7.4. *Let K be as above and $f \in K[X]$ monic of degree n. If the Newton polygon of f consists of only one finite side of slope $-m/n$, with m relatively prime to n, then f is irreducible in $K[X]$.*

Proof. Under these assumptions, the theorem above tells us that all the roots of f have valuation m/n (for the valuation ν_L extending ν to L : the splitting field of f over K). Let α be one of the roots. Let us prove that the ramification index of $K(\alpha)/K$ is divisible by n. ν_L is a valuation on $K(\alpha)$ extending ν, so by the uniqueness of such a valuation, it is $\nu_{K(\alpha)}$.
Let us denote by e the ramification index of the extension $K(\alpha)/K$, so that :

$$\nu_L(K(\alpha)) = \frac{1}{e}\mathbf{Z}$$

(We are still implicitly assuming that ν is normalized, for it not restrictive at all)
Then $\nu_L(\alpha) \in \nu_L(K(\alpha))$, hence :

$$\frac{m}{n} \in \frac{1}{e}\mathbf{Z}$$

Therefore, $n \mid em$, and since m and n are relatively prime, this implies that n divides e. But we also know that $e \mid [K(\alpha) : K]$ from proposition 3.1. Hence $n \mid [K(\alpha) : K]$. But α is a root of f which is of degree n, so the minimal polynomial of α over K has degree smaller than n, and its degree is $[K(\alpha) : K]$. Therefore, $n \mid [K(\alpha) : K] \leqslant n$, so $n = [K(\alpha) : K]$ and f is the minimal polynomial of α. In particular, f is irreducible.

□

7.2 Projective limits

Let $G = (I, A, s, t)$ be an oriented graph : I is a set (the set of vertices), A is another set (the set of edges), s and t are two maps :

$$\textit{source } s : A \to I \text{ and } \textit{target } t : A \to I$$

An inverse system of groups (resp. rings) indexed by G is the datum :

(1) For any $i \in I$, a group (resp. ring) A_i

(2) For any $a \in A$, a group (resp.ring) homomorphism $\phi_a : A_{s(a)} \to A_{t(a)}$

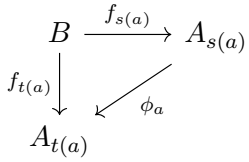
We define the projective limit $\varprojlim_{i \in I} A_i$ as :

$$\varprojlim_{i \in I} A_i := \{(a_i)_{i \in I} \mid \forall i \in I, a_i \in A_i \text{ and } \forall a \in A, \phi_a\left(a_{s(a)}\right) = a_{t(a)}\}$$

- $\varprojlim_{i \in I} A_i$ is a subgroup (resp. subring) of $\prod_{i \in I} A_i$.

- It satisfies the following universal property :

  For any group (resp. ring) B, the datum of a homomorphism $f : B \to \varprojlim_{i \in I} A_i$ is equivalent to the datum of homomorphisms $f_i : B \to A_i$ such that for all $a \in A$, the following diagram commutes :



Examples :

- Let $p \in \mathbf{N}$ be a prime number. We define the ring of p-adic integers (denoted by $\mathbf{Z}_p$) as the projective limit of the rings $\mathbf{Z}/p^n\mathbf{Z}$ as follows :

  Formally, we take $G = (I, A, s, t)$ in the construction above with :

  $$I = \mathbf{N}^*,\ A = \mathbf{N}^*,\ s : n \mapsto n+1 \text{ and } t : n \mapsto n$$

  For all $i \in I$, we take the ring A_i to be $\mathbf{Z}/p^i\mathbf{Z}$. For all $a \in A$, we have a natural ring homomorphism :

  $$\begin{array}{rccc} \phi_a & : & \mathbf{Z}/p^{a+1}\mathbf{Z} & \to & \mathbf{Z}/p^a\mathbf{Z} \\ & & k \bmod p^{a+1} & \mapsto & k \bmod p^a \end{array}$$

  This gives us an inverse system of rings in the sense of the definition above, so we can define the ring :

  $$\mathbf{Z}_p := \varprojlim_{n \geqslant 1} \mathbf{Z}/p^n\mathbf{Z}$$

- Likewise, we would like to define a new ring as the projective limit of all the rings $\mathbf{Z}/n\mathbf{Z}$, for all $n \geqslant 2$. The difference with the preceding example is that this time, we cannot define a natural ring homomorphism from $\mathbf{Z}/n\mathbf{Z}$ to $\mathbf{Z}/m\mathbf{Z}$ for all $m \leqslant n$. This is only the case when $n\mathbf{Z} \subset m\mathbf{Z}$, i.e. when $m \mid n$. This is why we take $G = (I, A, s, t)$ with :

  $$I = \mathbf{N}_{>1},\ A = \{(n, m) \in \mathbf{N}_{>1}^2 \mid m \text{ divides } n\},\ s : (n, m) \mapsto n,\ t : (n, m) \mapsto m$$

  where $\mathbf{N}_{>1}$ denotes the set of natural integers > 1. Then, for all $i \in I$, we set $A_i := \mathbf{Z}/i\mathbf{Z}$. For all $a = (n, m) \in A$, we have a natural ring homomorphism :

  $$\begin{array}{rccc} \phi_a & : & A_{s(a)} & \to & A_{t(a)} \\ & & k \bmod n & \mapsto & k \bmod m \end{array}$$

  Therefore, we have defined an inverse system of rings indexed by $G = (I, A, s, t)$, and we can define the ring :

  $$\widehat{\mathbf{Z}} := \varprojlim_{n \geqslant 2} \mathbf{Z}/n\mathbf{Z}$$

  As a group, $\widehat{\mathbf{Z}}$ plays an important role in number theory because if $\overline{\mathbf{F}_q}$ denotes an algebraic closure of a finite field of order q, then $Gal(\overline{\mathbf{F}_q}/\mathbf{F}_q) \simeq \widehat{\mathbf{Z}}$

Remark : It is a nice exercice to prove there is a ring isomorphism :

$$\widehat{\mathbf{Z}} \simeq \prod_{p \text{ prime}} \mathbf{Z}_p$$

It is a good way to get used to the notion of projective limit, its universal property, and it also involves the Chinese remainder theorem, which is always good to remember.

7.3 Proof of proposition 4.2

(*i*) Let α be a root of f. Since f is irreducible, f is the minimal polynomial of α over K. Hence : $[K(\alpha) : K] = \deg(f) = n$. Besides, $K \subset K(\alpha) \subset L$, because L is the splitting field of f over K. Therefore, $[K(\alpha) : K]$ divides $[L : K] = \#Gal(L/K) = \#G$. Thus,

$$n \mid \#G$$

(*ii*) Let us explain more precisely what we mean when we say that G is a transitive subgroup of $\mathfrak{S}_n$. As we saw, there is an embedding $\varphi : G \hookrightarrow \mathfrak{S}_n$. Therefore, $\varphi(G)$ is a subgroup of $\mathfrak{S}_n$, so it acts on $\{1, \dots, n\}$, and we say that this subgroup is transitive when there is only one orbit in $\{1, \dots, n\}$ under the action of $\varphi(G)$. This means that for any two roots of f, say α_i and α_j, there exists $\sigma \in G$ such that $\sigma(\alpha_i) = \alpha_j$.

Now, let us prove that f is irreducible if and only if G is a transitive subgroup of $\mathfrak{S}_n$. We denote by $\mathcal{C}_1, \dots, \mathcal{C}_m$ the orbits of $\{\alpha_1, \dots, \alpha_n\}$ under the action of G. Then :

$$f = \prod_{i=1}^{n} (X - \alpha_i) = \prod_{k=1}^{m} \underbrace{\prod_{\alpha \in \mathcal{C}_k} (X - \alpha)}_{:= f_k}$$

Let $k \in \{1, \dots, m\}$. Let us prove that f_k is in $K[X]$, and that it is irreducible.

First, if one takes $\sigma \in G$, then σ induces a permutation of $\mathcal{C}_k$. Indeed, if $\alpha \in \mathcal{C}_k$, then :

$$\mathcal{C}_k = \{\tau(\alpha),\ \tau \in G\} \text{ (by definition)}$$

so that $\sigma(\alpha) \in \mathcal{C}_k$. Therefore, $\sigma(\mathcal{C}_k) \subset \mathcal{C}_k$, and since σ is injective and $\mathcal{C}_k$ is finite, we have : $\sigma(\mathcal{C}_k) = \mathcal{C}_k$. Therefore, $\mathcal{C}_k$ is globally fixed by the action of σ, for all $\sigma \in G = Gal(L/K)$. Since the coefficients of f_k are symmetric polynomials in the elements of $\mathcal{C}_k$, they are fixed by $Gal(L/K)$, so they are in K. Thus, $f_k \in K[X]$.

Now, let $g \in K[X]$ be an irreducible monic factor of f_k in $K[X]$. Let α be a root of g (in particular, $\alpha \in \mathcal{C}_k$) and let β be any root of f_k. Then since G acts transitively on $\mathcal{C}_k$, there exists $\sigma \in G$ such that $\sigma(\alpha) = \beta$. Then :

$$g(\beta) = g(\sigma(\alpha)) = \sigma(g(\alpha)) = \sigma(0) = 0$$

Thus, any root of f_k is a root of g, so $f_k \mid g$. Therefore, $g = f_k$ and f_k is irreducible in $K[X]$.

So the decomposition :

$$f = \prod_{k=1}^{m} f_k$$

is the decomposition of f into irreducible factors in $K[X]$. Hence :

$$f \text{ is irreducible } \iff m = 1 \iff G \text{ is a transitive subgroup of } \mathfrak{S}_n$$

7.4 Local class field theory

This section contains a corollary of the main theorem of local class field theory, that will be useful in our attempt to classify $\mathfrak{S}_3$-extensions of $\mathbf{Q}_3$ in section 7.6. I attended the *Algebraic Number Theory 2* class by Mr. Heinloth at the University in Essen, where we studied the proof in detail. However, including the proof would require another long report, and I acknowledge that I need more time to understand it completely. It involves a lot of interesting tools, such as Lubin-Tate formal group laws, group homology, group cohomology, and Tate's cohomology to put these two together for a finite group. During this class, we mostly followed the notes from [Mi] on Class field theory. However, there are many references, for instance [Yo] : an article proving local class field theory using Lubin-Tate formal groups laws, or [Ne], Chapter V.

Let K be a field. We say that a finite extension L/K is abelian if it is Galois with an abelian Galois group. Local class field theory brings back the study of the abelian extensions of a local field to the study of subgroups of $K^\times$:

Theorem 7.5. *Let K be a local field of characteristic 0. Then, the rule :*

$$L \mapsto \mathcal{N}_L := Nm_{L/K}(L^\times)$$

gives a 1 to 1 correspondence between finite abelian extensions of K and subgroups of finite index in $K^\times$. If L/K is finite abelian, then there is an isomorphism :

$$K^\times/Nm_{L/K}(L^\times) \simeq Gal(L/K)$$

In particular, subgroups of index n correspond to extensions of degree n.

This theorem falls within the following beautiful summary of what Class field theory is about (although Chevalley refers to global fields more than local fields here) :

"L'objet de la théorie du corps de classes est de montrer comment les extensions abéliennes d'un corps de nombres algébriques K peuvent être déterminées par des éléments tirés de la connaissance de K lui-même; ou, si l'on veut présenter les choses en termes dialectiques, comment un corps possède en soi les éléments de son propre dépassement" CHEVALLEY, 1940

Remark : The assumption *"of characteristic zero"* in theorem 7.5 is here to avoid a discussion on topology. Indeed, the correspondence also works when K does not have characteristic 0, but it is between finite abelian extensions and *open* subgroups of finite index in $K^\times$, with respect to the *norm topology* on $K^\times$. In characteristic zero, subgroups of finite index in $K^\times$ are automatically open, so the statement is simplified. Since we are only concerned with $\mathbf{Q}_p$ and its extensions, we can reduce the statement to local fields of characteristic zero.

7.5 Structure of $K^\times$ when K is a finite extension of $\mathbf{Q}_p$

Let $K/\mathbf{Q}_p$ be a finite extension of degree n. We fix a uniformizer π in K. Since every element $x \in K^\times$ can be written uniquely $x = u.\pi^m$, with $m \in \mathbf{Z}$ and $u \in \mathcal{O}_K^\times$, we have an isomorphism :

$$K^\times \simeq \mathbf{Z} \times \mathcal{O}_K^\times$$

Moreover, we have an exact sequence :

$$1 \longrightarrow 1 + (\pi) \longrightarrow \mathcal{O}_K^\times \longrightarrow \mathbf{F}_q^\times \longrightarrow 1$$

where $q = p^f$, with f denoting the inertia degree of $K/\mathbf{Q}_p$. Using Hensel's lemma, one proves that this exacts sequence of abelian groups splits, hence :

$$\mathcal{O}_K^\times \simeq \mathbf{F}_q^\times \times (1 + \mathfrak{p}_K)$$

Therefore,

$$K^\times \simeq \mathbf{Z} \times \mathbf{Z}/(q-1)\mathbf{Z} \times (1 + \mathfrak{p}_K)$$

Now, we want to understand the group $(1 + \mathfrak{p}_K) = U_K^{(1)}$ (this notation has been introduced in section 3.4, equation (8)). This group can be endowed with a $\mathbf{Z}_p$-module structure, as it is done in [Ne], Chapter II, §5, and it happens to be finitely generated as a $\mathbf{Z}_p$-module. Therefore, by the structure theorem for finitely generated modules over a principal ideal domain :

$$U_K^{(1)} \simeq \mathbf{Z}_p^r \times \mathrm{Tor}_{\mathbf{Z}_p}\left(U_K^{(1)}\right)$$

where r is the rank of $U_K^{(1)}$ as a $\mathbf{Z}_p$-module. Besides,

$$\mathrm{Tor}_{\mathbf{Z}_p}\left(U_K^{(1)}\right) = \{a \in U_K^{(1)} \mid \exists m \in \mathbf{Z},\ a^{p^m} = 1\} := \mu_{p^\infty}(K)$$

This torsion submodule is isomorphic, as a group, to $\mathbf{Z}/p^m\mathbf{Z}$, for some $m \in \mathbf{N}$. Thus :

$$K^\times \simeq \mathbf{Z} \times \mathbf{Z}/(q-1)\mathbf{Z} \times \mathbf{Z}/p^m\mathbf{Z} \times \mathbf{Z}_p^r$$

It remains to determine the rank r of the free part of the $\mathbf{Z}_p$-module $U_K^{(1)} = 1 + \mathfrak{p}_K$.

Proposition 7.6. *We denote by e the ramification index of $K/\mathbf{Q}_p$. For all $m > \frac{e}{p-1}$,*

$$(1 + \mathfrak{p}_K^m)^p = 1 + \mathfrak{p}_K^{m+e}$$

where $(1 + \mathfrak{p}_K^m)^p$ denotes $\{x^p,\ x \in U_K^{(m)}\}$

Proof. Let $m > \frac{e}{p-1}$. We denote by ν_K the unique valuation on K extending the standard valuation on $\mathbf{Q}_p$. Then we normalize this discrete valuation to get a valuation ν on K. This valuation satisfies $\nu(p) = e$ and $\nu(\pi) = 1$. Let us prove the first inclusion :

$\boxed{\subset}$: Let $a \in \mathfrak{p}_K^m = (\pi)^m$. We write $a = \pi^m b$, where $b \in \mathcal{O}_K$. We want to prove :

$$(1 + a)^p \in 1 + \mathfrak{p}_K^{m+e}$$

We have :

$$(1 + a)^p = \sum_{k=0}^{p} \binom{p}{k} a^k = 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k + a^p$$

Besides,

$$\forall 1 \leqslant k \leqslant p-1,\ \nu\left(\binom{p}{k} a^k\right) = \nu\left(\binom{p}{k}\right) + k.\nu(a) = e + k\nu(\pi^m b) = e + k(m + \nu(b))$$

so that :

$$\forall 1 \leqslant k \leqslant p-1,\ \nu\left(\binom{p}{k} a^k\right) \geqslant m + e$$

This implies that :

$$\nu\left(\sum_{k=1}^{p-1}\binom{p}{k}a^k\right) \geqslant m+e$$

Moreover,

$$\nu(a^p) = p.\nu(\pi^m b) = p(m+\nu(b)) \geqslant mp$$

and :

$$m > \frac{e}{p-1} \implies m \geqslant \frac{e}{p-1} \implies mp \geqslant m+e$$

hence $\nu(a^p) \geqslant m+e$. Thus,

$$\nu\left(\sum_{k=1}^{p-1}\binom{p}{k}a^k + a^p\right) \geqslant m+e \quad \text{i.e.} \quad (1+a)^p \in U_K^{(m+e)}$$

$\boxed{\supset}$ Let $a \in \mathfrak{p}_K^{m+e}$, say $a = b\pi^{m+e}$, with $b \in \mathcal{O}_K$. Let us show that the polynomial $P := (1+X)^p - (1+a)$ has a root in $\mathfrak{p}_K^m$.

We have :

$$P = X^p + \sum_{k=1}^{p-1}\binom{p}{k}X^k - a$$

Since for all $1 \leqslant k \leqslant p-1$, $\nu\left(\binom{p}{k}\right) = e$, and $\nu(a) = \nu(b) + m + e$, the Newton polygon of P looks like this :

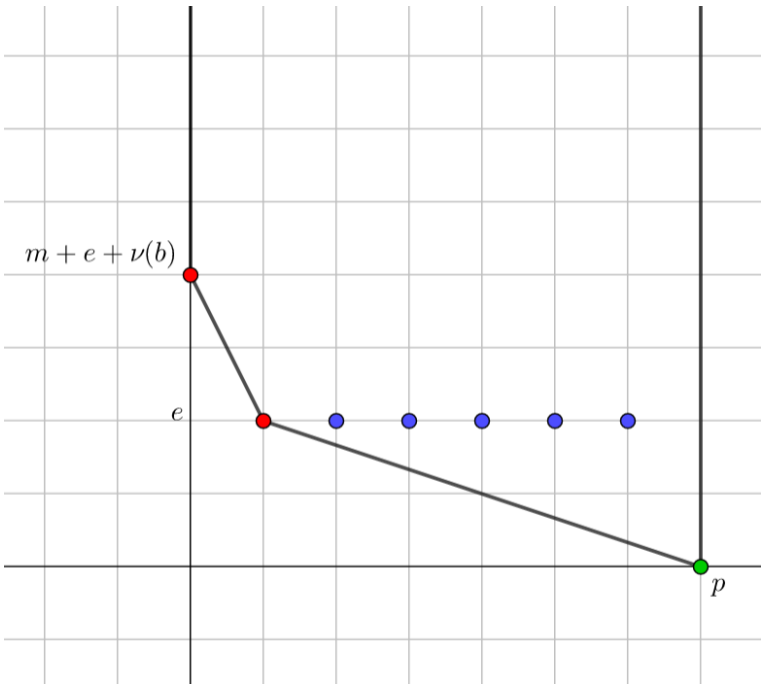


Figure 6: Newton polygon of $P = (1+X)^p - (1+a) \in K[X]$

The equation of the line passing through the two red points is :

$$y = -(m + \nu(b)).x + m + e + \nu(b)$$

so that the green point with coordinates $(p, 0)$ belongs to this line if and only if :

$$(m + \nu(b)).p = m + e + \nu(b) \quad \text{i.e.} \quad m = \frac{e}{p-1} - \underbrace{\nu(b)}_{\geqslant 0}$$

Thus, the assumption $m > \frac{e}{p-1}$ ensures that the green point is not on the first finite side. This implies that the Newton polygon of P has exactly two finite sides. The first side corresponds to a single root, which necessarily lie in K, and which valuation is $m + \nu(b)$. In particular, the root is in $\mathfrak{p}_K^m$, that is what we wanted to prove. □

In particular, the proof shows that if $m > \frac{e}{p-1}$, then for all $x \in U_K^{(m+e)}$, there exists a unique $y \in U_K^{(m)}$ such that $y^p = x$. Indeed, the other side of the Newton polygon of P has slope $-\frac{e}{p-1}$, so all the other roots of P have valuation $\frac{e}{p-1} < m$, so they cannot be in $\mathfrak{p}_K^m$.

Special case : Take $x = 1 \in U_K^{(m+e)}$. Then there exists a unique $y \in U_K^{(m)}$ such that $y^p = 1$. But $y = 1$ clearly works, hence :

$$\forall m > \frac{e}{p-1}, \quad U_K^{(m)} \cap \mu_{p^\infty}(K) = \{1\}$$

Therefore, for m sufficiently large, $U_K^{(m)}$ is torsion free. Thus, there exists $s \in \mathbf{N}$ such that :

$$U_K^{(m)} \simeq \mathbf{Z}_p^s \text{ as } \mathbf{Z}_p\text{-modules}$$

This implies :

$$U_K^{(m)} / \left(U_K^{(m)}\right)^p \simeq \left(\mathbf{Z}/p\mathbf{Z}\right)^s \text{ as groups}$$

Thus,

$$\# \frac{1 + \mathfrak{p}_K^m}{\left(1 + \mathfrak{p}_K^m\right)^p} = p^s \tag{16}$$

But proposition 7.6 allows us to compute the cardinality of this quotient by a filtration. Indeed, since $(1 + \mathfrak{p}_K^m)^p = U_K^{(m+e)}$, we can compute as follows :

$$\# \frac{1 + \mathfrak{p}_K^m}{\left(1 + \mathfrak{p}_K^m\right)^p} = \# \frac{U_K^{(m)}}{U_K^{(m+e)}} = \prod_{i=0}^{e-1} \# \frac{U_K^{(m+i)}}{U_K^{(m+i+1)}}$$

By proposition 3.17, we know that each quotient :

$$\frac{U_K^{(m+i)}}{U_K^{(m+i+1)}}$$

is isomorphic to $(\kappa_K, +)$, so it has $q = p^f$ elements. Therefore,

$$\# \frac{1 + \mathfrak{p}_K^m}{\left(1 + \mathfrak{p}_K^m\right)^p} = \prod_{i=0}^{e-1} \# \frac{U_K^{(m+i)}}{U_K^{(m+i+1)}} = \prod_{i=0}^{e-1} p^f = p^{ef} \tag{17}$$

Thanks to proposition 3.1, we also have : $ef = [K : \mathbf{Q}_p] = n$. Finally, (16) and (17) implie : $s = n$.

Conclusion :

$$\text{If } m > \frac{e}{p-1}, \text{ then } U_K^{(m)} \text{ is a free } \mathbf{Z}_p\text{-module of rank } n$$

Now, the quotient $U_K^{(1)}/U_K^{(m)}$ is finite, because once again, we can compute its cardinality using a filtration. Therefore, $U_K^{(m)}$ is a submodule of $U_K^{(1)}$ of finite index ! Thus, the rank of their free component must be the same, hence :

$$U_K^{(1)} = 1 + \mathfrak{p}_K \simeq \mu_{p^\infty}(K) \times \mathbf{Z}_p^n$$

We can summarize what we did in the following theorem :

Theorem 7.7. *Let $K/\mathbf{Q}_p$ be a finite extension of degree n, with ramification index e, inertia degree f, and residue field of order $q = p^f$. Then :*

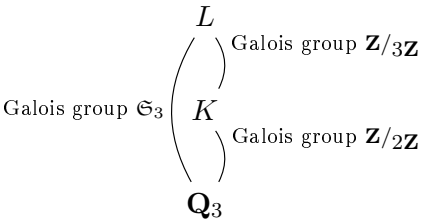
$$K^\times \simeq \mathbf{Z} \times \mathcal{O}_K^\times \simeq \mathbf{Z} \times \mathbf{Z}/(q-1)\mathbf{Z} \times U_K^{(1)} \simeq \mathbf{Z} \times \mathbf{Z}/(q-1)\mathbf{Z} \times \mu_{p^\infty}(K) \times \mathbf{Z}_p^n$$

Besides, $\mu_{p^\infty}(K) \simeq \mathbf{Z}/p^a\mathbf{Z}$ for some $a \in \mathbf{N}$, hence :

$$K^\times \simeq \mathbf{Z} \times \mathbf{Z}/(q-1)\mathbf{Z} \times \mathbf{Z}/p^a\mathbf{Z} \times \mathbf{Z}_p^n$$

7.6 Attempt to classify $\mathfrak{S}_3$-extensions of $\mathbf{Q}_3$

Suppose $L/\mathbf{Q}_3$ is a finite Galois extension with $G := Gal(L/\mathbf{Q}_3) \simeq \mathfrak{S}_3$. Let H be the subgroup of G corresponding to $\mathfrak{A}_3$ under the identification "$G = \mathfrak{S}_3$". Then $H \triangleleft G$, so that $L^H/\mathbf{Q}_3$ is Galois. Let us denote L^H by K. We have :



Therefore, $L/\mathbf{Q}_3$ is formed by a Galois extension of degree 2, hence abelian, followed by a Galois extension of degree 3, also automatically abelian. Since class field theory's aim is to classify abelian extensions, it is not surprising that it helps us in this problem. Namely, it gives us the following result :

Proposition 7.8. *Let $K/\mathbf{Q}_p$ be a finite extension of degree n. Then the number of abelian extensions L/K of degree p is given by :*

$$\frac{p^d - 1}{p - 1}$$

with $d = n + 2$ if K contains a pth root of 1, and $d = n + 1$ otherwise.

Proof. By theorem 7.5, the abelian extensions L/K with degree p correspond to subgroups of index p in $K^\times$. It is not hard to see that if H is a subgroup of index p in $K^\times$, then : $(K^\times)^p \subset H \subset K^\times$.

Now, subgroups of $K^\times$ containing the subgroup $(K^\times)^p$ correspond one to one to subgroups of the quotient $K^\times/(K^\times)^p$, and this correspondence preserves the index. Therefore, the number of abelian extensions of K of degree p is equal to the number of subgroups of index p in $K^\times/(K^\times)^p$.

By theorem 7.7 :

$$K^\times \simeq \mathbf{Z} \times \mathbf{Z}/(q-1)\mathbf{Z} \times \mathbf{Z}/p^a\mathbf{Z} \times \mathbf{Z}_p^n$$

with $a = 0$ if $K \cap \mu_{p^\infty}(K) = \{1\}$ (i.e. if K does not contains p power roots of 1), and $a > 0$ otherwise.

Thus :

$$K^\times/(K^\times)^p \simeq \frac{\mathbf{Z}}{p\mathbf{Z}} \times \underbrace{\frac{\mathbf{Z}/(q-1)\mathbf{Z}}{p\left(\mathbf{Z}/(q-1)\mathbf{Z}\right)}}_{:=A} \times \underbrace{\frac{\mathbf{Z}/p^a\mathbf{Z}}{p\left(\mathbf{Z}/p^a\mathbf{Z}\right)}}_{:=B} \times \underbrace{\frac{\mathbf{Z}_p^n}{p\mathbf{Z}_p^n}}_{:=C}$$

And :

$$A \simeq \{1\} \text{ because } (q-1) \text{ is prime to } p$$

$$B \simeq \begin{cases} \mathbf{Z}/p\mathbf{Z} \text{ if } a > 0 \\ \{1\} \text{ else} \end{cases}$$

$$C \simeq \left(\mathbf{Z}_p/p\mathbf{Z}_p\right)^n \simeq \left(\mathbf{Z}/p\mathbf{Z}\right)^n$$

Therefore,

$$K^\times/(K^\times)^p \simeq \mathbf{F}_p^d \text{ with } d = \begin{cases} n+1 \text{ if } K \cap \mu_{p^\infty}(K) = \{1\} \\ n+2 \text{ else} \end{cases}$$

Subgroups of index p in $K^\times/(K^\times)^p$ correspond to subspaces of codimension 1 in a $\mathbf{F}_p$ vector space of dimension d. But if we dualize, it suffices to count the number of 1-dimensional subspaces of $\mathbf{F}_p^d$, and there are $(p^d-1)/(p-1)$ such subspaces (number of non-zero vectors / number of non-zero scalars). Hence the conclusion. □

Using this, we can make a little progress. Indeed, we know that there are exactly three quadratic extensions of $\mathbf{Q}_3$ (see section 6.1) :

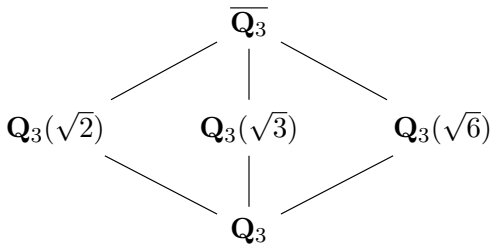


Figure 7: The three quadratic extensions of $\mathbf{Q}_3$

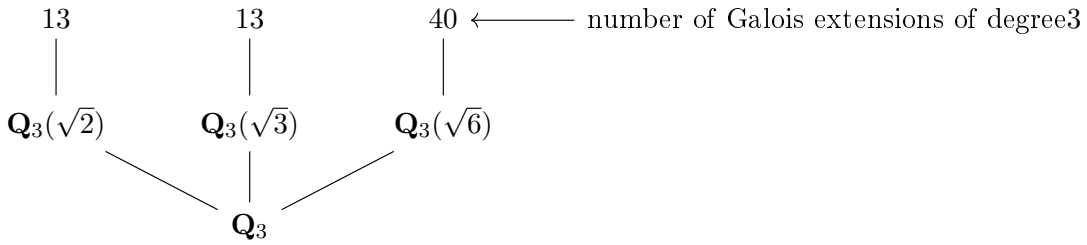
Therefore, if $L/\mathbf{Q}_3$ is a $\mathfrak{S}_3$-extension, then the subextension K introduced above is one of these 3 quadratic extensions of $\mathbf{Q}_3$. Moreover, K is a finite extension of $\mathbf{Q}_3$, and L/K is an extension of degree 3, so proposition 7.8 applies ! Since :

$$\frac{3^{2+1}-1}{3-1} = 13 \quad \text{and} \quad \frac{3^{3+1}-1}{3-1} = 40,$$

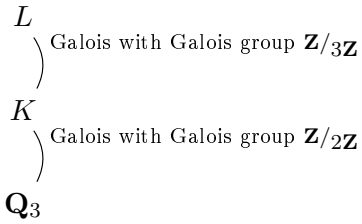
There are 13 or 40 possible extensions L/K that are Galois of degree 3, depending on whether or not K contains the third roots of unity. But as we have already seen, $\mu_3 \subset K$ if and only if $X^3 - 1$ splits in K,

if and only if $disc(X^2+X+1) \in (K^\times)^2$. This discriminant equals -3, and it is easy to prove that it is a square in a quadratic extension of $\mathbf{Q}_3$ if and only if this extension is $\mathbf{Q}_3(\sqrt{6})$.

Thus :



This gives us that there are at most $13+13+40 = 66$ extensions of $\mathbf{Q}_3$ with Galois group $\mathfrak{S}_3$. However, this bound is very likely to be too large. Indeed, 66 is the number of distinct towers of extensions of the form :



But such towers do not always give $L/\mathbf{Q}_3$ Galois, and even if it is the case, we are not sure that the Galois group is isomorphic to $\mathfrak{S}_3$... This is confirmed by [LMFDB].

We need to find a way to translate the fact that $L/\mathbf{Q}_3$ is not just any quadratic extension $K/\mathbf{Q}_3$ followed by any degree 3 Galois extension L/K. We need to express that when we paste this two extensions, the big extension we obtain, namely $L/\mathbf{Q}_3$, is still Galois.

Besides, we need to take into account is that $\mathfrak{S}_3$ is a semi direct product :

$$\mathfrak{S}_3 \simeq \mathbf{Z}/_{3\mathbf{Z}} \rtimes_\varphi \mathbf{Z}/_{2\mathbf{Z}}$$

where $\varphi : \mathbf{Z}/_{2\mathbf{Z}} \to \mathrm{Aut}(\mathbf{Z}/_{3\mathbf{Z}})$ maps 0 to id and 1 to $-id$.

Or as an inner semi-direct product : $\mathfrak{S}_3 \simeq N \rtimes H$ if we denote $N := \langle (1\ 2\ 3) \rangle$ $(= \mathfrak{A}_3)$ and $H := \langle (1\ 2) \rangle$.

Therefore, if $L/\mathbf{Q}_3$ is a $\mathfrak{S}_3$ extension, and if K is as above, we can expect the following : Since in the tower $\mathbf{Q}_3 \subset K \subset L$, $Gal(L/K)$ is identified with $\mathfrak{A}_3$, we expect some group of order 2 to act on $Gal(L/K)$. The problem is that $Gal(K/\mathbf{Q}_3)$ does not naturally act on $Gal(L/K)$.

However, let us introduce $K^{ab}[3]$: the composite of all abelian extensions of degree 3 of K. Recall that if E/K and F/K are finite Galois, then EF/K is Galois, and $Gal(EF/K)$ embeds in $Gal(E/K) \times Gal(F/K)$. In particular the compositum of two finite abelian extension is also finite abelian. By proposition 7.8, we know there are only finitely many such extensions, so $K^{ab}[3]/K$ is finite abelian as a compositum of finitely many finite abelian extensions.

It is not hard to show that $K^{ab}[3]/\mathbf{Q}_3$ is also Galois. Thus $Gal(K^{ab}[3]/K)$ is a subgroup of $Gal(K^{ab}[3]/\mathbf{Q}_3)$. Since $K/\mathbf{Q}_3$ is Galois, this subgroup is normal. Therefore, $Gal(K^{ab}[3]/\mathbf{Q}_3)$ acts on $Gal(K^{ab}[3]/K)$ via conjugation. But if $\sigma, \tau \in Gal(K^{ab}[3]/\mathbf{Q}_3)$ are such that $\sigma_{|K} = \tau_{|K}$, then their action is the same. Indeed, consider :

$$\begin{array}{rccc} \phi & : & Gal(K^{ab}[3]/\mathbf{Q}_3) & \to & \mathrm{Aut}\left(Gal(K^{ab}[3]/K)\right) \\ & & \sigma & \mapsto & c_\sigma \end{array}$$

where c_σ denote conjugation by σ, namely :

$$\begin{array}{rccc} c_\sigma & : & Gal(K^{ab}[3]/K) & \to & Gal(K^{ab}[3]/K) \\ & & h & \mapsto & \sigma h \sigma^{-1} \end{array}$$

Then, since $Gal(K^{ab}[3]/K)$ is abelian, it is clear that $Gal(K^{ab}[3]/K) \subset \ker(\phi)$. Now, if $\sigma_{|K} = \tau_{|K}$, then $\sigma\tau^{-1} \in Gal(K^{ab}[3]/K) \subset \ker(\phi)$, hence $c_\sigma = c_\tau$. This defines an action of $Gal(K/\mathbf{Q}_3)$ on $Gal(K^{ab}[3]/K)$: For any $s \in Gal(K/\mathbf{Q}_3)$, take any $\sigma \in Gal(K^{ab}[3]/\mathbf{Q}_3)$ such that $\sigma_{|K} = s$, and define the action of s on $Gal(K^{ab}[3]/K)$ by the conjugation by σ.

Likewise, $Gal(K/\mathbf{Q}_3)$ acts on $Gal(L/K)$: For any $s \in Gal(K/\mathbf{Q}_3)$, take any lift $\tilde{\sigma} \in Gal(L/\mathbf{Q}_3)$ and define the action of s on $Gal(L/K)$ by conjugation by $\tilde{\sigma}$. It is clear that this action is compatible with the restriction homomorphism from $Gal(K^{ab}[3]/K)$ to $Gal(L/K)$: For all $s \in Gal(K/\mathbf{Q}_3)$, for all $\tilde{\sigma} \in Gal(L/\mathbf{Q}_3)$ such that $\tilde{\sigma}_{|K} = s$, for all $\sigma \in Gal(K^{ab}[3]/\mathbf{Q}_3)$ such that $\sigma_{|K} = s$, the following diagram commutes :

$$\begin{array}{ccc} Gal(K^{ab}[3]/K) & \xrightarrow{|L} & Gal(L/K) \\ \downarrow{\scriptstyle c_\sigma} & & \downarrow{\scriptstyle c_{\tilde{\sigma}}} \\ Gal(K^{ab}[3]/K) & \xrightarrow{|L} & Gal(L/K) \end{array}$$

We say that the homomorphism :

$$Gal(K^{ab}[3]/K) \xrightarrow{|L} Gal(L/K)$$

is $Gal(K/\mathbf{Q}_3)$-equivariant.

Besides, one can prove that $Gal(K^{ab}[3]/K) \simeq K^\times/(K^\times)^3$ via local class field theory, so it is a $\mathbf{F}_3$ vector space of dimension 3 if K is $\mathbf{Q}_3(\sqrt{2})$ or $\mathbf{Q}_3(\sqrt{3})$, and of dimension 4 if $K = \mathbf{Q}_3(\sqrt{6})$. Moreover, $Gal(L/K)$ is isomorphic to $\mathbf{Z}/3\mathbf{Z}$. So, with a lot of hand-waving, counting $\mathfrak{S}_3$-extensions of $\mathbf{Q}_3$ is equivalent to counting surjective group homomorphisms $\mathbf{F}_3^d \twoheadrightarrow \mathbf{F}_3$ satisfying some $\mathbf{Z}/2\mathbf{Z}$-equivariance property. This is what I need to understand more clearly to obtain a conclusion.

8 References

- [Co] : Keith Conrad's webpage, http://www.math.uconn.edu/~kconrad/

- [Dw] : Bernard Dwork, Giovanni Gerotto, & Francis J. Sullivan, *An Introduction to G-Functions*, Princeton University Press 1994.

- [Ga] : Notes on Newton polygons available on Paul Garrett's page : http://www-users.math.umn.edu/~garrett/

- [Go] : Ivan Gozard, *Théorie de Galois* 2^e édition, Collection Mathématiques à l'Université, Editions Ellipses.

- [LMFDB] *The L-functions and modular forms database*, which also provides a database of all the field extensions of $\mathbf{Q}_p$ of small degree : http://www.lmfdb.org/

- [Mi] : Course notes by James S. Milne in *Algebraic Number Theory, Class Field Theory*, and *Fields and Galois Theory* have been of great help to me. They are all available on the webpage of the author http://www.jmilne.org/math/index.html

- [Ne] : Jürgen Neukirch, *Algebraic Number Theory*, Springer-Verlag 1999.

- [Ro] : Alain M. Robert, *A Course in p-adic Analysis*, Springer-Verlag 2000.

- [Se] : Jean-Pierre Serre, *Corps locaux*.

- [Su] : Lecture notes by Andrew Sutherland, available at http://math.mit.edu/classes/18.785/2017fa/lectures.html

- [Yo] : Teruyoshi Yoshida, *Local class field theory via Lubin-Tate theory*, https://arxiv.org/abs/math/0606108v2