Quelques cas particuliers de la conjecture de modularité de Serre

Hanecart Valentin

2024

Table des matières

Introduction

Le 1er mai 1973, Jean-Pierre Serre envoya une lettre à John Tate dans laquelle il écrivit (entre autres !) la chose suivante (le lecteur intéressé pourra consulter [6] p.451 à 455) :

> Parlons plutôt de maths – les chances de s'y engueuler y sont nettement plus faibles ; j'ai envie de te raconter une conjecture sur les extensions galoisiennes de $\mathbb{Q}$ à groupe de Galois un sous-groupe de $\mathrm{GL}_2(\mathbb{F}_p)$:
>
> Je vais être prudent, et considérer uniquement des représentations
>
> $$\rho : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2\left(\mathbb{F}_q\right), \quad q = p^f,$$
>
> non ramifiées en dehors de p et vérifiant la condition suivante :
>
> $(*)$ $\det(\rho) : \mathrm{Gal} \longrightarrow \mathbb{F}_q^*$ est égal à χ^{k-1} (k pair)
>
> où $\chi : \mathrm{Gal} \longrightarrow \mathbb{F}_q^*$ est le caractère fondamental modulo p (donnant l'action sur μ_p).
> En fait, cette action équivaut à :
>
> $(**)$ L'image par ρ du Frobenius réel a pour valeurs propres $+1$ et -1 (*i.e.* $\det\rho$ est un caractère *impair*).

À la suite de cela, Jean-Pierre Serre énonça sa fameuse conjecture de modularité. Ce à quoi John Tate répondit (entre autres !) le 11 juin 1973 :

> Dear Serre,
> Your conjecture (or question if you want to be chicken) about modular representations of degree 2 of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ and modular forms is beautiful!

Autrement dit, si $\rho : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2\left(\mathbb{F}_q\right)$ est une représentation de degré 2 supposée irréductible et de déterminant impair, alors sa conjecture en question affirme que ρ est vraiment "modulaire", (c'est-à-dire qu'elle provient d'une forme modulaire parabolique modulo p qui est fonction propre des opérateurs de Hecke).

Dans sa lettre suivante du 2 juillet 1973, John Tate écrivit à Jean-Pierre Serre pour lui exposer sa solution du cas de la caractéristique 2 (dont il a eu l'intuition d'utiliser une estimation du discriminant) et cette idée a été développée beaucoup plus loin par Jean-Pierre Serre lors des années qui suivirent (le lecteur intéressé pourra consulter [5], p.179 à 230).

L'un des intérêts de cette conjecture est qu'elle fait le lien entre représentations et formes modulaires. Or, l'utilisation de formes modulaires est reliée à la notion de courbe elliptique et en particulier à la courbe de Frey qui est utilisée dans la preuve du théorème d'Andrew Wiles. On ne dit rien ici du contenu exact de ces théorèmes, encore moins de leurs preuves respectives. On se bornera à indiquer que l'étude des représentations du groupe $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ a joué un rôle clef dans cette histoire !

Notre but sera de donner une preuve de la conjecture de Serre dans le cas de la caractéristique 2,3 et 5. Pour cela, nous commencerons par donner dans une première partie des préliminaires sur des notions qui nous seront utiles dans les démonstrations (en particulier on ne démontrera pas ces résultats qui sont parfois très techniques), puis nous traiterons dans une deuxième partie du cas de la caractéristique 2 puis nous dirons un mot rapide sur le cas de la caractéristique 3 avant de finir par le cas de la caractéristique 5 dans une dernière partie.

I Préliminaires

Le but de cette première partie est de donner quelques outils permettant d'aborder les résultats démontrés plus loin. Les résultats donnés ici seront donc seulement énoncés.

I.1 Notion de groupe résoluble

On commence par parler de la notion de groupe résoluble en rappelant la définition et les premières propriétés, puis en donnant deux théorèmes importants que sont les théorèmes de Burnside et de Feit-Thompson et enfin on termine par quelques applications avec des résultats pratiques.

Dans toute cette sous-partie, on considère $(G, *)$ un groupe (noté simplement G par la suite) de neutre noté e_G.

I.1.1 Définitions et premières propriétés

Définition 1 : Groupe résoluble :
On dit que le groupe G est un **groupe résoluble** lorsqu'il existe une suite finie de sous-groupes :

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G \tag{1}$$

telle que :

* Pour tout $i \in [\![0; n-1]\!]$, G_i est un sous-groupe distingué de G_{i+1}.
* Pour tout $i \in [\![0; n-1]\!]$, G_{i+1}/G_i est un groupe abélien.

Exemple 1 :

* Tout groupe abélien est résoluble.
* Tout groupe cyclique est résoluble (car abélien).
* Le groupe symétrique $\mathfrak{S}_3$ est résoluble car possède un sous-groupe distingué engendré par le 3-cycle (1 2 3) dont le quotient est d'ordre 2 (donc abélien).
* Le groupe dihédral D_8 (d'ordre 8) est résoluble (en effet, il possède un sous-groupe cyclique S d'ordre 4 et le quotient D_8/S est un groupe d'ordre 2 et donc abélien).
* Le groupe symétrique $\mathfrak{S}_4$ est résoluble puisque l'on a :

  $$\left\{\mathrm{Id}_{[\![1;4]\!]}\right\} \lhd V_4 \lhd \mathfrak{A}_4 \lhd \mathfrak{S}_4$$

  où V_4 est le sous-groupe composé de $\mathrm{Id}_{[\![1;4]\!]}$, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3) et isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
* Les groupes $\mathfrak{S}_5$ et $\mathfrak{A}_5$ ne sont pas résolubles.
* Le groupe des quaternions est résoluble. En effet, on a :

  $$\mathbb{H}_8 := \{1, -1, i, -i, j, -j, k, -k\} \text{ et } i^2 = j^2 = k^2 = i \times j \times k = -1.$$

  Donc $< k >:= \{1, k, -1, -k\}$ est un sous-groupe distingué de $\mathbb{H}_8$ (car d'indice 2) et $\mathbb{H}_8/ < k >$ est un groupe d'ordre 2 (donc abélien). De plus, $< k >$ est un sous-groupe abélien, et donc $< k > /\{1_{\mathbb{H}_8}\} \cong < k >$ est aussi un groupe abélien.

Nous donnons maintenant les premiers résultats sur les groupes résolubles :

Proposition 1 :
Soient H un sous-groupe de G et N un sous-groupe distingué de G.

* Si G est résoluble, alors H est résoluble.
* Si G est résoluble, alors G/N est résoluble.

Remarque :
Par le premier théorème d'isomorphisme, le deuxième point de la proposition précédent est équivalent au fait que s'il existe un morphisme de groupes surjectif d'un groupe résoluble P dans G, alors G est résoluble.

Proposition 2 :
Soit N un sous-groupe distingué de G.
Si N et G/N sont résolubles, alors G est résoluble.

Remarque :
On peut remarquer que les deux propositions précédentes nous donnent l'équivalence :

$$(N \text{ et } G/N \text{ son résolubles}) \iff (G \text{ est résoluble}).$$

Corollaire 1 :
Si G n'est pas simple et que tout groupe d'ordre strictement inférieur à $\mathrm{Card}(G)$ est résoluble, alors G est résoluble.

I.1.2 Théorèmes de Burnside et de Feit-Thompson

Dans ce paragraphe, on énonce le théorème $p^a q^b$ de Burnside (tout groupe fini ayant au plus deux facteurs premiers distincts est résoluble) et le théorème de Feit-Thompson (tout groupe fini d'ordre impair est résoluble).

Commençons par le cas particulier suivant :

Proposition 3 :
Soit p un nombre premier.
Tout p-groupe est résoluble.

Donnons maintenant le théorème de Burnside :
Ce résultat étend les travaux de Camille Jordan publiés en 1898 (qui eux-mêmes viennent des travaux de Georg Frobenius sur le même sujet). Le théorème de Burnside utilise la théorie des représentations et exploite les propriétés des anneaux d'entiers de certains corps de nombres (même si certaines démonstrations n'utilisent pas la théorie des représentations).

Théorème 1 : Théorème de Burnside (1904) :
Soient p, q deux nombres premiers et a, b deux entiers naturels.
Si G est un groupe fini d'ordre $p^a q^b$, alors G est résoluble.

Remarque :
Le théorème de Burnside n'admet pas d'extension lorsque le cardinal de G admet au moins 3 facteurs premiers distincts. En effet, $\mathfrak{A}_5$ (de cardinal $60 = 2^2 \times 3 \times 5$) n'est pas résoluble (comme on le dira un peu plus bas).

Nous terminons ce paragraphe par le théorème de Feit-Thompson :
William Burnside conjectura en 1911 que tout groupe simple fini non abélien est d'ordre pair, ce qui est équivalent au fait que tout groupe fini d'ordre impair est résoluble (ce que Feit et Thompson prouvèrent en 1963).

Théorème 2 : Théorème de Feit-Thompson (1963) :
Tout groupe fini d'ordre impair est résoluble.

Remarque :
Le théorème en lui-même et de nombreuses méthodes introduites par Feit et Thompson dans leur preuve ont joué un rôle essentiel dans la classification des groupes simples finis. En outre, la preuve originale de Feit et Thompson, longue de plus de deux cent cinquante pages, a été simplifiée dans certains détails, mais elle n'a pas été considérablement raccourcie et sa structure générale n'a pas été modifiée.

I.1.3 Quelques applications

Définition 2 : Suite dérivée d'un groupe :
On appelle **suite dérivée de** G la suite $(D^n(G))_{n\in\mathbb{N}}$ définie par :

$$D^0(G) = G \text{ et } \forall n \in \mathbb{N},\ D^{n+1}(G) = D(D^n(G)).$$

On a alors une caractérisation d'un groupe résoluble par sa suite dérivée :

Théorème 3 : Caractérisation d'un groupe résoluble par sa suite dérivée :
G est un groupe résoluble si, et seulement si, sa suite dérivée est stationnaire à $\{e_G\}$.

On a alors le résultat suivant :

Corollaire 2 :
G est un groupe résoluble si, et seulement si, $D(G)$ est un groupe résoluble.

On termine ce paragraphe et cette partie avec l'étude du groupe symétrique $\mathfrak{S}_n$ et du groupe alterné $\mathfrak{A}_n$ pour un entier naturel $n \geq 5$.

On sait déjà que $\mathfrak{S}_3$ et $\mathfrak{S}_4$ sont résolubles d'après l'exemple 1 et donc, d'après la proposition 1, $\mathfrak{A}_3$ et $\mathfrak{A}_4$ sont également résolubles. Enfin, $\mathfrak{S}_1$, $\mathfrak{A}_1$, $\mathfrak{S}_2$ et $\mathfrak{A}_2$ sont résolubles car se sont des groupes abéliens (puisque leur cardinal est inférieur ou égal à 5).

Le théorème fondamental suivant est dû à Galois :

Théorème 4 :
Pour tout entier naturel $n \geq 5$, $\mathfrak{A}_n$ n'est pas un groupe résoluble.

On en déduit le corollaire suivant :

Corollaire 3 :
Pour tout entier naturel $n \geq 5$, $\mathfrak{S}_n$ n'est pas un groupe résoluble.

Remarque :
Ce résultat est très important car il est à la base de la théorie de la résolution des équations polynomiales par radicaux. En effet, c'est ce résultat qui montre que l'équation polynomiale générale de degré supérieur ou égal à 5 n'est pas résoluble par radicaux.

I.2 Théorème de la base de Burnside

On donne dans cette sous-partie un résultat qui nous sera utile lorsque l'on parlera des extensions galoisiennes non ramifiées en dehors de 5.

Dans toute cette sous-partie, on considère p un nombre premier et G un p-groupe.

Lemme 1 :
Tout sous-groupe maximal H de G est distingué et on a $G/H \cong \mathbb{Z}/p\mathbb{Z}$.

Théorème 5 : Théorème de la base de Burnside :
Les parties génératrices de G minimales (au sens de l'inclusion) ont toutes le même cardinal.

Remarques :

* Le preuve du théorème de la base de Burnside nous donne même une partie génératrice de G minimale. En effet, en notant $\Psi(G)$ le sous-groupe de Frattini de G (c'est-à-dire l'intersection de tous les sous-groupes maximaux de G), on a que $G/\Psi(G)$ a une structure de $\mathbb{F}_p$-espace vectoriel (car $G/\Psi(G)$ est abélien et de torsion p) de dimension finie notée d. Le $\mathbb{F}_p$-espace vectoriel $G/\Psi(G)$ possède donc une base notée $(\overline{x_1}, ..., \overline{x_d})$ et une partie génératrice de G minimale pour l'inclusion est donnée par $< x_1, ..., x_d >$.

∗ Le résultat n'est plus vrai lorsque le groupe G n'est plus un p-groupe. En effet, pour n un entier naturel supérieur ou égal à 4, $\mathfrak{S}_n$ est engendré de manière minimale par la famille $\{(1\ 2); (2\ 3); ...; (n-1\ n)\}$ et par la famille $\{(1\ 2\ 3\ ...\ n); (1\ 2)\}$...

I.3 Le théorème de Kronecker-Weber

On donne ici le théorème de Kronecker-Weber qui nous sera utile lors de l'étude des divers cas.

Théorème 6 : Théorème de Kronecker-Weber :
Toute extension abélienne finie de $\mathbb{Q}$ est incluse dans une extension cyclotomique.

Remarque :
La preuve du théorème consiste tout d'abord à restreindre les cas. En effet, comme le groupe de Galois d'une telle extension est abélien, par le théorème de structure des groupes abéliens, on peut se restreindre au cas où le groupe de Galois est un $\mathbb{Z}/p^m\mathbb{Z}$ (avec p un nombre premier et m un entier naturel non nul).
De plus, dans le cas $p = 2$, le théorème nous donne que toute extension abélienne de $\mathbb{Q}$ de degré 2^m telle que 2 soit le seul nombre premier ramifié est contenue dans l'extension cyclotomique $\mathbb{Q}\left(e^{\frac{2i\pi}{2^{m+2}}}\right)$. Enfin, pour le cas d'un nombre premier p impair, on a que si $\mathbb{K}$ est une extension abélienne de $\mathbb{Q}$ de degré p^m dans laquelle seul p se ramifie, alors $\mathbb{K}$ est l'unique sous-corps d'indice $p-1$ du p^{m+1}-ième corps cyclotomique.

I.4 Généralisations de l'hypothèse de Riemann

L'hypothèse de Riemann est l'une des plus importantes conjectures des mathématiques et concerne les zéros de la fonction ζ de Riemann. Divers objets géométriques et arithmétiques peuvent être décrits par ce que l'on appelle les fonctions L globales, qui sont similaires formellement à la fonction ζ de Riemann. On peut alors se poser la même question à propos des zéros de ces fonctions L, fournissant diverses généralisations de l'hypothèse de Riemann.

Les fonctions L globales peuvent être associées aux courbes elliptiques, aux corps de nombres (dans ce cas, elles sont appelées **fonctions ζ de Dedekind**) et aux caractères de Dirichlet (dans ce cas, elles sont appelées **fonctions L de Dirichlet**). Lorsque l'hypothèse de Riemann est formulée pour les fonctions ζ de Dedekind, elle est connue sous le nom **d'hypothèse de Riemann étendue** (HRE) et lorsqu'elle est formulée pour les fonctions L de Dirichlet, elle est connue sous le nom **d'hypothèse de Riemann généralisée** (HRG).

I.4.1 Hypothèse de Riemann généralisée

De même que l'hypothèse de Riemann originelle, elle a d'importantes conséquences sur la répartition des nombres premiers.

Définition 3 : Caractère de Dirichlet :
On appelle **caractère de Dirichlet** toute fonction arithmétique complètement multiplicative χ pour laquelle il existe un entier naturel $k > 0$ tel que :

$$\forall n \in \mathbb{N},\ \chi(n+k) = \begin{cases} \chi(n) & \text{si PGCD}(n,k) = 1 \\ 0 & \text{sinon.} \end{cases}$$

Définition 4 : Fonction L de Dirichlet d'un caractère χ :
On considère χ un caractère de Dirichlet.
On appelle **fonction L de Dirichlet du caractère** χ la fonction définie par :

$$\forall z \in \mathbb{C} \text{ tq } \mathrm{Re}(z) > 1,\ L(\chi, s) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}.$$

Remarque :
Par prolongement analytique, cette fonction peut être étendue à une fonction méromorphe définie sur tout le plan complexe.

L'énoncé de l'hypothèse de Riemann généralisée est le suivant :

Conjecture 1 : Hypothèse de Riemann généralisée :
Soit χ un caractère de Dirichlet.
Si s est un nombre complexe tel que $L(\chi, s) = 0$ et si sa partie réelle est strictement comprise entre 0 et 1, alors elle vaut en fait $\frac{1}{2}$.

Remarque :
Le cas du caractère trivial correspond à l'hypothèse de Riemann ordinaire.

I.4.2 Hypothèse de Riemann étendue

Pour $\mathbb{K}$ un corps de nombres, $\mathcal{O}_{\mathbb{K}}$ l'anneau de ses entiers et $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_{\mathbb{K}}$, on note sa norme absolue par $N(\mathfrak{a})$.

Définition 5 : Fonction ζ de Dedekind d'un corps de nombres :
On appelle **fonction ζ de Dedekind de** $\mathbb{K}$ la fonction définie par :

$$\forall z \in \mathbb{C} \text{ tq } \mathrm{Re}(z) > 1,\ \zeta_{\mathbb{K}}(s) = \sum_{\substack{\mathfrak{a} \text{ idéal de } \mathcal{O}_{\mathbb{K}} \\ \mathfrak{a} \neq (0)}} \frac{1}{(N(\mathfrak{a}))^s}.$$

Remarque :
La fonction ζ de Dedekind satisfait une équation fonctionnelle et peut être étendue par prolongement analytique sur le plan complexe entier. La fonction résultante contient ainsi des informations importantes sur le corps de nombres $\mathbb{K}$.

L'énoncé de l'hypothèse de Riemann étendue est le suivant :

Conjecture 2 : Hypothèse de Riemann étendue :
Soit $\mathbb{K}$ un corps de nombres.
Si s est un nombre complexe tel que $\zeta_{\mathbb{K}}(s) = 0$ et si sa partie réelle est strictement comprise entre 0 et 1, alors elle vaut en fait $\frac{1}{2}$.

Remarque :
Le cas de l'extension triviale ($\mathbb{K} = \mathbb{Q}$ et $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}$) correspond à l'hypothèse de Riemann ordinaire.

II Le cas $p = 2$ de la conjecture de Serre

Le but de cette partie sera de reprendre la preuve de John Tate envoyée à Jean-Pierre Serre (cf. [6], p.463 à 466) et de la détailler en vue d'aboutir au théorème énoncé ci-dessous :

Théorème 1 :
Soient $\mathbb{L}/\mathbb{Q}$ une extension de corps finie, galoisienne et qui est non ramifiée en dehors de 2 et G son groupe de Galois.
S'il existe une injection $\rho : G \longrightarrow \mathrm{SL}_2(\mathbb{K})$ (avec $\mathbb{K}$ un corps fini de caractéristique 2), alors on a $\mathbb{L} \subseteq \mathbb{Q}\left(i, \sqrt{2}\right)$ et pour tout $\sigma \in G$, $\mathrm{Tr}(\rho(\sigma)) = 0$.

Puisque le corps $\mathbb{K}$ est un corps fini de caractéristique 2, il est de la forme $\mathbb{K} = \mathbb{F}_{2^n}$ pour $n \in \mathbb{N}^*$. Ainsi, on a :

$$\mathrm{Card}(\mathrm{SL}_2(\mathbb{K})) = \frac{1}{2^n - 1} \prod_{k=0}^{1} \left((2^n)^2 - (2^n)^k \right) = \frac{2^n}{2^n - 1} \left(2^{2n} - 1\right)(2^n - 1) = 2^n \underbrace{\left(2^{2n} - 1\right)}_{=q} \tag{2}$$

où q n'est pas divisible par 2.

Or, G est un groupe fini et ρ est injectif, donc $\rho(G)$ est un sous-groupe fini de $\mathrm{SL}_2(\mathbb{K})$ de même cardinal que G et par le théorème de Lagrange, on a que $\mathrm{Card}(\rho(G)) = 2^r s$ (avec $r \in [\![0; n]\!]$ et $s \mid q$).

Remarquons que :

$$T = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ x \in \mathbb{K} \right\}$$

est un 2-Sylow de $\mathrm{SL}_2(\mathbb{K})$ puisque c'est un sous-groupe de $\mathrm{SL}_2(\mathbb{K})$ de cardinal 2^n (donc un 2-sous-groupe de Sylow maximal au sens de l'inclusion par (2)). En effet, on a un isomorphisme de groupes donné par :

$$\Psi : \left| \begin{array}{ccc} (T, \times) & \longrightarrow & (\mathbb{K}, +) \\ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} & \longmapsto & x \end{array} \right.$$

et donc en particulier on a également que T est isomorphe à $\mathbb{K}$ en tant que groupe. Or, puisque $\mathbb{K}$ est un corps de caractéristique 2, on en tire que T est un groupe abélien dont tous les éléments (sauf I_2) sont d'ordre 2, ainsi T est un 2-groupe élémentaire abélien (c'est donc en particulier un 2-groupe).

Considérons désormais S un 2-Sylow de $\rho(G)$.
On a alors que S est un 2-sous-groupe de Sylow de $\mathrm{SL}_2(\mathbb{K})$ (grâce à l'injection ρ du théorème), donc il existe un 2-Sylow $\widetilde{T}$ de $\mathrm{SL}_2(\mathbb{K})$ tel que S soit inclus dedans. Ainsi, puisque T et $\widetilde{T}$ sont conjugués dans $\mathrm{SL}_2(\mathbb{K})$, les propriétés de T se transportent à celles de $\widetilde{T}$ et donc $\widetilde{T}$ est un 2-groupe élémentaire abélien. Par conséquent, S est également un 2-groupe élémentaire abélien (d'après le théorème de Lagrange).

De plus, pour tout $M = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in T$, on a $\mathrm{Tr}(M) = 0$ (car $\mathbb{K}$ est de caractéristique 2). Donc si $\rho(G)$ est un 2-groupe, alors on a $S = \rho(G)$ (par la définition de S) et ainsi pour tout $y = \rho(\sigma) \in \rho(G)$, il existe $t \in T$ et $s \in \mathrm{SL}_2(\mathbb{K})$ tels que $y = sts^{-1}$ et ainsi :

$$\mathrm{Tr}(\rho(\sigma)) = \mathrm{Tr}(y) = \mathrm{Tr}\left(sts^{-1}\right) = \mathrm{Tr}(t) \underset{\substack{\text{car } t \in T}}{=} 0.$$

Finalement, si l'on montre que $\rho(G)$ est un 2-groupe, alors le résultat du théorème concernant les traces sera démontré.

II.1 Cas où G est résoluble

Supposons dans toute cette sous-partie que le groupe G soit résoluble.

Considérons $D(G)$ le sous-groupe dérivé de G.
Comme l'extension $\mathbb{L}/\mathbb{Q}$ est galoisienne, on a par la correspondance de Galois qu'il existe un sous-corps $\mathbb{M}$ de $\mathbb{L}$ contenant $\mathbb{Q}$ (c'est même le sous-corps de $\mathbb{L}$ stable par l'action de n'importe quel élément $\sigma \in D(G)$). Toujours par la correspondance de Galois, on peut affirmer que le groupe de Galois $\mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ est isomorphe à $G/D(G) = G^{\mathrm{ab}}$ qui est abélien. Donc par le théorème de Kronecker-Weber, $\mathbb{M}$ est inclus dans un corps cyclotomique notée $\mathbb{Q}(\zeta_n)$.

De plus, l'extension $\mathbb{M}/\mathbb{Q}$ étant non ramifiée en dehors de 2, on en déduit que n est de la forme 2^r avec $r \in \mathbb{N}^*$ (car si $r = 0$, alors 2 n'est pas ramifié). Ainsi, toujours par la correspondance de Galois, on a que $\mathrm{Card}(G/D(G)) = [\mathbb{M} : \mathbb{Q}]$ et par multiplicativité du degré, on a que $[\mathbb{M} : \mathbb{Q}]$ divise $[\mathbb{Q}(\zeta_{2^r}) : \mathbb{Q}] = \mathrm{Card}\left((\mathbb{Z}/2^r\mathbb{Z})^\times\right) = \varphi(2^r) = 2^{r-1}$.

Ainsi, $G/D(G)$ est un 2-groupe et la projection π de S sur $G/D(G)$ est surjective donc $G/D(G)$ est également élémentaire abélien. Ainsi, tous les éléments de $G/D(G)$ sont des éléments d'ordre 2 et finalement $\mathbb{M} \subseteq \mathbb{Q}(\zeta_8)$ (car $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$).

De plus, chaque sous-corps de $\mathbb{Q}(\zeta_8)$ a pour nombre de classe 1 et il y a un unique idéal premier au dessus de 2 (c'est-à-dire que 2 est totalement ramifié). Par la théorie des corps de classes, une telle extension de corps abélienne a pour degré une puissance de 2. Donc par le troisième théorème d'isomorphisme, $D(G)/D^{(2)}(G)$ (avec $D^{(2)}(G) = D(D(G))$) est un 2-groupe et $G/D^{(2)}(G)$ est abélien puisque la projection $\pi : S \longrightarrow G/D^{(2)}(G)$ est surjective. Ainsi, $D(G) = D^{(2)}(G)$ et donc la suite dérivée $\left(D^{(n)}(G)\right)_{n\in\mathbb{N}}$ est stationnaire et puisque G est résoluble, on a par unicité de la limite que $D(G) = \{e_G\}$. Finalement, on a $\mathbb{L} = \mathbb{M} \subseteq \mathbb{Q}(\zeta_8)$.

Or, on a $\mathbb{Q}(\zeta_8) = \mathbb{Q}\left(i, \sqrt{2}\right)$. En effet, on a d'une part que $\dim_{\mathbb{Q}}(\mathbb{Q}(\zeta_8)) = \varphi(8) = 4$ et par le théorème de la base télescopique on a $\dim_{\mathbb{Q}}\left(\mathbb{Q}\left(i, \sqrt{2}\right)\right) = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(i)] \times [\mathbb{Q}(i) : \mathbb{Q}] + 2 \times 2 = 4$. D'autre part, on a :

$$\zeta_8 = e^{\frac{2i\pi}{8}} = e^{\frac{i\pi}{4}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}.$$

Finalement, on a $\mathbb{Q}(\zeta_8) \subseteq \mathbb{Q}\left(i, \sqrt{2}\right)$ et par inclusion et égalité des dimensions (en tant que $\mathbb{Q}$-espace vectoriel), on a bien que $\mathbb{Q}(\zeta_8) = \mathbb{Q}\left(i, \sqrt{2}\right)$.

Finalement, on a $\mathbb{L} \subseteq \mathbb{Q}\left(i, \sqrt{2}\right)$ et G est un 2-groupe puisque $\mathrm{Card}(G) = [\mathbb{L} : \mathbb{Q}]$ divise $\left[\mathbb{Q}\left(i, \sqrt{2}\right) : \mathbb{Q}\right] = 8 = 2^3$ (par le théorème de la base télescopique) et on a ainsi le résultat concernant les traces puisque G et $\rho(G)$ ont le même cardinal (car ρ est un plongement).

II.2 Cas où G est non-résoluble

Dans toute cette sous-partie, on suppose que G n'est pas résoluble.

Le but sera d'obtenir une contradiction via l'estimation de Minkowski du discriminant d de $\mathbb{L}/\mathbb{Q}$ (cf. [10] p.119 et 120 pour plus de détails). En effet, si l'on note $n = [\mathbb{L} : \mathbb{Q}] = \mathrm{Card}(G)$, alors l'estimation est donnée par :

$$|d| \geq \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2} \geq \left(\frac{\pi e^2}{4}\right)^n \frac{1}{2\pi n e^{\frac{1}{6n}}}. \tag{3}$$

Remarque :
La preuve fonctionnera grâce au fait suivant :

$$2^{\frac{5}{2}} \approx 5,656 < \frac{\pi e^2}{4} \approx 5,80.$$

À savoir, nous montrerons plus loin que l'on a :

$$\begin{cases} |d| \leq 2^n & \text{si } \mathbb{L}/\mathbb{Q} \text{ est modérément ramifiée} \\ |d| \leq 2^{n\left(\frac{5}{2}-2^{1-m}\right)} & \text{si } \mathbb{L}/\mathbb{Q} \text{ a une ramification sauvage de degré } 2^m \text{ avec } m \in \mathbb{N}^*. \end{cases} \tag{4}$$

En effet, grâce à cela on obtient dans le cas modéré que :

$$2\pi n e^{\frac{1}{6n}} = \left(\frac{\pi e^2}{8}\right)^n > 2,9^n.$$

Or cela n'est plus vrai dès que $n \geq 3$ (on peut par exemple étudier la monotonie de la suite de terme général $u_n = 2\pi n e^{\frac{1}{6n}} - 2,9^n$ pour $n \geq 3$) et puisqu'ici le groupe G n'est pas résoluble, on obtient par le théorème $p^a q^b$ de Burnside que $n \geq 60$, d'où la contradiction.

Et dans le cas sauvage, on obtient :

$$n\left(\frac{5}{2} - 2^{1-m}\right)\ln(2) \geq \ln(|d|) \geq n\ln\left(\frac{\pi e^2}{4}\right) - \ln(2\pi n) - \frac{1}{6n}.$$

C'est-à-dire :

$$\ln(2\pi n) + \frac{1}{6n} \geq n\left(\ln\left(\frac{\pi e^2}{4}\right) - \frac{5}{2}\ln(2)\right) + \frac{n}{2^{m-1}}\ln(2).$$

De plus comme n a au moins 3 facteurs premiers distincts et que 2^m divise n (à cause de la ramification de degré 2^m), on a $n \geq 2^m \times 3 \times 5$ et donc :

$$\frac{n}{2^{m-1}} \geq 2 \times 3 \times 5 = 30.$$

Ainsi, on a :

$$\ln(n) + \frac{1}{6n} \geq n\left(\ln\left(\frac{\pi e^2}{4}\right) - \frac{5}{2}\ln(2)\right) + 30\ln(2) - \ln(2\pi) \geq \frac{n}{40} + 18.$$

Ce qui n'est pas possible puisque l'on a $n \geq 60$.

Afin d'achever la preuve, il nous reste donc à prouver (4) :
Considérons D, I et R respectivement le groupe de décomposition, d'inertie et de ramification d'une place v de $\mathbb{L}$ au dessus de 2, posons $\mathrm{Card}(R) = 2^m$ et notons $\mathcal{D}$ la différente de $\mathbb{L}/\mathbb{Q}$.

La relation (4) est alors équivalente à la relation :

$$\begin{cases} v(\mathcal{D}) \leq v(2) & \text{si } \mathbb{L}/\mathbb{Q} \text{ est modérément ramifiée} \\ v(\mathcal{D}) \leq \left(\frac{5}{2} - 2^{1-m}\right) v(2) & \text{si } \mathbb{L}/\mathbb{Q} \text{ a une ramification sauvage de degré } 2^m \text{ avec } m \in \mathbb{N}^*. \end{cases} \tag{5}$$

Or, dans le cas modéré, on sait que $v(\mathcal{D}) = \dfrac{e-1}{e} v(2) \geq v(2)$ (où $e = v(2)$ est l'indice de ramification). Il nous suffit donc de traiter le cas où la ramification est sauvage.

Soit S_D un 2-Sylow du groupe de décomposition D et choisissons un plongement $\rho : G \longrightarrow \mathrm{SL}_2(\mathbb{K})$ de sorte qu'on ait le plongement $\rho(S_D) \subseteq T = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ x \in \mathbb{K} \right\}$.

On obtient que $\rho(R)$ est un sous-groupe non trivial de T et ainsi, son normalisateur est contenu dans le sous-groupe de Borel $B = \left\{ \begin{pmatrix} a & * \\ 1 & a^{-1} \end{pmatrix},\ a \in \mathbb{K} \right\}$. De plus, on sait que R est un sous-groupe distingué de D, donc $\rho(R)$ est un sous-groupe distingué de $\rho(D)$ et par maximalité, on a que $\rho(D)$ est inclus dans le normalisateur de $\rho(R)$, d'où $\rho(D) \subseteq B$.

Ainsi, $\rho(S_D) = \rho(D) \cap T$ est un sous-groupe distingué de $\rho(D)$ et on a par le deuxième théorème d'isomorphisme :

$$D/S_D \cong \rho(D)/\rho(S_D) = \rho(D)/(\rho(D) \cap T) \cong \rho(D)T/T \subseteq B/T \cong \mathbb{K}^*.$$

Ainsi, comme D/S_D est un sous-groupe du groupe cyclique $\mathbb{K}^*$, il est lui-même cyclique et donc c'est le groupe de Galois d'une extension abélienne modérément ramifiée F de $\mathbb{Q}_2$. Or une telle extension est non ramifiée, donc $R = I \subseteq S_D$, et l'on est réduit à démontrer le lemme suivant (et dont nous admettons la preuve) :

Lemme 1 :
Soit F une extension finie et non ramifiée de $\mathbb{Q}_2$.
Si E/F est une extension totalement ramifiée dont le groupe de Galois R est un 2-groupe abélien élémentaire d'ordre 2^m ($m \in \mathbb{N}^*$), alors la différente de E/F divise 2^c avec $c = \dfrac{5}{2} - 2^{1-m}$.

Ainsi, on aboutit à une contradiction et on en déduit que G ne peut être que résoluble. Grâce au théorème, on en déduit que $\mathbb{L} \subseteq \mathbb{Q}\left(i, \sqrt{2}\right)$ et par la correspondance de Galois on peut trouver tous les corps $\mathbb{L}$ candidats et on connaît toutes leurs représentations.

III Un rapide mot sur le cas $p = 3$

On parle ici rapidement du cas des extensions galoisiennes non ramifiées en dehors de 3.

Dans le cas $p = 3$, on obtient le théorème suivant :

Théorème 1 :
Soient G le groupe de Galois d'une extension galoisienne finie $\mathbb{K}/\mathbb{Q}$ qui est non ramifiée en dehors de 3 et $\rho : G \longrightarrow \mathrm{GL}_2\left(\overline{\mathbb{F}_3}\right)$ une représentation impaire complètement réductible et fidèle.
On a la décomposition $\rho = 1 \oplus \chi_3$ (où χ_3 est le caractère cyclotomique).

La preuve du théorème suit le même principe que précédemment. En effet, si l'on remplace 2 par un nombre premier arbitraire ℓ, alors la relation (4) devient :

$$\begin{cases} |d| \leq \ell^n & \text{si } \mathbb{L}/\mathbb{Q} \text{ est modérément ramifiée} \\ |d| \leq \ell^{n\left(2+\frac{1}{\ell}-\frac{1}{(\ell-1)\ell^{m-1}}\right)} & \text{si } \mathbb{L}/\mathbb{Q} \text{ a une ramification sauvage de degré } \ell^m \text{ avec } m \in \mathbb{N}^*. \end{cases} \tag{6}$$

Et puisque $\ell^{2+\frac{1}{\ell}} > \dfrac{\pi e^2}{4}$ lorsque $\ell \geq 3$, cette estimation n'est pas suffisante... Pour montrer qu'il existe un ensemble fini de corps $\mathbb{L}/\mathbb{Q}$ pour un nombre premier ℓ donné via cette méthode, nous aurions besoin d'une amélioration de l'estimation de Minkowski (malheureusement Golod et Chafarevitch ont montré que ce n'est pas toujours possible)... Ainsi, dans l'article original de Tate, il mentionne que pour des petites valeurs de ℓ (c'est-à-dire 3, 5 et 7), il serait possible de gérer les cas résolubles via la théorie des corps de classes par une manière analogue à ce qui a été fait précédemment (et c'est en effet le cas mais avec un peu plus de travail), mais il ne sait pas comment s'occuper du cas non résoluble...

Heureusement, Jean-Pierre Serre montra (cf. [4] p.710) que la borne d'Odlyzko-Poitou était suffisante pour traiter le cas de la caractéristique 3. Il obtient alors que le cardinal du groupe de Galois G est inférieur ou égal à 38, donc que G est résoluble et par un travail similaire avec la théorie des corps de classes il trouve que $n = 2$ et que la représentation est $1 \oplus \chi_3$ (ce qui démontre sa conjecture pour ce cas).

IV Le cas $p = 5$ de la conjecture de Serre

Le but de cette partie sera de reprendre l'article de Sharon Brueggeman et de détailler la preuve de la conjecture de Serre pour la caractéristique 5.

IV.1 Introduction

Soient ℓ un nombre premier et $\overline{\rho} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2\left(\overline{\mathbb{F}_\ell}\right)$ une représentation galoisienne impaire complètement réductible (c'est-à-dire somme directe de représentations irréductibles) qui est non ramifiée en dehors de ℓ.

En supposant l'hypothèse de Riemann généralisée, nous allons démontré la conjecture de Serre pour $\ell = 5$. Pour cela, on considère G un sous-groupe fini de $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) / \mathrm{Ker}\left(\overline{\rho}\right)$ ainsi que la représentation fidèle $\rho : G \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ associée. Nous allons dans un premier temps supposer que G est résoluble et dans ce cas on trouve un groupe possible et toutes ses représentations sont en effet modulaires, puis dans un deuxième temps on supposera que G est non résoluble et on limitera la taille du groupe de Galois via une estimation du discriminant et nous réduirons G a deux groupes possibles via le théorème de Feit-Thompson et la classification de Dickson. Enfin, on borne le discriminant absolu de chacun de ces groupes et grâce à la base de donnée `LMFDB - Number fields` nous montrerons que les extensions avec les discriminants absolus ne coïncident pas avec les extensions dont le groupe de Galois fait parti de la liste trouvée précédemment.

Le théorème que nous voulons démontrer sera le suivant :

Théorème 1 :
Soient G le groupe de Galois d'une extension galoisienne finie $\mathbb{K}/\mathbb{Q}$ qui est non ramifiée en dehors de 5 et $\rho : G \longrightarrow \mathrm{GL}_2\left(\overline{\mathbb{F}_5}\right)$ une représentation impaire complètement réductible et fidèle.
Si l'hypothèse de Riemann généralisée est vérifiée, alors on a $\rho = \chi_5^a \oplus \chi_5^b$ pour $a \in \{0; 2\}$ et $b \in \{1; 3\}$ (où χ_5 est le caractère cyclotomique).

Remarque :
Puisque $\rho(G)$ est fini, il est possible de choisir un entier naturel n tel que l'application $\rho : G \longrightarrow \mathrm{GL}_2(\mathbb{F}_{5^n})$ soit une injection (en effet, on peut plonger $\mathrm{GL}_2(\mathbb{F}_{5^n})$ dans $\mathrm{GL}_2\left(\overline{\mathbb{F}_5}\right)$ de manière naturelle) mais pas une surjection.

Dans toute la suite de cette partie, on considère donc G, $\mathbb{K}$ et ρ comme définis ci-dessus.

IV.2 Cas où G est résoluble

Dans toute cette sous-partie, on suppose que G est résoluble.

Nous allons commencer par montrer que l'ordre de G est premier à 5 :

Lemme 1 :
Le nombre 5 ne divise pas $\mathrm{Card}(G)$.

Preuve :
$*$ Si $\rho(G)$ est irréductible :
Dmitrii Alekseevich Suprunenko a montré ([2]), pour tout nombre premier p, que tout sous-groupe maximal irréductible et résoluble de $\mathrm{GL}_2(\mathbb{F}_{p^n})$ est d'ordre $2\left(p^n - 1\right)$, $2\left(p^{2n} - 1\right)$ ou $24\left(p^n - 1\right)$.
Or, ici, $\rho(G)$ est un sous-groupe propre de $\mathrm{GL}_2(\mathbb{F}_{5^n})$ (qui est de cardinal fini), donc on sait qu'il existe un sous-groupe maximal, irréductible et résoluble H de $\mathrm{GL}_2(\mathbb{F}_{5^n})$ contenant $\rho(G)$.
En appliquant le résultat ci-dessus avec $p = 5$ on trouve que H a pour cardinal $2\left(5^n - 1\right)$, $2(5^{2n} - 1)$ ou $24(5^n - 1)$ et ainsi $\mathrm{Card}(H)$ n'est pas divisible par 5 et donc par le théorème de Lagrange, $\mathrm{Card}(G)$ non plus.

$*$ Si $\rho(G)$ est réductible :
Puisque ρ est complètement réductible, on en déduit que $\rho(G)$ est isomorphe à un sous-groupe matriciel de $\mathrm{GL}_2(\mathbb{F}_{5^n})$ composé uniquement de matrices diagonales. Ainsi, G peut être plongé dans le groupe $\mathbb{F}_{5^n}^\times \times \mathbb{F}_{5^n}^\times$ de cardinal $(5^n-1)^2$ (non divisible par 5) donc par le théorème de Lagrange, $\mathrm{Card}(G)$ n'est pas divisible par 5.

■

On considère désormais $D(G)$ le groupe dérivé de G.
Puisque le groupe $D(G)$ est un sous-groupe de G et que $\mathbb{K}/\mathbb{Q}$ est une extension galoisienne (finie), on obtient par la correspondance de Galois, qu'il existe $\mathbb{M}$ un sous-corps de $\mathbb{K}$ contenant $\mathbb{Q}$.

Lemme 2 :
Le corps $\mathbb{M}$ est égal à $\mathbb{Q}(\zeta_5)$.

Preuve :
L'extension $\mathbb{M}/\mathbb{Q}$ est abélienne (car son groupe de Galois est $G/D(G) = G^{\mathrm{ab}}$ d'après la correspondance de Galois) et elle est non ramifiée en dehors de 5 (car l'extension $\mathbb{K}/\mathbb{Q}$ ne l'est pas). Ainsi, par le théorème de Kronecker-Weber, $\mathbb{M}$ est inclus dans une extension cyclotomique de $\mathbb{Q}$ de la forme $\mathbb{Q}(\zeta_n)$ (pour $n \in \mathbb{N}^*$) et comme $\mathbb{M}/\mathbb{Q}$ est non ramifiée en dehors de 5, il existe $r \in \mathbb{N}$ tel que $\mathbb{M} = \mathbb{Q}(\zeta_{5^r})$.

Ainsi, par la correspondance de Galois, on a :

$$G/D(G) \cong \mathrm{Gal}(\mathbb{M}/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_{5^r})/\mathbb{Q}) \cong (\mathbb{Z}/5^r\mathbb{Z})^\times .$$

Or ici on a $r > 0$ (car l'extension est non triviale puisque dans le cas contraire 5 ne peut pas se ramifier) et par le théorème des restes chinois, on a : $(\mathbb{Z}/5^r\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5^{r-1}\mathbb{Z}$.

Ainsi, par le lemme 1, on en déduit que $r = 1$ et puisque $\det(\rho)$ est un caractère de Dirichlet impair de conducteur 5, on en déduit que $\det(\rho) = \chi_5$ ou χ_5^3 et ainsi $\mathbb{M} = \mathbb{Q}(\zeta_5)$.

■

Nous allons maintenant nous intéresser à $D(G)/D^{(2)}(G)$ en montrant que ce groupe est trivial.

Lemme 3 :
L'indice de $D^{(2)}(G)$ dans $D(G)$ divise 4.

Preuve :
Soit $\mathcal{O}_{\mathbb{M}}$ l'anneau des entiers de $\mathbb{M} = \mathbb{Q}(\zeta_5)$ (c'est-à-dire $\mathbb{Z}(\zeta_5)$).
Puisque 5 est totalement ramifié dans $\mathbb{M}$, il existe donc un unique premier $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{M}}$ au dessus de 5. De plus, on sait que $\mathbb{Q}(\zeta_5)$ a pour nombre de classe 1. Or, par la théorie des corps de classes le groupe de Galois de l'extension abélienne maximale de $\mathbb{M}$ de degré premier à 5 et non ramifiée en dehors de $\mathfrak{p}$ est un quotient de $(\mathcal{O}_{\mathbb{M}}/\mathfrak{p})^\times \cong \mathbb{F}_5^\times \cong \mathbb{Z}/4\mathbb{Z}$. Donc $D(G)/D^{(2)}(G)$ est un groupe cyclique d'ordre divisant 4 (toujours par la théorie des corps de classes).

■

Lemme 4 :
Le groupe G est abélien.

Preuve :
$*$ Si $\rho(G)$ est réductible :
Comme dans la preuve du lemme 1, on obtient que G peut être plongé dans le groupe abélien $\mathbb{F}_{5^n}^\times \times \mathbb{F}_{5^n}^\times$, donc il est abélien.

$*$ Si $\rho(G)$ est irréductible :
Par le lemme 2, on a $\mathrm{Card}(G/D(G)) = 4$ et par le lemme 3, $\mathrm{Card}\left(D(G)/D^{(2)}(G)\right)$ divise 4 (donc est égal à 1,2 ou 4). De plus, on a par le troisième théorème d'isomorphisme que :

$$\mathrm{Card}\left(G/D^{(2)}(G)\right) = \mathrm{Card}(G/D(G))\,\mathrm{Card}\left(D(G)/D^{(2)}(G)\right).$$

Finalement, $G/D^{(2)}(G)$ est un 2-groupe (d'ordre 4,8 ou 16).

Or, puisqu'il existe une unique extension quadratique de $\mathbb{Q}$ non ramifiée en dehors de 5 (qui est $\mathbb{Q}\left(\sqrt{5}\right)/\mathbb{Q}$), $G/D^{(2)}(G)$ possède uniquement un seul sous-groupe distingué qui est d'indice 2 (par la correspondance de Galois) et qui correspond donc à son sous-groupe de Frattini. Ainsi, par le lemme 1 du théorème de Burnside, on obtient que le quotient de $G/D^{(2)}(G)$ par son sous-groupe de Frattini est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et donc par le théorème de Burnside, $G/D^{(2)}(G)$ est cyclique et isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

■

On obtient ainsi que $D(G) = \{e_G\}$ (puisque G est abélien) et ainsi :

$$G \cong G/D(G) \cong \mathrm{Gal}(\mathbb{M}/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}.$$

Remarque :
Cette partie de la preuve ne dépend pas de l'hypothèse de Riemann généralisée.

IV.3 Cas où G est non résoluble

Dans toute cette sous-partie, on suppose que G n'est pas résoluble et on note d le discriminant de $\mathbb{K}/\mathbb{Q}$.

Supposons d'abord que $\mathbb{K}/\mathbb{Q}$ est modérément ramifiée en 5. L'estimation de Tameness et Minkowski donne que :

$$5^{\mathrm{Card}(G)} \geq |d| \geq \left(\frac{\pi e^2}{4}\right)^{\mathrm{Card}(G)} \frac{1}{2\pi\,\mathrm{Card}(G) e^{\frac{1}{6\,\mathrm{Card}(G)}}}.$$

On a alors que $\mathrm{Card}(G) < 37$ et donc que G est résoluble par le théorème $p^a q^b$ de Burnside, ce qui est contradictoire avec l'hypothèse de départ. On peut donc supposer sans pertes de généralités que $\mathbb{K}/\mathbb{Q}$ a une ramification sauvage de degré 5^m.

En utilisant un plongement de G dans $\mathrm{GL}_2\left(\overline{\mathbb{F}_5}\right)$ (par exemple en utilisant ρ construit dans l'introduction), John Tate a montré que :

$$\mathrm{Card}(G)\left(2 + \frac{1}{5} - \frac{1}{4}5^{1-m}\right)\ln(5) \geq \ln(|d|). \tag{7}$$

De plus, en supposant l'hypothèse de Riemann généralisée vérifiée, Georges Poitou a montré que ([3]) :

$$\ln(|d|) \geq \mathrm{Card}(G)\left(3,801 - \frac{20,766}{\ln(\mathrm{Card}(G))^2} - \frac{157,914\left(1 + \frac{1}{\mathrm{Card}(G)}\right)}{\ln(\mathrm{Card}(G))^3\left(1 + \frac{\pi^2}{\ln(\mathrm{Card}(G))^2}\right)^2}\right). \tag{8}$$

Après avoir réarrangé (7) et (8), on obtient :

$$\frac{11}{5}\ln(5)\,\mathrm{Card}(G) \geq \mathrm{Card}(G)\left(3,801 - \frac{20,766}{\ln(\mathrm{Card}(G))^2} - \frac{157,914\left(1 + \frac{1}{\mathrm{Card}(G)}\right)}{\ln(\mathrm{Card}(G))^3\left(1 + \frac{\pi^2}{\ln(\mathrm{Card}(G))^2}\right)^2}\right) + \frac{\ln(5)}{4}\frac{\mathrm{Card}(G)}{5^{m-1}}. \tag{9}$$

Lemme 5 :
Le cardinal de G est majoré par 75 602.

Preuve :
Puisque G est non résoluble, la contraposée du théorème de Burnside implique que $\mathrm{Card}(G)$ a au moins 3 facteurs premiers distincts. De plus 5^m divise $\mathrm{Card}(G)$ (à cause de la ramification de degré 5^m) et donc 5 divise $\dfrac{\mathrm{Card}(G)}{5^{m-1}}$. Ainsi :

$$\frac{\mathrm{Card}(G)}{5^{m-1}} \geq 2 \times 3 \times 5 = 30.$$

Enfin, en remplaçant $\dfrac{\mathrm{Card}(G)}{5^{m-1}}$ par 30 dans (9), on obtient une contradiction dès que $\mathrm{Card}(G) \geq 75603$.

■

Considérons $\rho : G \longrightarrow \mathrm{GL}_2(\mathbb{F}_{5^n})$ un plongement (c'est-à-dire que ρ est fidèle).
Remarquons que $\rho(G)/(\rho(G) \cap \mathrm{SL}_2(\mathbb{F}_{5^n}))$ peut être plonger dans $\mathrm{GL}_2(\mathbb{F}_{5^n})/\mathrm{SL}_2(\mathbb{F}_{5^n})$ puisque par le deuxième théorème d'isomorphisme on a :

$$\rho(G)/(\rho(G) \cap \mathrm{SL}_2(\mathbb{F}_{5^n})) \cong (\rho(G)\,\mathrm{SL}_2(\mathbb{F}_{5^n}))\,/\,\mathrm{SL}_2(\mathbb{F}_{5^n}) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_{5^n})/\,\mathrm{SL}_2(\mathbb{F}_{5^n})$$

et que ce même quotient est cyclique (puisque le groupe $\mathrm{GL}_2(\mathbb{F}_{5^n})/\,\mathrm{SL}_2(\mathbb{F}_{5^n})$ est un sous-groupe du groupe cyclique $\mathbb{F}_{5^n}^{\times}$ via le morphisme déterminant).

Or, $\rho(G) \cap \mathrm{SL}_2(\mathbb{F}_{5^n})$ n'est pas résoluble (sinon G le serait aussi par l'injection ci-dessus) et par le théorème de Feit-Thompson, on a que $\mathrm{Card}(\rho(G) \cap \mathrm{SL}_2(\mathbb{F}_{5^n}))$ est pair. Donc $\rho(G) \cap \mathrm{SL}_2(\mathbb{F}_{5^n})$ contient au moins un élément d'ordre 2 (toujours pas l'injection ci-dessus) et puisque $\mathrm{SL}_2(\mathbb{F}_{5^n})$ a pour unique élément d'ordre 2 l'élément $-I_2$, on en déduit que $-I_2 \in \rho(G)$ et ainsi $\{-I_2; I_2\}$ est un sous-groupe de $\rho(G)$.

Lemme 6 :
Soit $\pi : \mathrm{GL}_2(\mathbb{F}_{5^n}) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_{5^n})$ la projection canonique.
$(\pi \circ \rho)(G)$ est isomorphe à $\mathrm{PGL}_2(\mathbb{F}_5)$ ou $\mathrm{PSL}_2(\mathbb{F}_5)$.

Preuve :
Soit $\pi : \mathrm{GL}_2(\mathbb{F}_{5^n}) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_{5^n})$ la projection canonique.
Par la classification de Dickson [8], la non résolubilité de $\rho(G)$ implique que $(\pi \circ \rho)(G)$ est conjugué à $\mathrm{PGL}_2(\mathbb{F}_{5^r})$ ou $\mathrm{PSL}_2(\mathbb{F}_{5^r})$ dans $\mathrm{PGL}_2\left(\overline{\mathbb{F}_5}\right)$ pour un certain $r > 0$.

Or, on a $\mathrm{Card}\left(\mathrm{PSL}_2(\mathbb{F}_{5^3})\right) > 75\,602$, donc par le lemme 5 on en déduit que $r \in \{1; 2\}$.
Supposons que $r = 2$.
Par le premier théorème d'isomorphisme, on a :

$$\mathrm{Card}(G) = \mathrm{Card}(\rho(G)) = \mathrm{Card}((\pi \circ \rho)(G))\,\mathrm{Card}\left(\mathrm{Ker}\left(\pi|_{\rho(G)}\right)\right)$$

avec $\left\{-\overline{I_2}; \overline{I_2}\right\} \subseteq \mathrm{Ker}\left(\pi|_{\rho(G)}\right)$.

- Si l'on a $(\pi \circ \rho)(G) \cong \mathrm{PGL}_2(\mathbb{F}_{5^2})$, on a alors $\mathrm{Card}(\rho(G)) \geq 15\,600 \times 2 = 31\,200$ et si l'on a l'isomorphisme $(\pi \circ \rho)(G) \cong \mathrm{PGL}_2(\mathbb{F}_{5^r}) \cong \mathrm{PSL}_2(\mathbb{F}_{5^2})$ et $\mathrm{Card}\left(\mathrm{Ker}\left(\pi|_{\rho(G)}\right)\right) > 2$ on a alors $\mathrm{Card}(G) \geq 7\,800 \times 4 = 31\,200$.
  Dans chacun des deux cas on a alors :
  $$\frac{\mathrm{Card}(G)}{5^{m-1}} \geq \frac{31\,200}{5} = 6\,240.$$
  Ainsi, par (9) on obtient une contradiction puisque l'on aboutit à $110\,471,818 \geq 111\,324,055$.

- Enfin, si $(\pi \circ \rho)(G) \cong \mathrm{PGL}_2(\mathbb{F}_{5^r}) \cong \mathrm{PSL}_2(\mathbb{F}_{5^2})$ et $\mathrm{Card}\left(\mathrm{Ker}\left(\pi|_{\rho(G)}\right)\right) = \left\{-\overline{I_2}; \overline{I_2}\right\}$, alors l'inégalité (9) n'est pas en défaut... À la place, nous utilisons un autre argument :
  On a que $\rho(G) \cap \mathrm{SL}_2(\mathbb{F}_{25})$ est distingué dans $\rho(G)$ et $\rho(G)/\left\{-\overline{I_2}; \overline{I_2}\right\}$ est un groupe simple, donc on a $\rho(G) \cap \mathrm{SL}_2(\mathbb{F}_{25}) = \rho(G)$ ou $\left\{-\overline{I_2}; \overline{I_2}\right\}$. Or, puisque $\rho(G) \cap \mathrm{SL}_2(\mathbb{F}_{25})$ n'est pas résoluble, on obtient que $\rho(G) = \rho(G) \cap \mathrm{SL}_2(\mathbb{F}_{25})$ et ainsi $\rho(G) \subseteq \mathrm{SL}_2(\mathbb{F}_{25})$. On aboutit alors à une contradiction car le déterminant est égal à 1 donc la représentation est paire.

■

Nous avons ainsi montré que $(\pi \circ \rho)(G)$ est isomorphe ou bien à $\mathrm{PGL}_2(\mathbb{F}_5) \cong \mathfrak{S}_5$ ou à $\mathrm{PSL}_2(\mathbb{F}_5) \cong \mathfrak{A}_5$ (isomorphismes exceptionnels) . Par le premier théorème d'isomorphisme, G possède donc un quotient isomorphe à l'un de ces deux groupes et par la correspondance de Galois, $\mathbb{K}$ possède un sous-corps contenant $\mathbb{Q}$ et stable par ce quotient.

Supposons que $\mathbb{K}$ soit ce sous-corps en question et montrons que cela contredit l'hypothèse sur la ramification (notons également que dans les deux cas, $\mathbb{K}$ est le corps de décomposition d'un polynôme de degré 5 sur $\mathbb{Q}$).
Maintenant que nous avons limité les groupes de Galois possibles, nous pouvons utiliser la formule de John Tate "à l'envers" pour borner le discriminant :

* Supposons que $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathfrak{A}_5$ et $m = 1$.
  On obtient en remplaçant dans (7) que :

$$|d| \leq 5^{60\left(2+\frac{1}{5}-\frac{1}{4}\right)} = 5^{117}.$$

  Soit $\mathbb{M}$ un sous-corps de $\mathbb{K}$ de degré 5 sur $\mathbb{Q}$.
  On obtient en conséquence que :

$$d = N_{\mathbb{M}/\mathbb{Q}}(d(\mathbb{K}/\mathbb{M})) \times d(\mathbb{M}/\mathbb{Q})^{12}.$$

  Donc $|d(\mathbb{M}/\mathbb{Q})| \leq 5^{\frac{117}{12}} = 5^{9,75}$.

* Pour $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathfrak{S}_5$ et $m = 1$, on aboutit de même à l'estimation $|d(\mathbb{M}/\mathbb{Q})| \leq 5^{\frac{117}{12}} = 5^{9,75}$.

* Enfin, on vérifie qu'il n'existe pas de corps de degré 5 sur $\mathbb{Q}$ dont le groupe de Galois d'une clôture galoisienne est isomorphe à $\mathfrak{A}_5$ ou $\mathfrak{S}_5$ et dont le discriminant est égal à $\pm 5^q$ pour q un entier naturel inférieur ou égal à 9. On peut immédiatement éliminer les cas où $q \leq 4$ car 5^4 est plus petit que le discriminant absolu minimal (ici 1609) d'un corps de nombres de degré 5 (cf. [1]). Enfin, on utilise la base de donnée `LMFDB - Number fields` et on y trouve alors les corps de degré 5 avec ces discriminants mais les groupes de Galois associés sont de cardinaux inférieurs ou égaux à 20, d'où une contradiction.

Finalement, on aboutit alors à une contradiction et le seul cas possible est celui où G est résoluble et on est ramené au résultat établi dans la sous-partie précédente.

Remarque :
Cette preuve ne peut pas s'étendre au cas où $\ell = 7$ car l'inégalité (9) devient :

$$\frac{15}{7}\ln(7)\,\mathrm{Card}(G) \geq \mathrm{Card}(G)\left(3,8.1 - \frac{20,766}{\ln(\mathrm{Card}(G))^2} - \frac{157,914\left(1+\frac{1}{\mathrm{Card}(G)}\right)}{\ln(\mathrm{Card}(G))^3\left(1+\frac{\pi^2}{\ln(\mathrm{Card}(G))^2}\right)^2}\right) + \frac{\ln(7)}{6} \times \frac{\mathrm{Card}(G)}{7^{m-1}} \tag{10}$$

et puisque $\frac{15}{7}\ln(7) > 3,801 + \frac{1}{6}\ln(7)$, nous n'obtiendrons pas de contradiction comme précédemment...

Références

[1] Albert Schwarz & Michael Pohst & Francisco Diaz y Diaz. A table of quintic number fields (1994). American Mathematical Society.

[2] Dmitrii Alekseevich Suprunenko. Matrix Groups (1976). American Mathematical Society.

[3] Georges Poitou. Sur les petits discriminants (1976). Séminaire Delange-Pisot-Poitou.

[4] Jean-Pierre Serre. Œuvres, volume 3 (1986). Springer-Verlag.

[5] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ (1987). Duke Mathematical Journal.

[6] Jean-Pierre Serre & Pierre Colmez. Correspondance Serre-Tate, Volume 2 (2015). Société Mathématique de France.

[7] John Tate. The Non-Existence of Certain Galois Extensions of $\mathbb{Q}$ Unramified Outside 2 (1994). American Mathematical Society.

[8] Leonard Eugene Dickson. Linear Groups (1958). Dover Publications Inc.

[9] Sharon Brueggeman. The Non-Existence of Certain Galois Extensions Unramified Outside 5 (1999). Journal of Number Theory.

[10] Serge Lang. Algebraic Number Theory (1970). Addison Wesley Publishing Company.