BACHELOR'S THESIS

Degree in Mathematics

Title: Scholz-Reichardt's Theorem

Author: Alejandro Sáez Coma

Advisor: Jordi Quer Bosor

Department: Mathematics

Academic year: 2017-2018

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Table of content

1 Introduction

Determining whether a quintic polynomial is solvable by radicals and assessing the constructibility of regular polygons by a straightedge and compass are questions Galois theory can answer. Galois theory associates groups to certain algebraic field extensions establishing a correspondence between subgroups and subextensions. In this thesis we examine a particular case of the converse linkage. It is an open problem if every finite group has a corresponding field extension over the rationals, known as Galois' inverse problem. Some cases are known, in the undergraduate's subject on Galois theory we already saw that abelian groups occur as Galois groups over the rationals. In 1937 Arnold Scholz and Hans Reichardt proved that for odd p-groups the answer is affirmative as well. This is the theorem we will prove. As a consequence any nilpotent group of odd order is in fact realizable as a Galois group over the rationals and taking some results for granted we will see that every solvable group has indeed a corresponding field too.

Our approach will strongly rely on the ease with which we can construct composition series of p-groups. We will filter our p-group in a tower with simple cyclic quotients and follow an inductive procedure. At every step we will consider a particular group extension and solve an embedding problem, concepts that will be timely introduced. Not only will we associate a field to the current group but we will also have to guarantee that we can keep doing the same. To ensure the latter, we will impose a condition on the pursued field named after Scholz himself.

As some of the deployed techniques lie beyond the scope of the regular undergraduate's curriculum we have chosen to structure this work as follows. First we introduce a set of preliminary concepts for this thesis to be as self contained as possible. Then a section on the Galois embedding problem is presented due to its relevance in the accomplishment of the proof. With these tools in hand the main body of the thesis arises, the proof of Scholz-Reichardt's theorem. After the proof some remarks and particular examples are provided to better portray the far reaching consequences of the theorem.

Scholz-Reichardt's discovery not only helped the works of succeeding mathematicians but also solved the simplest type of a large family of problems that is today a topic of research and discussion. The solvability of embedding problems with a prescribed kernel.

Before going any further I would like to place on record my deepest sense of gratitude to professor Jordi Quer. Not only for guiding me through the field lattice to finally encounter $\tilde{L}$ but also for the three magnificent subjects I have had the pleasure to have him as a professor for during the bachelor's degree.

2 Contextualization within Galois' inverse problem

It is nowadays customary to teach polynomial arithmetic at a high school level. This widespread habit has its roots in the relevance polynomials play in modern era society rather than on their aesthetic beauty. Justifying the fact that they appear naturally with the two basic operations or that they are the easiest way to enlarge rings or other algebraic structures would be a failed attempt to explain their existence. The notion of what is natural and what is not is highly biased by our backgrounds. One could argue that if someone were raised with no contact with society whatsoever then those constructions would not strike to him as rare. This last assertion is unfortunately just that, an assertion. Going back to our initial concern, we present a brief note on the history of the most related polynomial discoveries and let the reader draw his own conclusions with regards to the "naturality" of it all.

Even if the first instance in which polynomials appeared in literature is not clear we can say that they were the most fashionable topic in 16th century mathematics. In the Italian Renaissance figures like Cardano, Tartaglia and Ferrari were avidly publishing on the topic and participating in root-finding competitions. Some attribute the discovery of the formulae to compute cubic polynomial roots to Niccolò Fontana thanks to a competition held in Bologna in 1535, character who would later be remembered as Tartaglia for a war injury that severely damaged his speaking capacity. Coetaneous to him there were many more eager mathematicians in what some depict as a cut-throat environment. Among them Gerolamo Cardano stood out, a true renaissance man who published 131 books and had expertise in many fields such as medicine and set the grounds for what would later be probability theory. Student of whom Lodovico Ferrari was, Ferrari is accredited with finding the generic solution for quartic equations in 1540. Later on other authors analyzed the interplay of the roots through permutations like Lagrange's work in 1770 or the acclaimed theorem due to Abel and Ruffini in 1799 in response to Gauss' 1798' conjecture on the non existence of a general quintic solution by radicals. Their importance relative to this work is not in that they invented anything but rather that they set up a common ground, asked a set of questions and established a notation that would later evolve into what is nowadays used. Taking a step forward, in 1830 Évariste Galois wrote 3 papers, one on number theory another one on root-finding and another one on what would later be named Galois theory. He received no recognition during his life despite submitting his findings to names like Cauchy or Fourier and went on to live a very intricate life and die at the age of 20. Among other breakthroughs Galois totally classified 5th degree polynomials according to their solvability by radicals. Some years after the concept of Galois theory was established relevant mathematicians took a shot at the inverse Galois problem:

Given a finite group G and a field K, find an extension E/K whose Galois group is G

We will restrict ourselves to the classic and still most common case, that of $K = \mathbb{Q}$, but other base fields have been analyzed as well with great detail. It is known that the Galois inverse problem is always solvable over both $\mathbb{C}(t)$ and $\overline{\mathbb{Q}}(t)$. The analysis on those base fields gave

rise to the so called rigidity method which consists on imposing conditions on the conjugacy classes and if satisfied searching in $\mathbb{Q}(t)$ instead of $\mathbb{Q}$ since if a given group occurs as a Galois group over the field of functions then it naturally occurs over the rationals. More on this topic can be found in [SAI]. This famous result is a consequence of:

Theorem 1. *(Hilbert's irreducibility theorem): Let* $\{f_i(X_1, \cdots, X_r, Y_1, \cdots, Y_s)\}_i$ *be a family of irreducible polynomials in* $\mathbb{Q}[X_1, \cdots, X_r, Y_1, \cdots, Y_s]$ *then there exists some* $(a_1, \cdots, a_r) \in \mathbb{Q}^r$ *for which* $\{f_i(a_1, \cdots, a_r, Y_1, \cdots, Y_s)\}_i$ *are irreducible over* $\mathbb{Q}[Y_1, \cdots, Y_s]$.

Proof. A proof which begins from the two variable case and argues by induction can be found in [ADA] p.104. □

Several attempts and progress in the rational base case have been successfully made. Those range from the early discovery, which some attribute to Hilbert, that any abelian group occurs as a Galois group over the rationals to the celebrated and somewhat polemic Shafarevich theorem which states that for any solvable group we have a positive answer as well. Now some attempts at providing insights in the general case consist of realizing the already classified finite simple groups as Galois groups. If one could only do both, associate a field to every finite simple group and solve every possible associated embedding problem then Galois' inverse problem would be solved in this case by brute force. This approach even if structured does not seem feasible as of today. Not only are we far from knowing whether every finite simple group is realizable as a Galois group but the amount of associated embedding problems is massive.

Even if this is a far from exhaustive and miscellaneous presentation of the time-line leading up to and from Scholz and Reichardt's discovery, for a more detailed reference on Galois' inverse problem see [VOL] and [VIL].

3 Preliminaries

In order for this work to be as intended, namely intuitive and self-contained, some prior definitions are needed before delving into the real tasks this problem entails.

3.1 Groups

Even if Scholz-Reichardt's proof is for groups of odd prime power order, as a consequence we will have the same result for all nilpotent groups of odd order. This is the most general case we can accomplish without invoking other results. Henceforth building an intuition and analyzing the interplay between p-groups and nilpotent ones is a must.

Definition 1. *A group G is said to be nilpotent if all of its Sylow subgroups are normal.*

Lemma 1. *The following are equivalent.*

1. *G is nilpotent*
2. *G has no proper self-normalizing subgroup*
3. *Every maximal subgroup is normal*
4. *G is the direct product of its Sylow subgroups*
5. *G allows a central series $\{1\} = A_0 \lhd A_1 \lhd \cdots \lhd A_n = G$ such that $[G, A_{i+1}] \subseteq A_i$*

By a central series in the last equivalence we refer to the fact that A_{i+1}/A_i is in $Z(G/A_i)$. The length of the shortest central series G allows is called the nilpotency degree. From the same equivalence we see that we are strengthening the solvability condition. As it is the case, every p-group is nilpotent and every nilpotent group is solvable. And even though the converse is definitely not true, the rigidity of nilpotent groups often allows us to establish results over p-groups and extend them naturally for all nilpotent ones.

Definition 2. *The Frattini subgroup $\Phi(G)$ of a group G is the intersection of all maximal subgroups of G.*

A particular case of interest is that of a p-group, if G is a p-group then $\Phi(G) = G^p * G'$. Frattini subgroups appear in our work as a tool to establish a more general result. The next properties on the Frattini subgroup are borrowed from p.170 of [NEU].

Proposition 1. *If a group G is generated by X and $\Phi(G)$ then X generates G itself.*

Proof. If the subgroup generated by X is proper, the maximal subgroup it is contained into contains both $\Phi(G)$ and X yielding the impossibility for the two to span the entire G. □

Proposition 2. *Let $P \subseteq H \lhd G$ where P is a p-Sylow of H and let N be P's normalizer in G. Then $NH = G$.*

Corollary 1. *The Frattini subgroup of a finite group G is nilpotent.*

Proposition 3. *If $\Phi(G) \subseteq H \lhd G$ and $H/\Phi(G)$ is nilpotent then H is also nilpotent.*

Definition 3. *The exponent of a group is the least common multiple of the orders of all elements of the group. Should this number be ill-defined, it is taken to be infinity.*

Definition 4. *The rank of a group is defined as* $\operatorname{rank}(G) = \min\{|X| \text{ s.t. } X \subseteq G \text{ and } \langle X \rangle = G\}$.

If P is a p-group $\operatorname{rank}(P) = \dim(P/\Phi(P))$ seen as a vector space over $\mathbb{F}_p$.

Definition 5. *A group G is said to be supersolvable if there exists a normal series $\{1\} = A_0 \lhd A_1 \lhd \cdots \lhd A_n = G$ such that each quotient A_{i+1}/A_i is cyclic and each A_i is normal in G.*

Some groups that occur as combination of others are a topic of discussion in this work as well. The main two will be a particular case of the fibre product and the semidirect product of groups. There is a broad definition of fibre products over any category together with its underlying theory but here we describe a particular kind of product since it is the only one we will require throughout the proof.[1]

Definition 6. *Given three groups G, H, K and two group homomorphisms $f : G \to K$ and $g : H \to K$ then $G \times_K H := \{(x, y) \in G \times H : f(x) = g(y)\}$.*

And the notion of semidirect product extends that of direct product by allowing some interplay. If G has N and H as subgroups, N is normal, $N \cap H = 1$ and $NH = G$ then we say that G is a semidirect product of N and H. More particularly, the semidirect product is isomorphic to the Cartesian product together with the inner operation $(n, h)(n', h') := (n\psi_h(n'), hh')$ where:

$$\begin{aligned} \psi : H &\longrightarrow \operatorname{Aut}(N) \\ h &\longmapsto (n \longmapsto hnh^{-1}) \end{aligned}$$

3.2 Algebraic number theory

Some instruments our toolkit has to unavoidably feature are borrowed from algebraic number theory. More particularly, we are interested in understanding the primes of fields over $\mathbb{Q}$. Not only because we are dealing with p-groups and we would like to have the intuitive notion of how the rational primes are carried to other fields but because the Galois group of an extension of number fields is very underpinned to how the primes of the base field behave in the larger one.

Definition 7. *Let $E/\mathbb{Q}$ be a number field. The ring of integers $\mathcal{O}_E$ is defined as the set of algebraic elements of $E/\mathbb{Q}$ whose minimal polynomial is monic.*

Just like when we say a rational prime we mean an integer prime, when we say a prime in E, $\mathfrak{p}$ is really a prime ideal in $\mathcal{O}_E$. A more general type of rings in which the rings of integers we will see belong are Dedekind domains.

Lemma 2. *Every number ring $\mathcal{O}_E$ is a free abelian group of finite rank equal to the degree of the field extension $[E : \mathbb{Q}]$.*

[1] Even if some sources ask for additional behaviour for the maps f and g, any homomorphism will do.

Definition 8. *A Dedekind domain is an integral domain R in which:*

- *Every ideal is finitely generated (Noetherian)*
- *Every nonzero prime ideal is maximal*
- *R is integrally closed in its field of fractions*

A crucial characterization of Dedekind domains that is often taken as the definition itself is the fact that every nonzero ideal I of a Dedekind domain can be uniquely written as $I = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$ with $\mathfrak{P}_i$ being prime.

Lemma 3. *Every number ring is a Dedekind domain.*

Proof. Thanks to the fact that every number ring is a free abelian group of finite rank, any ideal is also a free abelian group of finite rank and hence finitely generated.
If R is our number ring, to see that every nonzero prime ideal is maximal it suffices to see that R/P is finite for P prime. As if R/P is finite then it will immediately be a field and hence P will be maximal as desired. Take a nonzero $\alpha \in P$ and let $m := \prod_\sigma \sigma(\alpha) = \beta\alpha$ β is an algebraic integer which means that both β and m lie in P. Now $R/(m)$ is finite hence R/P is finite. To see the last condition, suppose that α is a root of a monic polynomial over R, $f(x) = a_0 + \cdots + a_{n-1}x^n + x^n$. Then $\mathbb{Z}[a_0, \cdots, a_{n-1}, \alpha]$ is finitely generated and hence R is integrally closed. □

From now on E/K will denote a number field extension with $[E : K] = n$ and $\mathfrak{p}$ being a prime ideal of $\mathcal{O}_K$ whose factorization in $\mathcal{O}_E$ is $\prod_{j=1}^{g} \mathfrak{P}_j$.

Definition 9. *For every j we can consider $\phi : \mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_E/\mathfrak{P}_j$ and $f_j := [\mathcal{O}_E/\mathfrak{P}_j : \mathcal{O}_K/\mathfrak{p}]$ is the inertia or residual degree of $\mathfrak{P}_j$ over $\mathfrak{p}$.*

Proposition 4. *If E/K is Galois then for every prime of $\mathcal{O}_K$: $e_i = e_j$, $f_i = f_j$ $\forall i, j$. And as a consequence $efg = n$.*

Proof. Since one has $\mathfrak{p}\mathcal{O}_E = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ and $\mathrm{Gal}(E/K)$ acts transitively on the $\mathfrak{P}_i$ there is no option but for the e_i's and f_i's to be equal. □

According to how the indices e, f and g are we will call $\mathfrak{p}$ differently.

Definition 10. *With the previous notation:*

- *If $e > 1$, $\mathfrak{p}$ is said to ramify and e is the ramification index.*
- *If $f = g = 1$, $\mathfrak{p}$ is said to be totally ramified, i.e. $\mathfrak{p} = \mathfrak{P}^n$.*
- *If $e = f = 1$, $\mathfrak{p}$ is said to split completely, i.e. $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_n$.*
- *If $e = g = 1$, $\mathfrak{p}$ is said to be inert, i.e. $\mathfrak{p} = \mathfrak{P}$.*
- *If $(e_{\mathfrak{P}/\mathfrak{p}}, \mathrm{char}(\mathcal{O}_K/\mathfrak{p})) = 1$, E/K is said to be tamely ramified.*

Lemma 4. *Both the ramification indices and residual degrees have a multiplicative nature. That is, if we have $E/L/K$ and p, $\mathfrak{p}$, $\mathfrak{P}$ primes one above the other of K, L and E respectively, then $e_{\mathfrak{P}/p} = e_{\mathfrak{P}/\mathfrak{p}} e_{\mathfrak{p}/p}$ and $f_{\mathfrak{P}/p} = f_{\mathfrak{P}/\mathfrak{p}} f_{\mathfrak{p}/p}$.*

Definition 11. *If $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ and $\mathfrak{P}$ a prime of $\mathcal{O}_E$ over $\mathfrak{p}$, then the decomposition group of $\mathfrak{P}$ is $D_{\mathfrak{P}} := \{\sigma \in \mathrm{Gal}(E/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$. $\sigma \in D_{\mathfrak{P}}$ induces an automorphism of $\mathcal{O}_E/\mathfrak{P}$ in itself, $\tilde{\sigma}$. The inertia subgroup $I_{\mathfrak{P}} \subseteq D_{\mathfrak{P}}$ is $I_{\mathfrak{P}} := \{\sigma \in D_{\mathfrak{P}} : \tilde{\sigma}(\alpha) = \alpha \ \forall \alpha \in \mathcal{O}_E/\mathfrak{P}\} = \{\sigma \in D_{\mathfrak{P}} : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \ \forall \alpha \in \mathcal{O}_E\}$.*

Two equivalent conditions of a tame ramification that are often used are the fact that $\forall \mathfrak{P}|\mathfrak{p} \quad \mathrm{char}(\mathcal{O}_K/\mathfrak{p}) \nmid |\ I_{\mathfrak{P}/\mathfrak{p}}\ |$ which happens to be in turn equivalent to having that $\forall \mathfrak{P}|\mathfrak{p}$ $\mathrm{char}(\mathcal{O}_K/\mathfrak{p}) \nmid [L : K^U]$[2]. The motivating relation we introduced between the decomposition of primes in a Galois extension and the respective Galois group is evidenced with the inertia and decomposition subgroups of the Galois group.

Proposition 5. *$|D_{\mathfrak{P}}| = ef$, $|I_{\mathfrak{P}}| = e$.*

Proof. The Galois group acts transitively on the set of prime ideals over $\mathfrak{p}$ and hence there is a relation between the group's order and that of a particular stabilizer, $D_{\mathfrak{P}}$, $|D_{\mathfrak{P}}| = n/g = ef$. Though not necessary, it is easy to see that they are all conjugates, that is for any i, j there exists a $\sigma \in \mathrm{Gal}(E/K)$ with $D_{\mathfrak{P}_i} = \sigma D_{\mathfrak{P}_j} \sigma^{-1}$. The argument is analogous for the inertia subgroup, one can either argue that it fixes a set of elements in the group or that $I(\mathfrak{P}/\mathfrak{p}) = \ker(D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(O_E/\mathfrak{P}/O_K/\mathfrak{p}))$ □

Phrased like this one may lose connection with the meaning of the decomposition and inertia subgroups. To get a good grasp they are often regarded as follows.

Lemma 5. *Let E/K be a finite extension of number fields, $\mathfrak{p}$ a prime in K and consider the tower $E/E^I/E^D/K$. Then $\mathfrak{p}$ splits completely in E^D, any prime in E^D above $\mathfrak{p}$ is inert in E^I and any prime in E^I above $\mathfrak{p}$ is totally ramified in E.*

Essentially this goes to say that they provide a tool to see which part of an extension splits completely and which is totally ramified. An exact sequence that relates the two and is often used is the following.

$$1 \longrightarrow I_{\mathfrak{p}} \longrightarrow D_{\mathfrak{p}} \longrightarrow \mathrm{Gal}(\mathcal{O}_E/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p}) \longrightarrow 1$$

Proposition 6. *Let $E/\mathbb{Q}$ be finite, then $E = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathcal{O}_E$.*

Proof. Suppose $E = \mathbb{Q}(\beta)$ and $\mathrm{Irr}(\beta, \mathbb{Q}; X) = a_0 + a_1 x + \cdots + a_n x^n$. Then we know that $a_0 a_n^{n-1} + a_1 a_n^{n-1}\beta + \cdots + a_n^n \beta^n = 0$ and setting $\alpha := a_n \beta$ we have an isomorphic extension whose minimal polynomial over $\mathbb{Z}$ is monic. □

Proposition 7. *Let E/K be a number field extension then the prime $\mathfrak{p}$ of $\mathcal{O}_K$ ramifies in $\mathcal{O}_E$ if and only if $\Delta_{\mathcal{O}_E/\mathcal{O}_K} \subseteq \mathfrak{p}$.*

Proof. A proof that first examines the case where the ring of integers allows a power basis and then attacks the general one can be found in [CON3]. □

[2] K^U stands for the maximal unramified extension of K.

As a consequence there is a finite amount of ramified primes. Moreover, there are always ramified primes in $\mathcal{O}_{L/\mathbb{Q}}$ since $\Delta_{\mathbb{Z}}(\mathcal{O}_K)$ is never a unit of $\mathbb{Z}$. This often referred to as Minkowski's theorem is a consequence of the celebrated lower bound on the discriminant a certain field extension can take.

Theorem 2. ***(Minkowski's bound)****: Let r_1 and r_2 be the number of real and complex embeddings of K respectively and $n = [K : \mathbb{Q}]$, then one has:*

$$|D_{K/\mathbb{Q}}| \geq \left(\frac{\pi}{4}\right)^{2r_2} \left(\frac{n^n}{n!}\right)^2$$

And hence yielding the impossibility for a number field over the rationals to take values ± 1 for its discriminant. A neat proof of the previous theorem can be found in [SUT].
The factorization of prime ideals over larger number rings will be a topic of interest throughout this paper and in the broader sense it is a challenging to characterize behaviour, that of distinguishing which type of ramification they have. The following result helps to better comprehend the relation between the degrees of a certain prime with those of the factors of the minimal polynomial generating the extension.

Proposition 8. *Let E/K be a finite field extension with $\mathcal{O}_E = \mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_E$ and $f(x) = \mathrm{Irr}(\alpha, K; X)$, then if $f(x) = \prod g_i(x)^{e_i} \pmod{\mathfrak{p}}$, where g_i are monic and irreducible modulo $\mathfrak{p}$, and $\mathfrak{p} \nmid \Delta$ then e_i are precisely the ramification degrees above $\mathfrak{p}$.*

Proof. We have an isomorphism from $\mathcal{O}_K[X]/(f(x))$ to $\mathcal{O}_E$ which naturally induces an isomorphism from $(\mathcal{O}_K/\mathfrak{p})[X]/(\tilde{f}(X))$ to $\mathcal{O}_E/\mathfrak{p}\mathcal{O}_E$ by reducing modulo $\mathfrak{p}$. If we take the ideals $(\tilde{g}_i)$ which lie inside of $(\tilde{f})$ those naturally correspond to ideals of $\mathcal{O}_E/\mathfrak{p}\mathcal{O}_E$ of the form $(g_i(\alpha)) + \mathfrak{p}\mathcal{O}_K$ and this correspond to $\mathfrak{P}_i = (\mathfrak{p}, g_i(\alpha))$ in $\mathcal{O}_E$. Since those are all containing $p\mathcal{O}_E$ and we can go back with this procedure we have the correspondence of the degrees not only for $e(\mathfrak{P}, \mathfrak{p}) = e((\mathfrak{p}, g_i(\alpha)), \mathfrak{p})$ but we have that $e(\mathfrak{P}_i, \mathfrak{p}) = \deg(\tilde{g}_i(x))$ □

For the sake of simplicity this has only been proved for the case $\mathcal{O}_E = \mathcal{O}_K[\alpha]$ nevertheless this constitutes no loss of generality as reducing it to the local case and then checking the factorization there will eventually yield the total factorization. And for the local case the ring of integers always allows a power basis. The following result constitutes a stepping stone in the non split case of the proof.

Proposition 9. *Let $E/\mathbb{Q}$ be a finite field extension, then there are infinitely many primes that split completely over E.*

Proof. Since it suffices to prove the statement for a larger extension, let L be E's Galoisian closure over the rationals. Then $L = \mathbb{Q}(\alpha)$ for some α and $f(x) = \mathrm{Irr}(\alpha, L, X) \in \mathbb{Z}$[X]. A prime p will split completely if p does not divide $\Delta(f)$ and there is a prime $\mathfrak{P}$ of degree 1 above p which is the same as saying that $p|f(n)$ for some $n \in \mathbb{Z}$. Let now P be the set of such primes together with those that ramify over E and suppose P to be finite to hopefully reach a contradiction. Let t be such that $\mathrm{ord}_p(t) > \mathrm{ord}_p(f(0))\ \forall p \in P$ then $\forall m\ f(mt) \equiv f(0) \pmod{t} \implies \mathrm{ord}_p(f(mt)) = \mathrm{ord}_p(f(0))\ \forall p \in P$ nevertheless $f(mt) \to \infty$ as $m \to \infty$ which implies that there must be some factor outside of P contradicting its finiteness. □

Proposition 10. *A prime $\mathfrak{p}$ splits completely in L and K if and only if it splits completely in LK.*

Proof. One direction is immediate, if it splits completely in LK, by the multiplicative nature of the indices, it will split completely in both L and K. Now let E be a galoisian closure of LK and $\mathfrak{P}$ be a prime above $\mathfrak{p}$, then $\mathfrak{p}_K = K \cap \mathfrak{P}$ has trivial indices e and f if and only if the decomposition $D_{\mathfrak{P}/\mathfrak{p}} \subseteq \mathrm{Gal}(E/K)$, the same holds for L. As this is the case by assumption, we have that for any prime of the shape $\mathfrak{p}_K$ in K, respectively in L, the result holds. But the primes above $\mathfrak{p}$ in those fields always happen to be the intersection of $\mathfrak{P}$ with the intermediate field. □

The behaviour of primes also provides useful information as to how certain field extensions differ. The clearest example is when the ramification is completely different.

Proposition 11. *Let $K/\mathbb{Q}$ and $F/\mathbb{Q}$ be field extensions where p is unramified and totally ramified respectively. Then K and F are disjoint over the rationals.*

Proof. Consider the intersection $L = K \cap F$, then by the multiplicative nature of the ramification indices p is both totally ramified and unramified in L forcing L to be the rationals. □

Some contextualization about cyclotomic fields should as well be given since we will strongly rely on them to construct our extensions. That is, in most of the cases we will restrict ourselves to fixed subfields by the Galois action over a larger cyclotomic field and hence seeing how they behave on a general scenario is a must. A theorem we will refer to and we present without proof is the famous Kronecker-Weber result.

Theorem 3. ***(Kronecker-Weber)*** *Every finite abelian extension of $\mathbb{Q}$ is a subfield of a cyclotomic field.*

Proof. An instructive proof that attacks the problem from different viewpoints can be found in [CUL]. □

As we have seen, an important tool to describe a field's behaviour is to analyze its ring of integers. Computing such a ring renders a hard task in the general case but for cyclotomic fields we have a huge simplification.

Proposition 12. *Let $K = \mathbb{Q}(\zeta_m)$ for some m, then $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$.*

And just as simplified the computation of its Galois group is.

Proposition 13. *Let $K = \mathbb{Q}(\zeta_m)$ for some m, then $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$.*

This rigidity provides the necessary tools to impose some conditions over the decomposition of primes in those fields which is ultimately what we are interested in.

Proposition 14. *Ramifying primes in $\mathbb{Q}(\zeta_m)$ are precisely those dividing m.*

Proof. As cyclotomic fields of relatively prime order are disjoint the proof reduces to the computation of the discriminant for cyclotomic fields of prime power roots of the unity. Let ζ be a primitive p^r-th root of the unity, as detailed in [MAT4250], the discriminant of $\mathbb{Q}(\zeta)$ is $(-1)^{\phi(p^r)/2} p^{p^{r-1}(pr-r-1)}$. In the same document the general case is also computed and the result we are interested in comes as corollary. □

Furthermore,

Proposition 15. *Let $K = \mathbb{Q}(\zeta_m)$ for some m and p a prime not dividing m, then p splits into $\varphi(m)/f_p$[3] primes in $\mathbb{Q}(\zeta_m)$.*

The previous claim may look like a triviality given the analysis on the possible values e, f and g could take. Nevertheless it allows us to establish a result we will deploy in many instances. Namely the fact that a prime splits completely in the m-th cyclotomic field if and only if it is congruent with 1 modulo m. The next result was presented in the Galois theory course and will be used in the proof.

Proposition 16. *Given $n \in \mathbb{N}$, there are infinitely many primes $p \equiv 1 \pmod{n}$.*

Besides some basic ramification theory and its properties over cyclotomic fields we cannot escape from providing an introduction and a set of properties concerning p-adic numbers for they will play a major role in our conclusion drawing.

Definition 12. *Given a field K, an absolute value in K is a map $|\cdot|: K \to \mathbb{R}^+$ such that $\forall a, b \in K$:*

- $|ab| = |a||b|$
- $|a + b| \leq |a| + |b|$
- $|a| = 0 \iff a = 0$

An absolute value is said to be non-archimedian if the right hand side of the triangle inequality can be replaced with $\max(|a|, |b|)$.
Just as we define extensions over fields and extensions of morphisms in Galois' theory context, an extension of an absolute value is another map that lives in a larger field whose restriction is the same as the below absolute value. We say that a certain field K is complete with respect to an absolute value if every Cauchy sequence converges to an element in K.
A possible way to regard the way in which p-adic numbers arise is by asking whether one can extend $\mathbb{Q}$ to be complete other than under the trivial absolute value, i.e. constructing $\mathbb{R}$. It turns out that with the previous constraints one can define the p-adic absolute value of $a = p^n b/c \in \mathbb{Q}$ to be p^{-n} and 0 if $a = 0$. And $\mathbb{Q}_p$ is simply the completion of $\mathbb{Q}$ under this absolute value. A strong result guarantees that there are no further completions of the rational numbers.

Theorem 4. *(Ostrowski): Every non-trivial absolute value in $\mathbb{Q}$ is either equivalent to the ordinary absolute value or the p-adic one for some prime p.*

Proof. A brief yet complete proof can be found in [CON2]. □

[3] We relax the notation when the Galois conditions for a certain extension are granted and hence all primes above p share the same indices.

To deal with p-adic equations and extract particular results other equivalent presentations come in as handy tools other than this somewhat cumbersome previous presentation. An explicit construction which requires no algebraic background consists of saying that a p-adic integer is a sequence $(a_0, a_1, \cdots)$ such that $\forall n$:

$$a_n \in \mathbb{Z}/p^{n+1}\mathbb{Z} \quad \text{and} \quad a_{n+1} \equiv a_n \pmod{p^n}$$

Then construct the field $\mathbb{Q}_p$ as the field of fractions of all p-adic integers.
Another construction that will be deployed is that of the inverse limit of the rings $\mathbb{Z}/n\mathbb{Z}$ or the profinite completition of $\mathbb{Z}$, $\hat{\mathbb{Z}}$. $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$. A result that only after the introduction of the p-adics is mentioned is one that will briefly be used during the proof but is of capital importance.

Proposition 17. *Let F be a p-adic number field. Then for each n there is a unique, up-to-isomorphism, unramified extension E of F of degree n.*

Proof. It comes as a corollary of the conducted construction of the ramification section in page 36 of [STE]. □

3.3 Group extensions

Definition 13. *A group extension is a way to describe a group G from a normal subgroup N and its quotient Q making use of a short exact sequence of homomorphisms.*

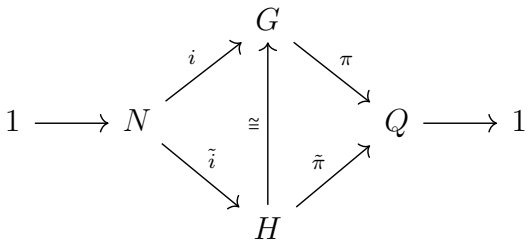
$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1$$

The extension is central if N is abelian and $\mathrm{Im}(N)$ is contained in the center of G. The sequence is said to be an extension of Q by N[4]. In case an isomorphism exists that makes the following diagram commutative we say that G and G' define equivalent extensions of Q by N.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & Q & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \beta} & & \| & & \\ 1 & \longrightarrow & N & \longrightarrow & G' & \longrightarrow & Q & \longrightarrow & 1 \end{array}$$

Additionally, we say that a given extension is split if any of the three following equivalent conditions is satisfied.

- There exists a subgroup of G which contains exactly one element from each coset of G modulo N.
- There exists a morphism $\theta : Q \to G$ such that $\pi(\theta) = \mathrm{id}_Q$.
- There is a commutative diagram:



Where we denote by H an arbitrary semidirect product of Q by N. The distinction of whether or not a particular group extension is split will play a major role in the proof. It basically "splits" it in two directions. Having this definition in hand, we can see why this will help us deal with arbitrary p-groups.

Lemma 6. *Every p-group can be regarded as a series of central extensions of degree p.*

Proof. Since we can filter a p-group G as $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ with $[G_{i+1} : G_i] = p$, freely choosing a way π_i to project G_{i+1} onto G_i we have a central extension of degree p $1 \longrightarrow C_p \longrightarrow G/G_i \longrightarrow G/G_{i+1} \longrightarrow 1$ thanks to the nontriviality of p-group's center. □

[4]Here an abuse of notation is made since the extension itself is the short exact sequence rather than the group. Some texts use the order of Q by N or N by Q interchangeably nevertheless it is more common to find: an extension of Q by N.

It turns out that classes of group extensions under the previous equivalence form a group when N is abelian. A way to assign a sum to the set of classes of extensions of G by N is by letting the sum of $\tilde{G}_1$, $\tilde{G}_2$ (two extensions of G by N) be the last short exact sequence of the diagram that follows.[5] Where $X = \{(g_1, g_2) \in \tilde{G}_1 \times \tilde{G}_2 : \pi_1(g_1) = \pi_2(g_2)\}$ and $Y = X/\{(n, -n) : n \in N\}$.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & N \times N & \longrightarrow & \tilde{G}_1 \times \tilde{G}_2 & \xrightarrow{(\pi_1 \pi_2)} & G \times G & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \mathrm{id}} & & \uparrow & & \uparrow{\scriptstyle \mathrm{diag}} & & \\
1 & \longrightarrow & N \times N & \longrightarrow & X & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle +} & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\
1 & \longrightarrow & N & \longrightarrow & Y & \longrightarrow & G & \longrightarrow & 1
\end{array}$$

Even if visually appealing, the last construction lacks good properties to do computations. A group which happens to be isomorphic to the one just described is the second cohomology group $H^2(G, N)$. Before analyzing what this equivalence exactly means a definition of the second cohomology group is in order. The classic definition of the cohomology groups would yield that H^2 is the group formed by the 2-cocycles modulo the 2-coboundaries. Given an action of G upon N, i.e. a map $\varphi : G \to \mathrm{Aut}(N)$, the 2-cocycles are maps $f : G \times G \to N$ satisfying $\varphi(g_1)(f(g_2, g_3)) + f(g_1, g_2 g_3) = f(g_1 g_2, g_3) + f(g_1, g_2) \quad \forall g_1, g_2, g_3 \in G$. While the 2-coboundaries are functions $f : G \to N$ for which there exists a function $\phi : G \to N$ such that $f(g_1, g_2) = g_1 \phi(g_2) - \phi(g_1 g_2) + \phi(g)$. More on the classical construction of the cohomology groups can be found in [AKH]. Even if it lies beyond the scope of this work to discuss the classical construction further, there is a constructive way to address the second cohomology group description following which all the elements are presented sequentially. More precisely, fix a group extension of G by N[6] and consider the action of G upon N as the map $\psi : G \to \mathrm{Aut}(N)$ defined as $\psi_g(n) := e_g n e_g^{-1}$. Where e_g is a pre-image of g in $\tilde{G}$:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & N & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \\
 & & & & e_g & \longmapsto & g & &
\end{array}$$

Even if e_g need not be unique ψ_g is well defined, does not depend on the choice of e_g, thanks to the commutativity of N. Furhtermore, let f be a particular map of the following shape.

$$\begin{array}{rcl}
f : G \times G & \longrightarrow & N \\
(g, h) & \longmapsto & e_g e_h e_{gh}^{-1}
\end{array}$$

Then not only does this match the above description of a 2-cocycle but given G, K, ψ and f we can define an extension of G by N letting $\tilde{G}$ be the group whose elements lie in the direct product together with the operation $(a, g)(b, h) := (a \psi_g(b) f(g, h), gh)$. Nevertheless f is not uniquely defined and here naturally appears the necessity of the coboundaries.

[5] More on this is found in this introduction to the cohomology of groups.

[6] We will only consider extensions whose kernel is abelian, i.e. N is commutative from now on.

Theorem 5. *If $\psi : G \to \mathrm{Aut}(N)$ is an homomorphism and N is an abelian group then there is a bijective correspondence between elements of $H^2(G, N)$ and equivalence classes of extensions of G by N.*

Proof. Most of what's to prove has been done in the constructive procedure. For a given group extension we can assign a cocycle f just as before, since equivalent extensions yield the same action and the same cocycle class the assignment is well defined. Surjectivity follows from the fact that an extension taking f as a fixed cocycle can be explicitly built. On the other hand, it is injective because if we had two extensions with the same cocycle f then the two extensions are necesarily equivalent. That is if $\tilde{G}$ and $\tilde{G}'$ are extensions of $f(g,h) = e_g e_h e_{gh}^{-1} = e'_g e'_h e_{gh}^{-1\prime}$ then we could build a $\tau : \tilde{G} \to \tilde{G}'$ such that $\pi'(\tau(ne_g)) = g = \pi(ne_g)$:

$$1 \longrightarrow N \xrightarrow{i'} \tilde{G}' \xrightarrow{\pi'} G \longrightarrow 1$$

$$N \xleftarrow[f]{} G \times G$$

$$1 \longrightarrow N \xrightarrow{i} \tilde{G} \xrightarrow{\pi} G \longrightarrow 1$$

□

Some technical details have been omitted since a thorough discussion on group extensions lies beyond the scope of this work. More particularly, we will only be interested in central extensions with simple cyclic kernel, a particular case in which the theory of group extensions is considerably simplified. A broader picture like the crash introduction presented up until here cannot damage. A proposition that will be useful later on is the following:

Proposition 18. *A group extension of G by N is split if and only if the extended group is isomorphic to the semidirect product of G and N.*

Since we will be dealing only with central extensions and the action of conjugation in those cases is trivial we will have the trivial case of the semidirect product when the extension is split, i.e. the direct product.

4 Embedding problem

Definition 14. *Given two epimorphisms $\pi : \tilde{G} \to G$ and $\phi : H \to G$ we say that the embedding problem for the pair (π, ϕ) consists in finding $\tilde{\phi}$ such that $\pi \circ \tilde{\phi} = \phi$. We say that a solution is proper if $\tilde{\phi}$ is surjective as well.*

Phrased as it is, this definition may look like a purely group theoretic matter. It is not the case. Recall that Galois' inverse problem focuses on finding a field over $\mathbb{Q}$ with a prescribed Galois group. Determining a number field with Galois group G is equivalent up to isomorphism to defining an epimorphism from $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ to G. Indeed, if we had $\rho : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \twoheadrightarrow G$ then taking $\overline{\mathbb{Q}}^{\ker(\rho)}$ we would be done. Knowing this and foreseeing that we will follow a step-wise path towards the desired field we can frame the embedding problem in a much more convenient way. We will say that the embedding problem for L (a finite Galois extension of $\mathbb{Q}$) and $\tilde{G}$ (the group in-between an extension of G by another group N) consists in finding $\tilde{L}$ such that $\mathrm{Gal}(\tilde{L}/\mathbb{Q}) \cong \tilde{G}$ and the following diagram commutes.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & N & \xrightarrow{\ i\ } & \tilde{G} & \xrightarrow{\ \pi\ } & G & \longrightarrow & 1 \\
 & & \| & & \wr\| & & \| & & \\
1 & \longrightarrow & \mathrm{Gal}\left(\tilde{L}/L\right) & \longrightarrow & \mathrm{Gal}\left(\tilde{L}/K\right) & \longrightarrow & \mathrm{Gal}\left(L/K\right) & \longrightarrow & 1
\end{array}$$

Which is equivalent to finding a surjective $\tilde{\phi}$ for which the following diagram commutes.

$$\begin{array}{ccccccccc}
 & & & & & & \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) & & \\
 & & & & & \swarrow^{\tilde{\phi}} & \downarrow{\scriptstyle \phi} & & \\
1 & \longrightarrow & N = \mathrm{Gal}\left(\tilde{L}/L\right) & \longrightarrow & \tilde{G} = \mathrm{Gal}\left(\tilde{L}/\mathbb{Q}\right) & \longrightarrow & \mathrm{Gal}\left(L/\mathbb{Q}\right) & \longrightarrow & 1
\end{array}$$

Similar presentations are adopted in nearly any paper that tries to deal with Galois' inverse problem. We will focus in a particular type of embedding problems. The case when N is cyclic of prime order and injected into $\tilde{G}$'s center. In short, a cyclic central extension. A less particular viewpoint is presented in [SON] where the nonsolvability of the groups considered forces a more general approach. In the same paper a step-wise path towards G is also taken, meaning $G_n = \{1\} \subseteq G_{n-1} \subseteq \cdots \subseteq G_0 = G$ and the embedding problem is rephrased as follows. Suppose K_i/k is Galois and $\gamma_i : \mathrm{Gal}(K_i/k) \to G/G_i$ is an isomorphism. Then the embedding problem consists in finding K_{i+1}/k Galois for which an isomorphism γ_{i+1} exists and the following diagram commutes:

$$\begin{array}{ccc}
\mathrm{Gal}\left(K_{i+1}/k\right) & \xrightarrow{\ \mathrm{res}\ } & \mathrm{Gal}\left(K_i/k\right) \\
\downarrow{\scriptstyle \gamma_{i+1}} & & \downarrow{\scriptstyle \gamma_i} \\
G/G_{i+1} & \xrightarrow{\ \pi\ } & G/G_i
\end{array}$$

Our main concern during the proof will be to assert whether under some conditions a proper solution $\tilde{\phi}$ for a given embedding problem exists. At the end of the proof some examples of embedding problems without solution are presented to see that our analysis is not empty.

As we anticipated and we will elaborate upon later, the distinction of whether or not the group extension considered splits is of capital importance. Note that in our case, since $N = C_p$ for some p, if the extension doesn't split then any nontrivial $\tilde{\phi}$ is necessarily surjective. As if it didn't fill $\tilde{G}$ entirely $\mathrm{Im}(\tilde{\phi}) = G$ and a splitting would exist. Moreover, given a solution $\tilde{\phi}$ of a particular central embedding problem, any solution is obtained by twisting it.

Definition 15. *A twist of a solution $\tilde{\phi}$ of the central embedding problem*

$$\begin{array}{ccccccccc} & & & & & & H & & \\ & & & & & \swarrow^{\tilde{\phi}} & \downarrow{\scriptstyle \phi} & & \\ 1 & \longrightarrow & N & \xrightarrow{i} & \tilde{G} & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array}$$

is an homomorphism $\chi : H \to N$. We say that the twisted solution is $\chi \cdot \tilde{\phi}$.

Note that this does not denote the composition nor the concatenation of paths but rather the plain product. The new lift consists of taking an element $\sigma \in H$ and sending it to $\tilde{\phi} \cdot i(\chi)(\sigma) = \tilde{\phi}(\sigma) \cdot i(\chi(\sigma))$. In general this need not be well defined but as $i(N)$ is in $\tilde{G}$'s center, everything behaves appropriately.

Lemma 7. *Let $\tilde{\phi}$ denote a solution to a central embedding problem. Then any solution of the embedding problem is a twist of $\tilde{\phi}$.*

Observe that the embedding problem with trivial group G is simply Galois' inverse problem. Setting G to be an intermediate quotient of our desired group gives us a structured path towards finding an extension for the end group. This among others is the reason why we disseminate our group into pieces the solvability of which is feasible. This comes at the expense of having to "paste" the partial solutions which in itself is a challenge and is thoroughly discussed in the proof. A nice result that relies on the classification of finitely generated abelian groups shows why restricting ourselves to p-groups does not carry that big a loss in generality.

Proposition 19. *The solvability of an embedding problem with abelian kernel is equivalent to the solvability of all the respective embedding problems with p-group kernel in which the abelian kernel factors with disjoint solutions.*

In the definition we do not care to specify whether the fields considered are local or global. In the proof we will see that by localizing, i.e. completing the fields with respect to a given prime and augmenting the maps of the embedding problem yields a new embedding problem. The relations between those two will be a concern of ours during the proof.

The somewhat unreasonable motif by which so much is accomplished, i.e. the proof of the theorem, with apparently so little is in part due to the ease with which abelian group extensions are classified. Nonetheless the embedding problems, as seen in [SON] are a widespread tool in many fields.

5 Scholz-Reichardt's proof

As detailed above, our intention is to present a self-contained proof of the following theorem.

Theorem 6. *Every p-group* $(p \neq 2)$ *can be seen as a Galois group over* $\mathbb{Q}$.

The most natural approach would go along the lines of analyzing the subgroup lattice and associate a sequence of fields strongly relying on Galois' correspondence to end up finding a field over $\mathbb{Q}$ whose group is the entire G. This procedure is nevertheless doomed to fail since not all paths lead to the final desired field extension. At the end of the proof, motivating examples justifying the necessity of the stringent conditions are presented to better contextualize our approach. Since it is preferred to use p as default, when a prime is initially fixed it is often denoted by ℓ to have p at our disposal later on. In order for us to later ensure that we can "keep climbing along the tree", we introduce the following condition on the intermediate extensions.

Definition 16. *A field extension* $E/\mathbb{Q}$ *whose Galois group is an* ℓ*-group is said to have the property* S_N *if every ramified prime* p *satisfies:*

- $p \equiv 1 \pmod{\ell^N}$
- *For every* $\mathfrak{p}|p$ *we have* $I_\mathfrak{p} = D_\mathfrak{p}$

Proposition 20. *The second condition is equivalent to saying that* $L_\mathfrak{p}/\mathbb{Q}_p$ *is totally ramified.*

Proof. This means that the ramification index of $\mathfrak{p}$ in $L/\mathbb{Q}$ is equal to $[L_\mathfrak{p} : \mathbb{Q}_p]$ and hence $f_\mathfrak{p}$ is 1 and the decomposition and inertia subgroups coincide. Conversely, if they coincide since they carry up to the completions we would have that the residue extension is trivial meaning that $f_\mathfrak{p} = 1$ in $L_\mathfrak{p}/\mathbb{Q}_p$. □

Naively the proof can be thought of as an inductive procedure. We begin from an explicit description of the structure of G in terms of some of its subgroups as follows.

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

$$\{1\} \to C_\ell \hookrightarrow G/G_i \twoheadrightarrow G/G_{i+1} \to \{1\}$$

The base case if one wishes, is basically saying that there are Galois extensions over $\mathbb{Q}$ with group C_ℓ for all ℓ satisfying S_N's condition. And the inductive step is to find a Galois extension of the corresponding field of $G_i = \mathrm{Gal}(L/K)$, $\tilde{L}$ whose corresponding group is precisely $\tilde{G}$ and for which the following diagram commutes and S_N's condition holds. Finding such an $\tilde{L}$ is precisely solving the embedding problem.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & C_\ell & \xrightarrow{\quad i \quad} & \tilde{G} & \xrightarrow{\quad \pi \quad} & G & \longrightarrow & 1 \\
 & & \wr\uparrow & & \wr\uparrow & & \wr\uparrow & & \\
1 & \longrightarrow & \mathrm{Gal}\left(\tilde{L}/L\right) & \longrightarrow & \mathrm{Gal}\left(\tilde{L}/\mathbb{Q}\right) & \longrightarrow & \mathrm{Gal}\left(L/\mathbb{Q}\right) & \longrightarrow & 1
\end{array}$$

Proposition 21. *For every prime ℓ there exists a Galois extension $E/\mathbb{Q}$ with Galois group C_ℓ and verifying S_N's condition.*

Proof. As seen in the preliminaries, we can freely chose a prime $p \equiv 1 \pmod{\ell^N}$ and consider the cyclotomic field $\mathbb{Q}(\zeta_p)$ over the rationals. A C_ℓ field will exist in-between immediately satisfying the first condition by construction, recall that the only prime ramifying will be p, and since we will have that for all $\mathfrak{v}$ above p $e_{\mathfrak{v}/p} f_{\mathfrak{v}/p} g_p = \ell$ and $e_{\mathfrak{v}/p} > 1$ we get that the inertia and decomposition groups coincide. □

From now on the main concern will be assessing the truthfulness of the next result which ensures the existence of a path along the field lattice provided Scholz's condition is satisfied at every step.

Theorem 7. *Let $L/\mathbb{Q}$ be Galois with group G, assume that L has the property S_N and that ℓ^N is a multiple of the exponent of $\tilde{G}$. Then the embedding problem for L and $\tilde{G}$ has a solution $\tilde{L}$ which satisfies S_N.*

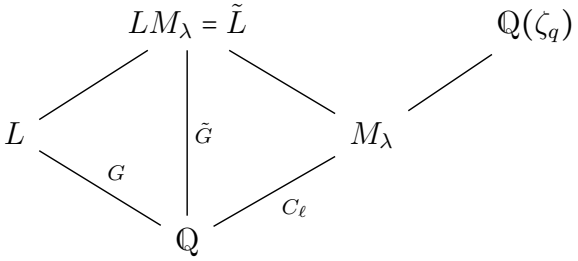
Additionally, as we will see across the proof, this constructed extension is tuned in such a way that $\tilde{L}$ is ramified at at most one more prime than L.

5.1 Split case: $\tilde{G} \cong G \times C_\ell$

Having such an explicit expression of the next group in our list, $\tilde{G}$, enables us to take a very intuitive approach when tackling the embedding problem in this particular setup. The basic idea is to find a prime q that behaves well enough so that we can define $\lambda : \left(\mathbb{Z}/q\mathbb{Z}\right)^* \twoheadrightarrow C_\ell$, $M_\lambda = \mathbb{Q}(\zeta_q)^{\ker(\lambda)}$ and ensure that the following conditions are satisfied.

- M_λ only ramifies at q
- M_λ is disjoint from L
- LM_λ satisfies S_N's condition

In this case we will have $\tilde{L} = LM_\lambda$ as desired:



Let $p_1, \cdots, p_m$ be the ramified primes over L, assume that L has the property S_N and that $\exp(\tilde{G}) \mid \ell^N$ then we wish to pick a prime q satisfying the following conditions.

- $q \equiv 1 \pmod{\ell^N}$
- q splits completely over L
- p_i are all ℓ-th powers in $\mathbb{F}_q$

Proposition 22. *The latter set of properties is equivalent to saying that q splits completely over not only L but also over $L(\zeta_{\ell^N}, \sqrt[\ell]{p_1}, \cdots, \sqrt[\ell]{p_m})$.*

The relevance of this equivalence is very significant in our understanding of the problem since it enables us to claim the existence of such a prime q, strongly relying on the infinity of totally split primes in number fields. This apparently flawless procedure does not come exempt of intricacies. To prove the equivalence we borrow the guideline presented in [MAS] (p.25).

Proposition 23. *A prime $q \nmid \ell^N$ splits completely in $\mathbb{Q}(\zeta_{\ell^N})$ if and only if $q \equiv 1 \pmod{\ell^N}$*

Proof. Since it does not divide ℓ^N we already know that q will be unramified and the fact that $f(\mathfrak{Q}/q) = 1$ for all $\mathfrak{Q}$ above q is a consequence of the next lemma. □

Lemma 8. *If q is a prime not dividing ℓ^N its residual degree in $\mathbb{Q}(\zeta_{\ell^N})/\mathbb{Q}$ is equal to the least integer f such that $q^f \equiv 1 \pmod{\ell^N}$.*

Proof. By definition the residual degree is the order of the group $\big(\mathbb{Q}(\zeta_{\ell^N})/\mathfrak{p}\mathbb{Q}(\zeta_{\ell^N})\big)/\big(\mathbb{Z}/q\mathbb{Z}\big)$ for any prime $\mathfrak{p}$ above q. And in the other hand the least integer f satisfying the condition happens to be the exponent of the group. We want to prove that they coincide provided that $q \nmid \ell^N$. Because of the uniqueness of unramified extensions of $\mathbb{Q}_q$ of a certain degree it is possible to deduce that $\mathbb{Q}_q(\zeta_{\ell^N})$ is minimal with the property that it has as residue class field $\mathbb{F}_{q^f}$. Now deploying the correspondence between the localized and non localized extensions we can say that q is unramified in $\mathbb{Q}(\zeta_{\ell^N})$ and will have residue class degree the same f. □

As a consequence, since $q \nmid \ell^N$ by hypothesis, q will split completely in $\mathbb{Q}(\zeta_{\ell^N})$

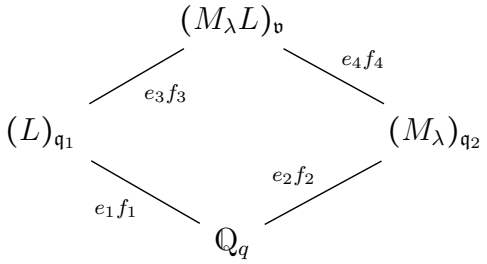
Lemma 9. *Suppose we have the following diagram, if p_i^f is the least power of p_i such that $p_i^f \equiv x^\ell \pmod{\mathfrak{Q}}$ is solvable, then f is precisely $f(\mathfrak{v}/\mathfrak{Q})$*

$$\begin{array}{ccc} \mathbb{Q}(\zeta_{\ell^N}, \sqrt[\ell]{p_i}) & \text{———} & \mathfrak{v} \\ | & & | \\ \mathbb{Q}(\zeta_{\ell^N}) & \text{———} & \mathfrak{Q} \\ | & & | \\ \mathbb{Q} & \text{———} & q \end{array}$$

Proof. This result comes as an immediate consequence if one constructs Kummer theory as it was done in [FRO]. For a detailed proof see the page 91 of the previous reference. □

And as a consequence of this lemma, since every p_i is an ℓ-th power modulo q and hence an ℓ-th power modulo $\mathfrak{Q}$, the residual degree $f(\mathfrak{v}/\mathfrak{Q}) = 1$ and q will split completely in the larger field if it does in the cyclotomic one, for which we already saw it did. Now using one of the propositions presented in the preliminaries, according to which a prime splits in a compositum of fields if and only if it does in every one separately we get the much desired equivalence.

With the previous construction we ensured the existence of such an $\tilde{L}$ above, nevertheless to finish the split case we have to verify that this step does not violate S_N's condition. As M_λ and L are linearly disjoint over $\mathbb{Q}$ the ramification can be examined separately. Since M_λ was constructed as a subfield of the q-th cyclotomic field, it only ramifies in q and q verifies again by construction Scholz's first condition. Since all p_i's ramifying in L verified S_N by the inductive step we have that the first condition immediately holds. To display how the inertia and decomposition groups of the ramifying primes coincide we will consider the two families separately.
For the second condition to hold at q it would suffice to have $f_{\mathfrak{v}/q} = 1$ for $\mathfrak{v} \in M_\lambda L$ which in turn is equivalent to having $f_{\mathfrak{v}/q} = 1$ for $\mathfrak{v} \in (M_\lambda L)_\mathfrak{v}$. It is coherent to factor f as the total local field happens to factor itself. The next diagram will serve as a guide to prove that $f_{\mathfrak{v}/q} = 1$.



Because of the multiplicative nature of the indices, describing the total ramification can be done in a step-wise maneer. $e_1 = f_1 = 1$ since q was chosen to split completely in L while $e_2 = \ell$ and $f_2 = 1$ as q is totally ramified in (M_λ).

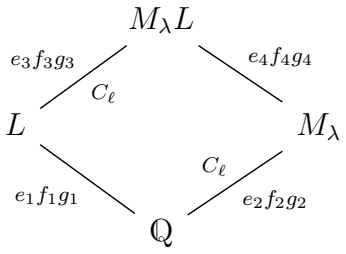
Proposition 24. *Let $L/\mathbb{Q}_p$ and $M/\mathbb{Q}_p$ be Galois extensions, then $e_{ML/L} \leq e_{M/\mathbb{Q}_p}$.*

As the last proposition is symmetric on the extensions above $\mathbb{Q}_p$, one has two immediate results, $e_{\mathfrak{v}/q} = e_3 e_1 = e_3 \leq e_2 = \ell$ and $e_4 \leq e_1 = 1 \implies e_4 = 1$. And as ℓ must divide $e_{\mathfrak{v}/q}$ since $e_2 = \ell$, we have that $e_{\mathfrak{v}/q} = \ell$ and the only remaining unknowns from the diagram are f_3 and f_4. The next lemma will shed some light.

Lemma 10. *Let $K/\mathbb{Q}$ be a finite Galois extension, then for every prime $q \in \mathbb{Q}$ and $\mathfrak{v}$ above one has $[K_\mathfrak{v} : \mathbb{Q}_q] = \frac{[K:\mathbb{Q}]}{g_\mathfrak{v}}$.*

Henceforth, $[(M_\lambda L)_\mathfrak{v} : \mathbb{Q}] = \frac{[M_\lambda L:\mathbb{Q}]}{g_\mathfrak{v}} = \ell$. Implying that $e_2 f_2 e_4 f_4$ must be ℓ forcing f_4 to be trivial and then $f_{\mathfrak{v}/q} = f_2 f_4 = 1$ as desired yielding $I_\mathfrak{v} = D_\mathfrak{v}$ for any $\mathfrak{v}$ above q.
Having checked both conditions for q we proceed to examine the second condition for the primes that already ramified in L. First off, note that by the congruences we imposed the

p_i's to satisfy, if p_i is ramified in L it immediately splits completely in M_λ. With that in mind we can already describe the behaviour through the next diagram.



And we know that $f_1 = 1$ since S_N held in the previous iteration, $e_2 = f_2 = 1$ as p_i splits completely in M_λ and since the restriction map res_{M_λ} is an isomorphism that sends a generator of $\mathrm{Gal}(M_\lambda L/L)$ to one of $\mathrm{Gal}(M_\lambda/\mathbb{Q})$ we have that $f_3 = 1$. Summing up, we wanted to see how the decomposition and inertia subgroups of $\mathrm{Gal}(M_\lambda L/\mathbb{Q})$ were equal for all p_i and they differ by $f_{\mathfrak{P}/p_i}$ which in turn is equal to $f_1 f_3 = 1$ yielding the equality.

5.2 Non split case

Having seen how to solve the embedding problem when the structure of the next group $\tilde{G}$ is as simple as the cartesian product of the previous by a C_ℓ, we wish to tackle the non split case. Notice how we do not refer to this as the "general case" as it is by no means a generalization of the previous one, the arguments used here do not apply for the direct product as we will shortly notice. In what follows the underlying assumption is that there is some interplay between the elements of the groups we are considering the extension by.

The proof to ensure the solvavility of every step will basically be a pipeline consisting of three steps:

- Finding an extension $\tilde{L}$ which solves the embedding problem
- Changing the previously found extension so that it ramifies only where L ramifies
- Modifying again $\tilde{L}$ so that it verifies S_N's condition at the expense of ramifying at at most one more prime

5.2.1 Step I: Finding $\tilde{L}$

As we have L, G and apparently no further information regarding $\tilde{G}$'s structure, it is natural to take a general approach and consider the map ϕ induced by L as a subfield of the algebraic closure of $\mathbb{Q}$, $\overline{\mathbb{Q}}$, defined as:

$$\begin{aligned} \phi : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) &\longrightarrow \mathrm{Gal}\left(L/\mathbb{Q}\right) \\ \sigma &\longmapsto \phi(\sigma) = \sigma|_L \end{aligned}$$

Note that due to normality, the restriction map ϕ is a well defined surjective morphism as there are no maps from L falling outside of it regarding it as a subfield of an algebraic closure. As we saw in the embedding problem section, finding $\tilde{L}$ is the same as finding a surjective lift of ϕ, for which the following diagram commutes since $\tilde{L} = \overline{\mathbb{Q}}^{\mathrm{Gal}(\overline{\mathbb{Q}}/\tilde{L})} = \overline{\mathbb{Q}}^{\ker(\tilde{\phi})}$.

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}} = \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) & & \\ & & & & & \swarrow^{\tilde{\phi}} & \downarrow{\scriptstyle \phi} & & \\ 1 & \longrightarrow & C_\ell \cong \mathrm{Gal}\left(\tilde{L}/L\right) & \xrightarrow{i} & \tilde{G} \cong \mathrm{Gal}\left(\tilde{L}/\mathbb{Q}\right) & \xrightarrow{\pi} & G \cong \mathrm{Gal}\left(L/\mathbb{Q}\right) & \longrightarrow & 1 \end{array}$$

Here $\tilde{\phi}$ will always be surjective. Should $\tilde{\phi}$ not fill $\tilde{G}$ entirely, then a split would exist as $\mathrm{ord}(\mathrm{Im}(\tilde{\phi})) = \mathrm{ord}(G)$ contradicting our non-split hypothesis. Now thanks to our previous discussion on group extensions we can take for granted the correspondence between elements of $H^2(G_{\mathbb{Q}}, C_\ell)$ and classes of group extensions of $G_{\mathbb{Q}}$ by C_ℓ. In particular, let ξ be the class of our extension, that is $\xi \in H^2(G, C_\ell)$, and consider the group homomorphism obtained by composing ϕ with the aforemention correspondence:

$$\phi^* : H^2(G, C_\ell) \to H^2(G_{\mathbb{Q}}, C_\ell)$$

This naturally yields a group extension of $G_{\mathbb{Q}}$ by C_ℓ, namely the one corresponding to $\phi^*(\xi)$.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_\ell & \xrightarrow{i_2} & \tilde{\tilde{G}} & \xrightarrow{\pi_2} & \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \pi_3} & & \downarrow{\scriptstyle \phi} & & \\ 1 & \longrightarrow & C_\ell \cong \mathrm{Gal}\left(\tilde{L}/L\right) & \xrightarrow{i_1} & \tilde{G} \cong \mathrm{Gal}\left(\tilde{L}/\mathbb{Q}\right) & \xrightarrow{\pi_1} & G \cong \mathrm{Gal}\left(L/\mathbb{Q}\right) & \longrightarrow & 1 \end{array}$$

This may all look a bit artificial but thanks to the following result we can infer some properties on our extension of interest.

Proposition 25. *A group extension $1 \to N \to \tilde{G} \to G \to 1$ splits if and only if the element corresponding to its class in $H^2(G, N)$ is trivial.*

Proof. Thanks to the correspondence theorem and the construction of the associated element of the extension in previous' sections we see that if the corresponding element is trivial then the extension is equivalent to that generated by the trivial cocycle, not only the class of the cocycle, $f = 1$. Hence the inner operation on the group $\tilde{G}$ is $(a, g)(b, h) = (a\psi_g(b)f(g, h), gh) = (a\psi_g(b), gh)$ which is precisely the relation of the semidirect product of $N \times_\psi G$, yielding that the extension is split.
Conversely, if the extension is split, relying again on the construction we see how there is no other choice for f but to be trivial and hence the extension corresponds to the trivial class in $H^2(G, N)$. □

Proposition 26. ***(Höchsmann)*** *The existence of $\tilde{\phi}$ is equivalent to the vanishing of $\phi^*(\xi)$, i.e. $\phi^*(\xi) = 0$.*

Proof. If $\tilde{\phi}$ exists we can without loss of generality set the up until now generic $\tilde{\tilde{G}}$ to be a particular group:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_\ell & \xrightarrow{i_2} & \tilde{G} \times_G G_{\mathbb{Q}} & \xrightarrow{\pi_2} & G_{\mathbb{Q}} & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \pi_3} & \swarrow{\scriptstyle \tilde{\phi}} & \downarrow{\scriptstyle \phi} & & \\ 1 & \longrightarrow & C_\ell & \xrightarrow{i_1} & \tilde{G} & \xrightarrow{\pi_1} & G & \longrightarrow & 1 \end{array}$$

And then we define δ to be the splitting morphism of the extension above, i.e. $\delta(a) := (\tilde{\phi}(a), a)$ and since $\pi_2(\delta) = \mathrm{id}_{G_{\mathbb{Q}}}$ we reach the desired implication.
Conversely, if $\phi^*(\xi) = 0$ by the previous proposition we know the extension on top splits and hence exists some τ such that $\pi_2(\tau) = \mathrm{id}_{G_{\mathbb{Q}}}$, take $\tilde{\phi}$ to be $\pi_3 \circ \tau$ and we are done. □

Because of the common appearance of $H^2(G_{\mathbb{Q}}, C_\ell)$ some authors relax the notation and refer to it as $H^2(\mathbb{Q}, C_\ell)$ instead. From now on we will use this convention as well.

As we will later explain, this path choice is not coincidental. Very often when trying to extract global results one restricts himself to the local problems. This becomes apparent when the inverse problem is constrained to having a certain set of primes ramifying and not all are allowed. For now we will believe the following theorem which basically acts as a bridge for $\phi^*(\xi)$ between $\mathbb{Q}$ and $\mathbb{Q}_p$.

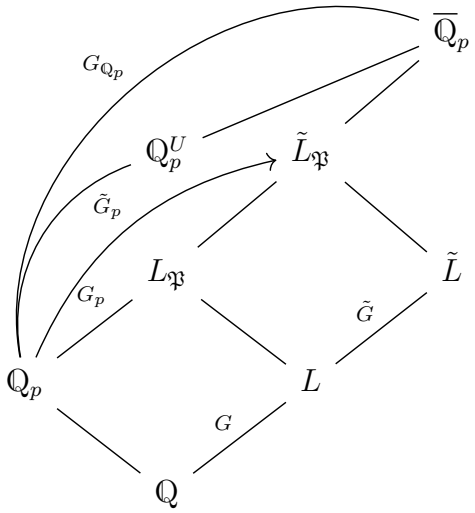
Theorem 8. *The restriction map $\mathfrak{R} : H^2(\mathbb{Q}, C_\ell) \to \prod_p H^2(\mathbb{Q}_p, C_\ell)$ is injective.*

The fact that the previous map is injective tells us that whenever a zero is found in the image, it necessarily comes from the trivial element. Henceforth reducing the problem to $\mathbb{Q}_p$. That is, the triviality of $\phi^*(\xi)$ not only implies the triviality of $\mathfrak{R}(\phi^*(\xi))$ but they are equivalent, and the triviality of the latter occurs only when projecting in the p-th component the result is zero as well. Summing up we have that the existence of such a desired $\tilde{\phi}$ is equivalent to the embedding problem being solvable locally at all primes p.
Note that we have yet to prove the existence of $\tilde{L}$ but with all of these consecutive reductions we have seen that its existence is equivalent to the solvability of the following embedding problem for all p.

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}_p} = \mathrm{Gal}\left(\overline{\mathbb{Q}}_p/\mathbb{Q}_p\right) & & \\ & & & & & \swarrow{\scriptstyle \tilde{\phi}_p} & \downarrow{\scriptstyle \phi_p} & & \\ 1 & \longrightarrow & C_\ell & \longrightarrow & \tilde{G}_p = \mathrm{Gal}\left(\tilde{L}_{\mathfrak{P}}/\mathbb{Q}_p\right) & \longrightarrow & G_p = \mathrm{Gal}\left(L_{\mathfrak{P}}/\mathbb{Q}_p\right) & \longrightarrow & 1 \end{array}$$

In [ROQ] instead of defining a new embedding problem they refer to this as the localized embedding problem of the initial one and they are treated as pairs. We say that the local-global-principle, LGP in short, holds if the solvability of all the localized embedding problems

implies that the global embedding problem is solvable.
Having discussed the equivalences we go on to see that the localized embedding problem is always solvable. We first examine the case when p does not ramify in L. If p is unramified in L then $e = 1$ and as a consequence its inertia group $I_{\mathfrak{P}} \subseteq G = \mathrm{Gal}(L/\mathbb{Q})$ will be trivial for all $\mathfrak{P}$ above p. And $G_p \cong D_{\mathfrak{P}}$ because $g = 1$, simply because of the fact that it is a local extension, i.e. only a maximal ideal can lie above p. In the other hand using again that the inertia is trivial we have that $D_{\mathfrak{P}} \cong \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}/\mathbb{Z}/p\mathbb{Z})$ and since any extension of finite fields is cyclic, G_p will be cyclic. The following diagram depicts what is happening and introduces $\mathbb{Q}_p^U$[7].



For any $\mathfrak{v} \in \overline{\mathbb{Q}}_p$ above $\mathfrak{P}$ we have that $G_{\mathbb{Q}_p}/I_{\mathfrak{v}} = G_{\mathbb{Q}_p}/I_{\mathfrak{P}} \cong \mathrm{Gal}(\mathbb{Q}_p^U/\mathbb{Q}_p) \cong \hat{\mathbb{Z}}$. If ψ is the previous isomorphism then we have an induced morphism $\hat{\mathbb{Z}} \xrightarrow{\psi^{-1}} G_{\mathbb{Q}_p}/I_p \xrightarrow{\pi^{-1}} G_{\mathbb{Q}_p} \xrightarrow{\phi_p} G_p$. And finding an appropriate $\tilde{\phi}_p$ is the same as finding a lift of one of the previous shape, i.e. parting from $\hat{\mathbb{Z}}$. Recalling that G_p is cyclic and that the extension is central there are only two possibilities. $\tilde{G}_p$ can only be isomorphic to the direct product or to an enlarged cyclic group. In either case we can associate the generator of $\hat{\mathbb{Z}}$ to any preimage of a generator of G_p within $\tilde{G}_p$ and that ultimately defines $\tilde{\phi}_p$ itself.

If p happens to ramify in L we proceed as follows. From the fact that the first Scholz condition still holds we have that $p \equiv 1 \pmod{\ell^N}$, in particular $\ell \nmid p$ and hence $L_{\mathfrak{P}}/\mathbb{Q}_p$ is tamely ramified ($(e_p, \mathrm{char}(\mathbb{Z}_p/p\mathbb{Z}_p)) = 1$). Arguing now by the second condition we have equality of I_p and D_p and hence $I_{\mathfrak{P}} = D_{\mathfrak{P}}$ and by properties of the ramification groups we get to see that those are cyclic. Bear in mind that here whenever we have localized g is trivial. Now recall that our purpose is to find a lift of $\phi_p : G_{\mathbb{Q}_p} \to G_p$. We define E to be the maximal abelian tame extension of $\mathbb{Q}_p$ with exponent dividing ℓ^N. To build our interpretability, E can be built from scratch $E = RS$. Where R is the unique unramified extension of $\mathbb{Q}_p$ of

[7]Some properties between the inertia/decomposition subgroups and the maximal unramified extensions are given in the preliminaries and used here without further explanation.

degree ℓ^N whose group can be seen that is $\mathbb{Z}/\ell^N\mathbb{Z}$. And S is the totally ramified extension $S = \mathbb{Q}_p(\sqrt[\ell^N]{p})/\mathbb{Q}_p$ whose group is $\mathbb{Z}/\ell^N\mathbb{Z}$ that happens to be Kummer. By their definitions it can be seen that they are disjoint and as a consequence $\mathrm{Gal}(E/\mathbb{Q}_p) = \mathbb{Z}/\ell^N\mathbb{Z} \times \mathbb{Z}/\ell^N\mathbb{Z}$ and it is projective in the category of abelian groups of exponent dividing ℓ^N. For an element P to be projective within a certain category it means that for any A, B, $\alpha : A \to B$ and $\beta : P \to B$ there is a morphism $\gamma : P \to A$ such that $\beta = \gamma\alpha$. Choosing at our convenience the elements A, B and α of the definition we can get the desired result. That is, by letting:

$$\begin{array}{ccccccccc} & & & & & & P = \mathrm{Gal}(E/\mathbb{Q}_p) & & \\ & & & & & \swarrow^{\gamma=\tilde{\phi_p}} & \downarrow{\scriptstyle \beta=\phi_p} & & \\ 1 & \longrightarrow & C_\ell & \longrightarrow & A = \tilde{G_p} & \longrightarrow & B = G_p & \longrightarrow & 1 \end{array}$$

Saying that $\mathbb{Z}/\ell^N\mathbb{Z} \times \mathbb{Z}/\ell^N\mathbb{Z}$ is projective in this particular category is a fancy way to phrase the fact that if we have two maps $\beta : \mathbb{Z}/\ell^N\mathbb{Z} \times \mathbb{Z}/\ell^N\mathbb{Z} \longrightarrow B$ and $\alpha : A \longrightarrow B$ we can associate the two generators of $\mathbb{Z}/\ell^N\mathbb{Z} \times \mathbb{Z}/\ell^N\mathbb{Z}$ to elements of A defining γ. This is possible thanks to the classification of finitely generated abelian groups. We can factor A and B into products of cyclic subgroups with exponent dividing ℓ^N and then the correspondence is obvious.
For all, the local embedding problem is solvable for all p and by the previous equivalence of the local-global-principle provided by the injectivity of the map ϕ^* we get that in the non-split case as a whole, the embedding problem is solvable. Now we have constructed a field extension $\tilde{L}$, if we had been on our penultimate step we could leave it here nevertheless for this to be an inductive procedure we have to verify that we will be able to repeat what was done up until here.

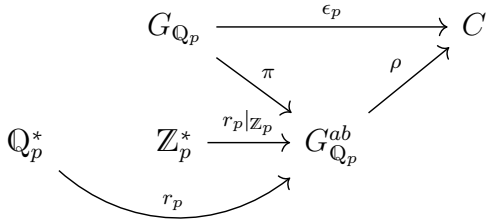
5.2.2 Step II: Ensuring low ramification

As said, we have to restrict the ramified primes in our constructed extension. Our goal from here onward is to make the extension $\tilde{L}$ depicted in the last section verify S_N yet the more primes ramifying the tougher it will be for the condition to hold. This control was feasible and easy to deal with in the split case when the constructions where explicit, in its counterpart, the non-split case, it is not constructive since we had to incur to the local-global-principle and appeal to existence arguments. Nevertheless an analog exists again relying on local-global ideas.
We will say that a group homomorphism $\varphi : \mathrm{Gal}(E/K) \to H$ is unramified if $E^{\ker(\varphi)}$ is unramified. An immediate yet important result is that a map is unramified if and only if its restriction to the inertia group is trivial. Indeed, if $\varphi(I_p) = 1$ then $I_p \subseteq \ker(\varphi)$ which implies that $E^{\ker(\varphi)} \subseteq E^{I_p} = E^{U_p}$ (maximal field unramified at p). And conversely, if φ is unramified then for every p I_p will be trivial and the restriction map as well.

Lemma 11. *For every prime p consider a continuous homomorphism $\epsilon_p : \mathrm{Gal}\left(\overline{\mathbb{Q}}_p/\mathbb{Q}\right) \to C$ where C is a finite abelian group. Suppose that all but a finite amount of ϵ_p's are unramified. Then there exists a unique $\epsilon : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to C$ such that for all p $\epsilon(I_p) = \epsilon_p(I_p)$.*

Proof. If we had a field E with some desired properties, by defining $\epsilon : G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(E/\mathbb{Q}) \longrightarrow C$ we would be done. The main restriction is the fact that we have an infinite amount of

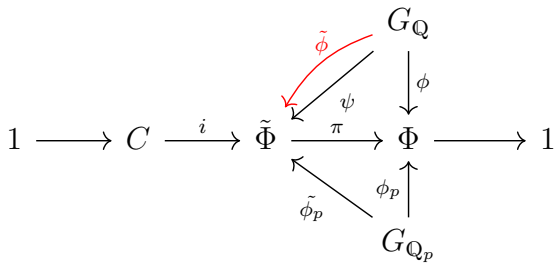
ϵ_p's. We will show that by sticking only with a finite amount of them the loss of information does not prevent us from defining ϵ. For every ϵ_p consider the map $\epsilon'_p := \rho \circ r_p|_{\mathbb{Z}_p}$:



Where r_p is the reciprocity map. With this construction, bridging through the abelian subgroup of the diagram, the association is ensured not to be ill defined. Now consider the map $\epsilon' : \prod \mathbb{Z}_p^* \longrightarrow C$ where $\epsilon'(u_p) := \prod \epsilon'_p(u_p)$. Now we claim that $\epsilon'_p(u_p)$ is trivial when p is unramified. Indeed, as it can be shown that $r_p(\mathbb{Z}_p^*) \cong \mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p^U) \cong I_p$ as the inertia degree is multiplicative and over the unramified subextension it is trivial, the result follows immediately. Then our ϵ' is a finite product of nontrivial p-adic integers for p ramified and hence finite. We will check that $\epsilon'(\prod_{p \text{ ramified}}(1 + p^{m_p}\mathbb{Z}_p^*))$ is trivial where m_p is the smallest integer n such that $1 + p^n\mathbb{Z}_p \subseteq \ker(\epsilon'_p)$. Once this fact is established, our previously defined ϵ' can be regarded as a map from $\prod \mathbb{Z}/p_p^m\mathbb{Z} \longrightarrow C$. And as mentioned in the beggining, the field E will in particular be the cyclotomic field whose Galois group over the rationals is $\mathbb{Z}/p^{m_p}\mathbb{Z}$ and it will naturally induce a morphism ϵ that satisfies $\epsilon_p(I_p) = \epsilon(I_p)$ for all p. Some details of the proof have been omitted, some of which are crucial to see that there is no loss of generality at every step taken but incur to class field theory. For a detailed proof, a sketch of whose this one is, refer to [MAS] p.36. □

The next result could easily be called a corollary of the previous lemma, nevertheless because of its importance in this section the term proposition is preferred.

Proposition 27. *Consider the following diagram:*



Where ϕ is a continuous homomorphism, $\phi_p = \phi|_{D_p}$ and the maps $\tilde{\phi}_p$ are all but a finite amount unramified. Then, under these hypotheses, there exists a unique lifting $\tilde{\phi} : G_{\mathbb{Q}} \to \tilde{\Phi}$ such that for every p $\tilde{\phi}(I_p) = \tilde{\phi}_p(I_p)$.

Proof. In the statement the morphisms from $G_{\mathbb{Q}_p}$ are taken to be the restriction of the ones parting from $G_{\mathbb{Q}}$ and so are the associated liftings. Now consider another homomorphism $\varphi_p : G_{\mathbb{Q}_p} \to \tilde{\Phi}$ which is another lifting of the restriction of ϕ localized, we take it to be unramified for all but a finite amount of p. That is, $\pi\varphi_p = \phi_p = \pi\tilde{\phi}_p$. As mentioned, there is

a strong relation with the preceding lemma and thereby we would want to construct a map from $\tilde{\Phi}$ to C. Note that $C \simeq i(C) = \ker(\pi)$ and $\varphi_p - \tilde{\phi}_p \in \ker(\pi)$. Then defining ϵ_p as:

$$\begin{aligned} \epsilon_p : \tilde{\Phi} &\longrightarrow C \\ \sigma &\longmapsto \epsilon_p(\sigma) = \varphi_p(\sigma) - \tilde{\phi}_p(\sigma) \end{aligned}$$

we have that by construction all but a finite amount of these homomorphisms are unramified and then by the lemma there exists a unique ϵ for which $\epsilon(I_p) = \epsilon_p(I_p)$. As we want $\tilde{\phi}(I_p) = \tilde{\phi}_p(I_p)$ and we have $\tilde{\phi}_p|_{I_p} = \epsilon_p|_{I_p} + \varphi_p|_{I_p} = \epsilon|_{I_p} + \psi|_{I_p}$, by ϵ's uniqueness, there is a unique $\tilde{\phi}$, $\tilde{\phi} = \epsilon + \psi$ that coincides with the localized $\tilde{\phi}_p$ in the inertia groups for all p. □

Corollary 2. *With the same hypotheses, a lifting $\tilde{\phi}$ can be chosen unramified at every prime where ϕ is unramified.*

Proof. The local version of this result was used in the first step where we chose a lifting $\tilde{\phi}_p$ of ϕ unramified where ϕ was. Now using the recently presented results, we can find a $\tilde{\phi}$ such that $\tilde{\phi}(I_p) = \tilde{\phi}_p(I_p)$ and since the behaviour over the inertia group totally determines where the maps ramify we get that ϕ and $\tilde{\phi}$ are ramified at the same places. □

It was a must for us to control the amount of ramified primes in the constructed extension $\tilde{L}$ since checking Scholz's condition would have rendered impossible otherwise. At this point we have an extension $\tilde{L}$ of L whose Galois group over $\mathbb{Q}$ is $\tilde{G}$, for which the diagram of the statement is commutative and ramified at the same places as L, nevertheless it will often fail to satisfy Scholz's condition.

5.2.3 Step III: Satisfying Scholz's condition

In the previous section we managed to tune $\tilde{L}$ in such a maneer that we could guarantee that the ramified primes were the same as those in L. Since L by the inductive hypothesis satisfies S_N we have that the first condition is immediately satisfied everywhere, i.e. for every ramified prime p in $\tilde{L}$ $p \equiv 1 \pmod{\ell^N}$. What is left to check is Scholz's second condition. Letting p be a ramified prime in $\tilde{L}$ a priori the relation between the inertia and decomposition subgroups of the in-between group of the extension of G by C_ℓ satisfy:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_\ell & \xrightarrow{\quad i \quad} & \tilde{G} & \xrightarrow{\quad \pi \quad} & G & \longrightarrow & 1 \\ & & & & \big| & & \big| & & \\ & & & & I'_p = \pi^{-1}(I_p) & & D_p & & \\ & & & & \big| & & \big\| & & \\ & & & & \tilde{D}_p & & I_p & & \\ & & & & \big| & & & & \\ & & & & \tilde{I}_p & & & & \end{array}$$

Where the chain of inclusions is $\tilde{I}_p \subseteq \tilde{D}_p \subseteq I'_p$ and $I_p = D_p$. The equality is again thanks to the fact that S_N is satisfied in L. Using this fact again we can claim that I_p is cyclic since $\ell \nmid p$ and as a consequence p is tamely ramified. We observe that I'_p is an extension of I_p by either 1 or C_ℓ. In the first case the preimage of I_p and D_p coincide and as a consequence the inclusions become equality and $\tilde{D}_p = \tilde{I}_p$ while in the second there are two more cases to examine. Since I'_p is an extension of I_p by C_ℓ it can either split or not split.

If it does not split and the order of I'_p is the same as that of I_p we again have a chain of equality as desired. Otherwise, if I'_p is a jump of degree ℓ, then we argue by the counter-reciprocal supposing that $\tilde{I}_p \subsetneq \tilde{D}_p$. In that case $i(C_\ell) \cap \tilde{I}_p = \varnothing$ and $\pi(i(C_\ell) \times \tilde{I}_p) \subseteq I_p$ and hence $i(C_\ell) \times \tilde{I}_p \subseteq I'_p$ and by cardinality the last expression is an equality yielding that I'_p is a split extension of I_p by C_ℓ which is a contradiction coming from the assumption that $\tilde{I}_p \subsetneq \tilde{D}_p$ hence the second Scholz condition for $\tilde{L}$ holds if the extension does not split. Further has been seen here, namely if the ℓ jump occurs from I_p to $\tilde{I}_p$ the second condition immediately holds. Thereby without loss of generality we will from now assume that $I_p \cong \tilde{I}_p$.

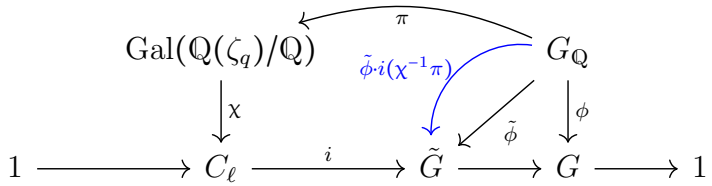
Should it split, we would have that $I'_p = \tilde{I}_p \times C_\ell$. Consider now $S = \{p \in \mathrm{ram}(L/\mathbb{Q}) : I'_p = \tilde{I}_p \times C_\ell\}$. We would like to show that $\tilde{D}_p/\tilde{I}_p$ can be trivial. If it is trivial already we are done. Otherwise, since at most the degree $[\tilde{D}_p : \tilde{I}_p]$ is ℓ we consider it to be a C_ℓ and we can associate $\mathrm{Frob}_p \in \tilde{D}_p/\tilde{I}_p$ to a generator c_p of the C_ℓ of the group extension.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_\ell & \longrightarrow & I'_p \cong C_\ell \times \tilde{I}_p \cong \tilde{D}_p/\tilde{I}_p \times \tilde{I}_p & \longrightarrow & I_p & \longrightarrow & 1 \\ & & c_p & \mapsto & & & \mathrm{Frob}_p & & \end{array}$$

It suffices to prove that by modifying the extensions the c_p can be trivial for all $p \in S$ since then the Frobenius will be trivial as well. Suppose now that there are some c_p's that are not trivial, then we need to further modify our extension. As was thoroughly discussed in the last section, talking about a particular extension is the same as restricting ourselves to a lift $\tilde{\phi}$. We thereby intend to modify $\tilde{\phi}$ in such a way that all c_p are 1. This procedure is very similar to the one followed in the construction of M_λ in the split case. We want to find a certain prime q satisfying a set of properties, we will see how these properties translate in terms of the associated fields and then we will argue by the same principle that was used before that such a prime q always exists. More particularly, we would like to find a prime q for which a map $\chi : \left(\mathbb{Z}/q\mathbb{Z}\right)^* \twoheadrightarrow C_\ell$ satisfying the following conditions exists.

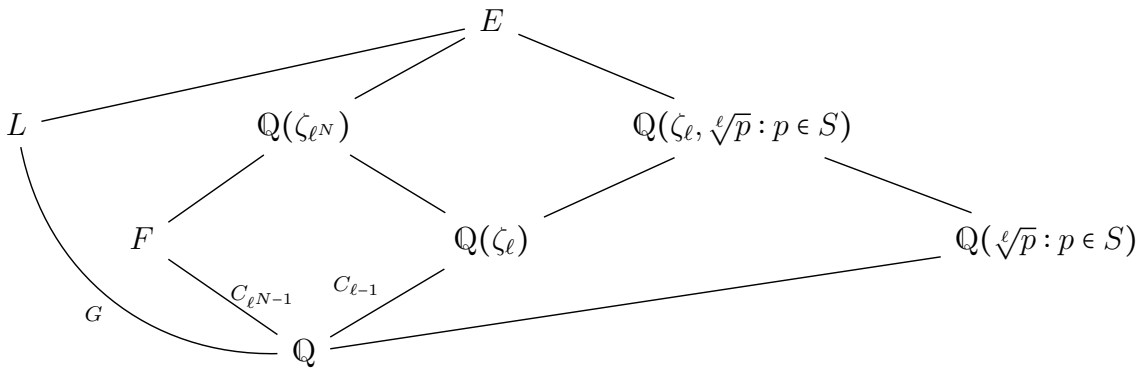
- $q \equiv 1 \pmod{\ell^N}$
- $\forall p \in S \quad \chi(p) = c_p$
- q splits completely in $L/\mathbb{Q}$

The motivation behind these properties is that if we were able to pick such a prime q, then defining $\chi(x) := x^{\frac{q-1}{\ell}}$ we would get an additional solution to the embedding problem, coexisting with $\tilde{\phi}$ with preferable and more suitable properties. Namely the equality of the inertia and decomposition subgroups at all ramifying primes. This lift is portrayed below.



Having seen the end goal, the left to prove facts are that this construction is always possible, much like in the previous' section fashion, establish that infinitely many of such q exist, and that S_N holds in this newly introduced extension. Note that as discussed in the embedding problem section, any lift is a shift of a base one, ϕ in this case, provided the extension is non-split yet this particular one need not exist a priori.

To assess the existence of such a q, we will see that q is of a particular type of unramified primes in a certain subfield compositum of E. Which will ultimately translate in its existence.



Where F is taken to be a ℓ^{N-1} cyclic extension of $\mathbb{Q}$ totally ramified in ℓ. The decomposition of the cyclotomic field $\mathbb{Q}(\zeta_{\ell^N})$ into this two factors is possible thanks to the decomposition at a group level. That is, since the multiplicative group of a prime power different from two behaves as portrayed, the fields follow the same behaviour. In particular if ℓ is odd, $\left(\mathbb{Z}/\ell^N\mathbb{Z}\right)^* \cong \mathbb{Z}/\ell^{N-1}\mathbb{Z} \times \mathbb{Z}/(\ell-1)\mathbb{Z}$ and the group structure is inherited in the fields.
The next lemma in itself has no particular importance but will render useful when describing the types of ramification q experiences over the different fields.

Lemma 12. *The fields L, F and $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p} : p \in S)$ are linearly disjoint over $\mathbb{Q}$.*

Proof. As we saw in the preliminaries, pairs of fields that split completely and ramified at a given prime are necessarily disjoint over the base field, in this case $\mathbb{Q}$. Take the behaviour of ℓ for instance, it is totally ramified in F since F is a subfield of $\mathbb{Q}(\ell^N)$ but ℓ is unramified in L yielding that L and F are disjoint. Now we would like to analyze their interplay with $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p} : p \in S)$, knowing that L and F are disjoint, saying that the three do not intersect is the same as saying that $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p} : p \in S)$ does not intersect LF. Since p_i is unramified in $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p} : p \in S, p \neq p_i)$ and p_i ramifies in LF and we can do this for every i, our three fields will be disjoint if and only if LF and $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p_i})$ are disjoint $\forall i$. Now note that any

subfield of LF of degree ℓ over $\mathbb{Q}$ will be Galois since the corresponding subgroup will be normal. Indeed, if $K \subseteq LF$ is such that $[K:\mathbb{Q}] = \ell$ then $K = LF^{\mathrm{Gal}(LF/K)}$ and $\mathrm{Gal}(LF/K)$ is a subgroup of $\mathrm{Gal}(LF/\mathbb{Q})$ of index the least prime dividing the order of the group hence normal forcing $\mathrm{Gal}(LF/K)$ to be normal and hence K Galois over the rationals. But any subfield of degree ℓ of $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p_i})$ fails to be Galois and since they can only potentially intersect in a field of degree ℓ we reach the desired claim. The three initial fields are disjoint over the rationals. □

Suppose now that $S = \{p_1, \cdots, p_k\}$ is ordered in such a way that c_{p_1} is not trivial, then since all c_{p_i} lie in C_ℓ, a set of integers $\{n_1, \cdots, n_k\}$ exists for which $c_{p_1}^{n_i} = c_{p_i}$.

Field	Behaviour of q	$x \mapsto x^q \quad \in \tilde{D}_p/\tilde{I}_p$
L	Splits completely	1
F	Splits completely	1
$\mathbb{Q}(\zeta_{\ell^N})$	Splits completely	1
$\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p} : p \in S)$	Unramified	$\neq 1$

We motivated the study of the behaviour of q in these fields with the pursuit of its existence. The resemblance with the split case, even if large is not total. That is, in the previous case we argued by saying how infinitely many completely splitting primes coexisted in any given number field whereas here q need not split completely in the compositum $LF\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p} : p \in S)$. Nevertheless, thanks to the previous lemma according to which the groups of the composition are in direct product and the analysis on the Frobenius morphism, we can establish q's existence using Chebotarev's density theorem. Even if we will not delve into too much detail, further explanation on this result is provided after the end of the proof. Essentialy the theorem applied to this setup goes to say that the set of unramified primes in $LF\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p} : p \in S)$ whose Frobenius conjugacy class, seen within a subset of $\mathrm{Gal}(LF\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p} : p \in S)/\mathbb{Q})$ has non-trivial density over the total number of primes. More particularly, the density will be the ratio of the conjugacy class with respect to the total group.

Summing up, since q is unramified in this extension, see table above, and its frobenius map $x \mapsto x^q$ uniquely defines a class in $\mathrm{Gal}(LF\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p} : p \in S)/\mathbb{Q})$ we can ensure infinitely many such q will exist in the chosen field extension.

As depicted above, letting $\tilde{\phi} \cdot \chi^{-1}$ be the new lift of ϕ, we have that the already ramified primes in L will still be congruent to 1 modulo ℓ^N and the inertia and decomposition groups, whose degree of difference is controlled by c_{p_i}, will be equal by construction, i.e. $\chi(p_i) = c_{p_i}$ and considering now the associated $\tilde{c}_{p_i} \in C_\ell$, they will all be $\tilde{c}_{p_i} = c_{p_i} \cdot c_{p_i}^{-1} = 1$ yielding equality of $\tilde{D}_p$ and $\tilde{I}_p$ for all p. This is not exhaustive yet as new primes could potentially have added repeated factors in $\tilde{L}$, i.e. the set S could have been enlarged. Thankfully only one more prime can be added to the list by the steps taken, namely q. Since the first condition is the same as Scholz's only the second one is left to be proved.

Using one of the last lemmas from the split case, the one that guaranteed the residual degree f to be 1 provided our congruence holds, we see that $|D_{\mathfrak{v}/q}| = e_{\mathfrak{v}/\mathfrak{P}}|D_{\mathfrak{P}/\mathfrak{q}}|$ for primes $\mathfrak{v} \in \tilde{L}$ and $\mathfrak{P} \in L$ above q. That being said, as q did not ramify in $\tilde{L}$ by construction, $\tilde{\phi}(D_{\mathfrak{v}})$ is trivial and then in the shifted extension one has that $\tilde{\phi} \cdot \chi^{-1}(D_{\mathfrak{v}}) = 1 \cdot \chi^{-1}(D_{\mathfrak{v}}) \subseteq i(C_\ell)$ and since the congruence forces $\chi^{-1}(I_{\mathfrak{v}}) = i(C_\ell)$ then we get the much desired equality ensuring the second Scholz's condition to be held in every ramifying prime of the induced extension by the new lift.

5.3 Obviated topics

For lack of a better term we group here some of the instances in which we took something for granted or the arguments got blurry.

One inflection point occurred when we assumed the restriction $\mathfrak{R} : H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), C_\ell) \to \prod_p H^2(\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p), C_\ell)$ to be injective and so effortlessly bridged from the global case to the local one. This is in fact a deep result which involves the associated Brauer group of the number field and then relies on the Brauer-Hasse-Noether theorem.

Another non-trivial result we failed to provide a detailed proof for was the Chebotarev density theorem. To modify the lift that later defined our extension so that it satisfied Scholz's conditions, we wished to encounter a particular prime q whose existence happened to be tightly underpinned to its stability, or the stability of the subgroup generated by its Frobenius map in the Galois group of a number field. This tightness yielded the use of Chebotarev necessary. Formally, and not vaguely as it was explained in the proof, the theorem states that:

Theorem 9. *Let L/K be a Galois extension over a number field with $\mathrm{Gal}(L/K) = G$ then the unramified primes whose Frobeniuses belong to a certain conjugation class $C \subseteq G$ have density $\frac{|C|}{|G|}$.*

A paper in which both the classical proof due to Chebotarev, a more recent one by Lagarias and Odlyzko and applications of this theorem are presented can be found in [TRI]. The density the statement refers to is:

Definition 17. *If A is a subset of the prime numbers of a larger set then the Dirichlet density of A is defined as $\delta(A) := \lim_{s\to 1^+} \frac{\sum_{p\in A} \frac{1}{p^s}}{\sum_p \frac{1}{p^s}}$.*

The density in the theorem can be thought of as the natural density as a semi-equivalence between the two exists. Besides the infiniteness of the splitting primes which was used during the proof, an important consequence of the theorem is that classifying Galois extensions of a fixed number field is the same as describing the splitting of the primes. We had a glimpse of this result previously where we handcrafted a proof to see that if a prime p had a particular different behaviour in L/K and in L'/K then $L \ncong L'$. More particularly Chebotarev has as a corolary that any extension of a fixed number field is uniquely determined by the primes that split completely[8].

We also anticipated and believed that saying that a particular embedding problem had a positive solution was not an empty statement. For $\ell = 2$ there is already a very simple instance in which the embedding problem may not have a solution.

Proposition 28. *The embedding problem for $\mathbb{Z}/4\mathbb{Z} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$ has solution if and only if a is the sum of two squares in $\mathbb{Z}$.*

[8] Corollary VII.13.10 in [NEU1].

The previous result was seen in the Galois theory course and interestingly enough it is mentioned in the very second page of [SCH]. They say that: "although we did not put local conditions, there might be a global arithmetic obstruction to the existence of our embedding problem".

Besides some obvious obstructions we drew attention to during the proof, the case $\ell = 2$ is of particularly greater difficulty, as in many number theoretic topics, since in this case the ℓ-th roots are in $\mathbb{Q}$. Arguments like the construction of E in the last step to check the existence of q wouldn't have been feasible, lemma 12 fails to hold if ℓ is allowed to be 2. In [MIC] groups of order 32 are realized as Galois groups using embedding problems with kernels of order 2 and 4. Even if it does not directly relate to our work, it can help to get rid of the preconceived fear towards $\ell = 2$.

Finally, in the beginning of the non-split case we stressed that it was not a generalization of the split one. Indeed, among others, when we were solving the local embedding problem and said that no generator of the C_ℓ we were considering the extension by was a generator of $\tilde{G}_p$ we were implicitly using the fact that the extension was non-split. This was a key moment as we could then use Frattini properties not available in the split case to solve the local embedding problem.

6 Consequences

The main aftermath of this theorem is not the mere veracity of its statement. The method presented here has given birth to many approaches both in considering general groups and to realize particular ones as Galois groups. We anticipated that Scholz-Reichardt could be used to regard any nilpotent odd group as a Galois group. Indeed, by one of the first equivalences regarding nilpotent groups, any nilpotent group G is the direct product of its Sylow subgroups, i.e. $G \cong K_1 \times \cdots \times K_r$ where the K_i's are p-groups with different p's. If additionally they are all odd we can apply Scholz-Reichardt to each and every one of them associating $L_i/\mathbb{Q}$ to K_i and finally $\mathrm{Gal}(L_1 \cdots L_r/\mathbb{Q}) \cong G$ since they are all disjoint.

Even if the celebrated Shafarevich theorem that we mentioned in the beginning uses a different set of tools, there is a nice way to reach such a powerful result. Should this theorem hold for the prime $\ell = 2$, (which we know for a fact it does but we haven't proved) then the concatenation of three results can lead to the realization of arbitrary solvable groups as Galois groups over $\mathbb{Q}$. Namely applying Scholz-Reichardt, Ore and a result from Ishanov. In what follows we will briefly discuss those. Interestingly enough a mistake was comitted regarding the prime $\ell = 2$ in Ishanov's case as well. A consequence of our previous work on the Frattini subgroups allows us to establish the next theorem.

Theorem 10. *For a finite solvable group G there exists a nilpotent normal subgroup H and a proper subgroup M such that $G = HM$.*

Proof. A detailed proof can be found in p.170 of [NEU]. If $\pi : G \to G/\Phi(G)$ and K is a normal nilpotent subgroup of $G/\Phi(G)$[9]. Then letting H be $\pi^{-1}(K)$ and M be a maximal subgroup that does not contain H we are done. □

The theorem by Ishanov states that the semidirect product $N \rtimes G$ where G is a Galois group and N is a nilpotent group upon which G acts also happens to occur as Galois over any prescribed number field. A proof can be found in p.20 of [SCH]. This result is very strong, in particular setting G to be trivial it says that every nilpotent group occurs as a Galois group over the rationals, the conclusion of Scholz-Reichardt's theorem. As announced, we are now in conditions to formulate and provide a proof taking for granted the $\ell = 2$ case for the much celebrated Shafarevich theorem.

Theorem 11. *For any finite solvable group G there exists a field E such that* $\mathrm{Gal}(E/\mathbb{Q}) \cong G$.

Proof. As anticipated, a detailed proof can only be accomplished (by the means of this procedure) demonstrating the veracity for $\ell = 2$ as in [SHA] or [SCH]. Nevertheless in p.134 of [NEU] a similar one to the following is presented. We will argue by induction over the order of G. The base case being when G is trivial and immediately holds. While for the inductive step we use the preceding theorem according to which we have a decomposition like $G = HM$, H being a normal nilpotent proper subgroup and M being proper. The map $\phi : M \longrightarrow \mathrm{Aut}(H)$ defines an action, i.e. $\phi(m)(h) := mhm^{-1}$ for $m \in M$ and $h \in H$.

[9] The existence of which is guaranteed by the preliminaries.

Consider now the next diagram where $\nu(h, m) \coloneqq hm$

$$\begin{array}{ccccccccc} & & & & G & & & & \\ & & & & \uparrow{\scriptstyle \nu} & & & & \\ 1 & \longrightarrow & H & \longrightarrow & H \rtimes M & \longrightarrow & M & \longrightarrow & 1 \end{array}$$

By the inductive hypothesis, as M is proper in G, there exists a field $F/\mathbb{Q}$ whose group is M. And now arguing by the theorem which guaranteed the solvability of the semidirect embedding problem with nilpotent kernel, there is a proper solution L. Then the field $L^{\ker(\nu)}$ has Galois group isomorphic to G as desired. $\square$

7 Particular examples

A good grasp of the interplay the different elements in the proof play is acquired when looking at particular examples. We will first examine, just like in the demonstration, the split case.
Let $\mathfrak{G} = C_7 \times C_7$ be the p-group whose Galois extension over $\mathbb{Q}$ we want to find. Then, as depicted in the constructive proof, after solving the base case we only have to solve the following embedding problem:

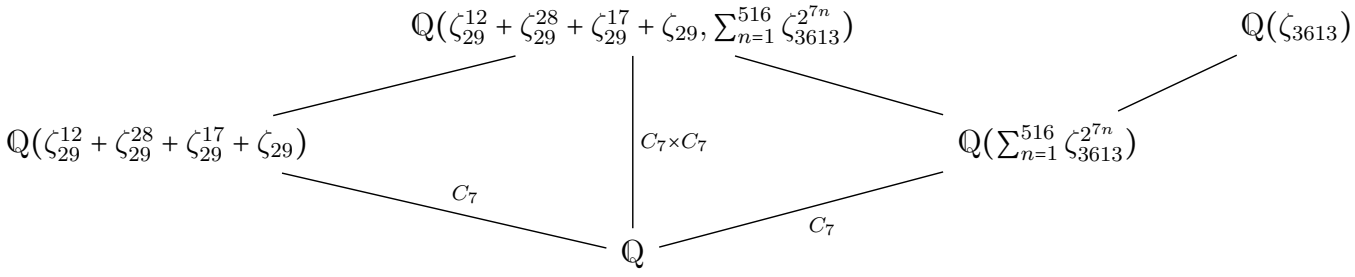
$$1 \longrightarrow C_7 \xrightarrow{i} C_7 \times C_7 \xrightarrow{\pi} C_7 \longrightarrow 1$$

Since 29 is prime $\mathrm{Gal}(\mathbb{Q}(\zeta_{29})/\mathbb{Q})$ has 28 elements and there will necessarily be a subfield whose group over $\mathbb{Q}$ is C_7. To find the desired cyclic subgroup of order 4 note that the map sending ζ_{29} to ζ_{29}^3 generates $\mathrm{Gal}(\mathbb{Q}(\zeta_{29})/\mathbb{Q})$ and consequently an element of order 4 will simply be a map sending ζ_{29} to $\zeta_{29}^{3^7} = \zeta_{29}^{12}$. Henceforth the fixed field of $\mathbb{Q}(\zeta_{29})$ by this subgroup is $\mathbb{Q}(\zeta_{29}^{3^7} + \zeta_{29}^{3^{14}} + \zeta_{29}^{3^{21}} + \zeta_{29}^{3^{28}}) = \mathbb{Q}(\zeta_{29}^{12} + \zeta_{29}^{28} + \zeta_{29}^{17} + \zeta_{29})$. Computing its minimal polynomial[10] yields that, if we denote $\zeta_{29}^{12} + \zeta_{29}^{28} + \zeta_{29}^{17} + \zeta_{29}$ by α, then $\mathrm{Irr}(\alpha, \mathbb{Q}; x) = x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1$ and its discriminant is $171903939769 = 17^2 29^6$, nevertheless this is not the discriminant we have been referring to but rather the polynomial's one, the number ring discriminant over $\mathbb{Z}$ is $594823321 = 29^6$. To further distinguish the primes 29 and 17, we regard $\mathrm{Irr}(\alpha, \mathbb{Q}; x) = (x+25)^7 \pmod{29}$ and $\mathrm{Irr}(\alpha, \mathbb{Q}; x) = (x+3)^2(x+9)(x+11)(x+13)(x+14)(x+16) \pmod{17}$ yielding two completely different types of factorizations.
To check Scholz's condition it suffices to see that $29 \equiv 1 \pmod{7^1}$ and that for any prime $\mathfrak{v}$ over 29 $I_{\mathfrak{v}} = D_{\mathfrak{v}}$. The first condition is immediately satisfied and the second follows from the fact that $e_{\mathfrak{v}/29} f_{\mathfrak{v}/29} g_{29} = 7$ and $e_{\mathfrak{v}/29} > 1$.

Solving the embedding problems means finding an extension of $\mathbb{Q}(\zeta_{29}^{12} + \zeta_{29}^{28} + \zeta_{29}^{17} + \zeta_{29})$ with group $C_7 \times C_7$ over $\mathbb{Q}$ satisfying S_N's condition[11]. Following the steps of the proof we wish to encounter a prime q congruent to 1 modulo 7, splitting completely over $\mathbb{Q}(\alpha)$ and being such that 29 is a 7-th power in $\mathbb{F}_q$. Filtering the integers according to the first and then applying the other conditions we see that 29 ramifies and hence cannot split completely, most have no solution for $29 \equiv x^7 \pmod{q}$ and others like 421 have solutions, 202 for instance, but fail to split completely, $f_{\mathfrak{v}/421} = 7 \quad \forall \mathfrak{v}$. A prime which satisfies the 3 conditions is 3613 since $3613 = 516 \cdot 7 + 1$, $29 \equiv 136^7 \pmod{3613}$ and $\mathrm{Irr}(\alpha, \mathbb{Q}; x) = (x + 1279)(x + 1756)(x + 2356)(x + 2830)(x + 2943)(x + 3366)(x + 3536) \pmod{3613}$. Now proceeding analogously to the proof, we take $\lambda : \left(\mathbb{Z}/3613\mathbb{Z}\right)^* \to C_7$ defined as the natural projection and consider $M_\lambda = \mathbb{Q}(\zeta_{3613})^{\ker(\lambda)}$. Since the map sending ζ_{3613} to ζ_{3613}^2 generates $\mathrm{Gal}(\mathbb{Q}(\zeta_{3613})/\mathbb{Q})$ we have that $M_\lambda = \mathbb{Q}(\sum_{n=1}^{516} \zeta_{3613}^{2^{7n}})$ and the field extension is as depicted, the compositum.

[10] Interestingly the same one appears in this post.

[11] Where here N is a multiple of 1, i.e. saying nothing, since the least common multiple of the degrees of the elements of C_7 is already 7.



With mathematical software the irreducible polynomial of the previous $C_7 \times C_7$ extension has been found but for prime powers larger than two finding it would render a much more challenging task. If we were to continue, building a $C_7 \times C_7 \times C_7$ extension would consist in finding a prime q such that $q \equiv 1 \pmod 7$, $x^7 \equiv 29 \pmod q$ and $y^7 \equiv 3613 \pmod q$ allowed solutions and furthermore, that it splited completely in the previously constructed field. Since $644687 = 92098 \cdot 7 + 1$, $28212^7 = 29 \pmod{644687}$, $131152^7 = 3613 \pmod{644687}$ and the 49th degree polynomial of $\zeta_{29}^{12}+\zeta_{29}^{28}+\zeta_{29}^{17}+\zeta_{29}+\sum_{n=1}^{516}\zeta_{3613}^{2^{7n}}$ splits in 49 factors, by Kummer's correspondence theorem we have its complete split guaranteed. This process of finding such primes, constructing the map and then the associated field extension can always be done for split extensions as was portrayed in the proof. Hopefully the split case is by now fully understood. It goes without saying that this procedure can be mimicked for any prime ℓ taken at first and any intermediate field extension taken as the base one.

In a general scenario to reach the desired extension the procedure will most likely involve solving problems from both types, split and non-split. No non-split example is explained as the constructive mechanisms cease the moment we incur the local-global principle and consider group extensions of the global Galois group. The existence arguments allow for a technical proof to be carried away at the expense of losing interpretability.

One should bear in mind that these are by no means the only steps we could have taken. A first choice is made when the central series for the group is picked compounded with the chosen representations and later some may collide because they may yield equivalent extensions. An interesting viewpoint would be that of focusing on how many ways there are to reach a particular group G following the steps of our proof. Arguments of counting and pruning the "tree" described by the proof are main topics of research nowadays. One may wish to find the extension satisfying a particular property or the number of such extensions. By far the most discussed is the least ramified, we have used the fact that at each step one more prime can be added to our bag of ramified primes nevertheless we do not care when or how this occurs. More about that will be presented in the final section.

Another important thing to bear in mind is that this procedure is not very efficient if we do not require the field extension to be buildable upon. We had to use mathematical software to compute a $C_7 \times C_7$ group following the steps of the proof nevertheless if our goal was merely that extension it could have been computed directly as the compositum of two mutually disjoint restrictions of cyclotomic fields.

8 Open problems

By now we hope the reader has gotten acquainted to both the general inverse Galois problem and the particular case of Scholz-Reichardt. By no means this is the state of the art of the matter, this result dates back to 1937 and major advances have been made on this field since. Maybe the big appeal and one of the driving motifs to thoroughly examine this proof is the fact that the general case is still a conjecture. Furthermore, simpler and more particular group associations are still open, for instance whether the group M_{23}[12] occurs as Galois over $\mathbb{Q}$ is unknown. The beauty behind most of this problems, as in mathematics in general, resides is the rather easy and simplistic way they can be formulated and yet their truthfulness renders very challenging to demonstrate. In this last section, much like in the first, a contextualization of where this thesis could lead us as a starting point looking forward is presented.

In one of the examples a note on the constraints upon the number of ramifying primes was made. More precisely an open problem is: given a set S of prime numbers and a group G, find a field over the rationals whose Galois group is G and ramified only at primes inside of S. This may look like a non-relevant twist at first but apparently procedures like this may eventually help to shed some light into the classic inverse problem. Another scenario where one restricts himself to considering only tamely ramified extensions of the rationals was proved for some groups in [PLA].

At the very beginning a possibility to attack the main problem with brute force was mentioned. In this thesis we have examined the solvability of central embedding problems with cyclic kernel of prime order which is just one of the families of finite simple groups. An interesting and natural continuation would go along the lines of analyzing how embedding problems with other prefixed finite simple groups as kernel relate to this one, moreover, when they are solvable. Hopefully this thesis works as a thorough enough gate opener to inquire those types of questions.

[12] A group in S_{23} with 10200960 elements. The rest of sporadic groups are known to be realisable as Galois groups, see [PAH] for instance.

References

[ADA] Damien Adams. *Galois theory and the Hilbert Irreducibility theorem.* Master's theses, San Jose State University. Spring 2013.

[AKH] Akhil Mathew. *Group Cohomology.* Notes on cohomology on Akhil's blog. 2009.

[CON1] Keith Conrad, *Groups of order p^3.* Expository papers on group theory.

[CON2] Keith Conrad, *Ostrowski's theorem for* $\mathbb{Q}$. Expository papers on algebraic number theory.

[CON3] Keith Conrad, *Discriminants and ramified primes.* Expository papers on algebraic number theory.

[CRA] David A. Craven. *The Theory of p-groups.* Lecture notes, Birmingham University. Hilary term 2008.

[CUL] Lucas Culler. *The Kronecker-Weber theorem.* REU papers 2007.

[FRO] Cassels and Frohlich, *Albegraic Number theory.* Thompson Book Company, Washington, D. C. 1967.

[HOE] Klaus Hoechsmann. Journal für die reine und angewandte Mathematik Volume: 229 p. 81-106, 1968.

[LAI] Johan Laine. *On p-groups of low power order.* Department of Mathematics KTH, 2010.

[MAS] Adam Massey, *The inverse Galois problem for nilpotent groups of odd order*, May 2006.

[MIC] Ivo M. Michailov, *Groups of order 32 as Galois groups.* Serdica Math. J. 33 p. 1-34, 2007.

[MM] Malle and Matzat, *Inverse Galois theory.* Springer Monographs in Mathematics, 1999.

[NEU] Jürgen Neukirch, *The embedding problem in Galois inverse problem.* AMS, 1997.

[NEU1] Jürgen Neukirch. *Algebraic Number Theory.* Springer 1999 . Grundlehren der mathematischen Wissenschaften's series.

[PAH] Herbert Pahlings, *Some sporadic groups as Galois groups.* Rendicoti del Seminario Matematico della Universita di Padova, Volume 79 p. 97-107, 1988.

[PLA] Bernat Plans, *Central Embedding Problems, the Arithmetic Lifting Property, and Tame Extensions of* $\mathbb{Q}$. International Mathematics Research Notices, 2003.

[ROQ] Peter Roquette. *On the embedding problem for global fields.* Comments to an old paper of Klaus Hoechsmann, August 27, 2003.

[SAI] Amin Saied, *The inverse Galois problem: The Rigidity Method.* Thesis in the Department of Mathematics, Imperial College London. June 24, 2011.

[SCH] Alexander Schmidt and Kay Wingberg. *Safarevic's Theorem on Solvable Groups as Galois Groups.*

[SERR] Jean-Pierre Serre, *Topics in Galois theory.* Course at Harvard university fall 1988.

[SHA] Igor Shafarevich, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR Ser. Mat., Volume 18, Issue 6, 525–578, 1954.

[SONN] Jack Sonn. *On the embedding problem for nonsolvable Galois groups of algebraic number fields: Reduction theorems.* Journal of number theory 4 p. 411-436, 1972.

[STE] Shaun Stevens. *4A22 Local Fields.* Notes on the local fields course, Spring semester 2003.

[SUT] Andrew Sutherland. *The Minkowski bound and finiteness results.* Lecture notes 14 on number theory. Fall 2017.

[TRI] Nicholas George Triantafillou. *The Chebotarev density theorem.*

[TSI] Michael Tsiang. *Group extensions.* University of California, Math 195.

[VIL] Núria Vila. *On the inverse problem of Galois theory.* Publicacions Matemàtiques, Volume 36, Number 2 p. 1053-1073, 1992.

[VOL] Helmut Volklein. *Review of [MM].* Bulletin of the American Mathematical Society, Volume 38, Number 2 p. 235-243. December 27, 2000.