About the structure of some Galois modules over local fields

Alexandre Eimer

Thèse

INSTITUT DE RECHERCHE MATHÉMATIQUE AVANCÉE

UMR 7501

Strasbourg

présentée pour obtenir le grade de docteur de l'Université de Strasbourg
Spécialité MATHÉMATIQUES

Alexandre Eimer

De quelques modules de Galois sur les corps locaux

Soutenue le 30 Novembre 2021
devant la commission d'examen

Pierre Guillot, directeur de thèse
Christian Maire, rapporteur
Serge Bouc, rapporteur
Christine Vespa, examinateur
Hans-Werner Henn, examinateur
Ivo Dell'Ambrogio, examinateur

irma.math.unistra.fr

IRMA
Institut de Recherche Mathématique Avancée

cnrs

Université de Strasbourg

Il y a un tas de choses qui me faisaient signe, je le sens, et que j'ai négligées !
Paul Claudel
Hong-Kong in *Connaissance de l'Est*

b

Remerciements

L'exercice des remerciements en début de thèse fait partie de ceux auxquels la fréquentation des vérités mathématiques ne saurait hélas nous préparer, car c'est un examen, bien difficile, de justice.

Comme il convient de rendre à chacun son dû, il me faut en premier lieu remercier mon directeur de thèse, Pierre Guillot, par qui tout a commencé. Ce n'est cependant pas tant sa capacité à trouver des sujets d'une rare élégance en liens avec plus d'un champ des mathématiques qui lui attire ces remerciements, que sa patience, qui a été une vertu extraordinaire. En effet, les relectures des documents tous plus remarquables les uns que les autres par les notations incohérentes et les raisonnements elliptiques sont autant de preuves de cette qualité qui chez lui ne semble pas connaître de bornes.

En second lieu, j'adresse mes remerciements à ceux par qui tout finira, c'est-à-dire les membres du jury. Je pense tout d'abord à MM. Maire et Bouc, qui en leur qualité de rapporteur, ont considérablement permis l'amélioration de ce mémoire par la pertinence de leurs remarques et leur exigence qui n'a pas fait obstacle à leur mansuétude. Ensuite je ne saurais négliger les autres membres, c'est-à-dire Hans-Werner Henn, Christine Vespa dont la présence à Strasbourg a toujours été stimulante et secourable ainsi qu'Ivo Dell'Ambrogio dont l'invitation à Lille a été d'une rare courtoisie.

Enfin parmi les personnes ayant par leur action contribué à ces résultats, je tenais à remercier D. Benson qui avec une grande générosité et un tact remarquable a su me suggérer de considérables améliorations dans mes preuves.

Mais entre ces deux extrémités, je n'ai pas été seul face à un écran en regardant hagard un fichier TeX à la recherche d'une accolade manquante, bien au contraire... Évidemment, je remercie David : après toutes ces années d'amitié - dix - je crois que les déclarations deviennent superflues et sonneraient un peu ridicule ; mais dans ce silence, le regard demeure. Paul, dont la fréquentation fut presque quotidienne, mérite toute mon amitié, et ma gratitude : pour supporter des bougonneries très-pédantesques appuyées sur une compréhension hâtive et bâclée de quelques obscures auteurs, il l'a bien mérité. Bien entendu, après ces deux noms, je ne peux oublier Alexis, *der Held der Nation*, titre mérité à jamais, quand bien même l'absence du thème littéraire quasi hebdomadaire aurait, de source sûre, eu des effets étonnants sur son allemand. Pour ces voyages partagés, sa capacité de vanter l'actuariat aux jeunes élèves de maths-eco, je ne saurais que dire : Ich bedanke mich bei ihm. Je remercie aussi Viet-Cuong, dont la liste intégrale des qualités pourrait étrangement ressembler à un de ces catalogues exhaustifs des vertus que les Anciens aimaient tant, pour cette saine admiration et estime qu'il a su susciter en moi : assurément, elle m'a grandi.

Quel homme serais-je si j'oubliais Emma, ma meilleure copine comme le veut l'usage (et la vérité) ? Assurément ses visites, qui m'ont permis de découvrir à quel point le luddisme était une théorie radicale lorsqu'il s'agissait de préparer un Mont Blanc ou de la pâte de pistaches, mais aussi de mieux voir le brun de Balthus, ont été des moments précieux et nécessaires : qu'elle en soit remerciée. Bien entendu, je ne saurais oublier Anne, Youna et Manon dont l'affection certaine m'a toujours été d'un grand secours, quand bien même elles ne s'en rendraient pas compte.

Il me faut aussi reconnaître la présence non-négligeable de Clément : en veillant, avec une grande exactitude, à ne *jamais* appliquer ses conseils, en dehors des lectures philosophiques, j'ai su m'affermir et garder une grande sérénité face aux épreuves de la vie (à l'exception notable

des ascensions cyclistes : je veux bien reconnaître de bon cœur mes erreurs). Et enfin je dois remercier aussi Maxime : qu'il lise attentivement mes remerciements envers mes amis et qu'il y trouve donc un seul soupçon de quelque tractation commerciale qui soit bonne dans le monde professionnelle, mais odieuse dans le monde amicale.

Á la fin de ces remerciements, que j'avais osé annoncer comme justes, je suis obligé d'admettre qu'une thèse se trouvant à la fin même d'un long parcours scolaire et humain, il serait inique de couper ces dernières années de toutes celles les ayant précédées. Que ceux auxquels je devrais exprimer ma gratitude et qui ne figurent pas plus haut, car appartenant à des périodes plus lointaines, mais tout aussi riches et denses, lisent en ces quelques lignes toute la gratitude que je leur dois. De la manière la plus évidente et la plus *naturelle*, ce sont mes parents, et par là j'entends toute ma parenté, auprès desquels il me faudrait m'étendre en remerciements : malheureusement cet exercice de remerciements doit rester concis, là où l'apport durant les périodes les plus cruciales de mon existence a été vaste. Enfin, parmi la multitude des oubliés, je pense notamment à de nombreux professeurs : ces années m'ont offert la joie de me mettre à leur place - même si être chargé de TD en mathématiques n'a que peu à voir avec le dur labeur d'initier des collégiens à la beauté des périodes cicéroniennes - qu'ils sachent qu'ils appartiennent à ces personnes dont le souvenir demeure en moi et m'éduque après que leur présence m'a instruit.

Contents

Introduction

La théorie des nombres présente l'étrange paradoxe de formuler des questions d'une simplicité déconcertante à introduire mais d'une difficulté remarquable à résoudre. En dépit de la complexité et de la technicité de toute la machinerie mise en œuvre pour répondre à ces interrogations, certains énoncés réussissent à demeurer aisés d'accès, d'une élégante sobriété, dissimulant mieux ainsi leur portée et leur profondeur. Parmi ceux-ci figure le fameux quatre-vingt-dixième théorème du *Zahlbericht* de Hilbert que nous rappelons ici.

Théorème (Hilbert, 90)**.** *Soit* $\mathbf{k}$ *un corps contenant une racine primitive* n*-ième de l'unité* ξ_n *et soit* $\mathbf{K}/\mathbf{k}$ *une extension cyclique d'ordre* n*. Soit* σ *un générateur de* $Gal(\mathbf{K}/\mathbf{k})$*, alors il existe* $x \in \mathbf{K}^\times$ *tel que*

$$\xi_n = \frac{\sigma \cdot x}{x}\,.$$

Plus d'un siècle après, de nombreux articles ont pu être rédigés, où il est encore mentionné, non pas uniquement comme un objet de respect mais comme le modèle même du résultat devant être obtenu : il est en effet souvent question de trouver un ersatz à ce théorème dans des circonstances un peu plus complexes (voir par exemple [MST14]). Ici, nous sommes cependant moins ambitieux : notre présomption connaissant ses limites, cette thèse ne cherche pas à émuler Hilbert, mais de labourer encore le sillon qu'il a déjà tracé.

Mais quel est donc cet ensemble de résultats dont nous nous prétendons les continuateurs et pourquoi perdurer dans cette tâche ?

Les réponses à ces deux questions s'entremêlent ; comme il convient de juger un arbre à ses fruits, il est pertinent de juger une théorie aux résultats qu'elle arrive à fournir et comment ces derniers s'insèrent dans un champ d'études plus vaste. Tentons cependant provisoirement de les séparer.

Motivations

Commençons par la seconde interrogation. Plus d'un ouvrage ou d'un article a tenté de remettre dans une perspective historique l'émergence de la théorie du corps de classe (cf. [Con], [Wym72], [Has67]) ; mais plutôt que d'avoir recours aux explications généalogiques en essayant de montrer l'importance de la théorie de Kummer dans cette genèse, contentons-nous d'en citer quelques accomplissements. Grâce à la théorie du corps de classe local, en fait aux théorèmes de Hasse-Minkowski, les formes quadratiques sur $\mathbf{Q}$ sont en grande partie comprises, c'est-à-dire que

$$a \cdot x^2 + b \cdot y^2 + c \cdot z^2 = 0\,, \quad a,\, b,\, c \in \mathbf{Q}^*$$

admet des solutions rationnelles si et seulement si elle admet des solutions dans toutes les complétions de $\mathbf{Q}$, c'est-à-dire dans $\mathbf{R}$ et les corps p-adiques $\mathbf{Q}_p$, ce qui autorise bien plus d'outils. Et son extension, le très célèbre théorème de Grunwald-Wang ([NSW08]), démontre encore plus de force et de précision dans l'entreprise de lier les problèmes globaux aux problèmes locaux, si bien que ces deux accomplissements, plus que des aboutissements, sont des commencements.

La capacité à résoudre des problèmes issus de l'étude des corps de nombres en étudiant les corps locaux constitue une avancée majeure : comme on le verra par la suite très rapidement dissimulé derrière quelques théorèmes, la théorie de Galois des corps locaux est en effet beaucoup plus simple que celle des corps globaux. Aussi, l'étude des corps locaux, tout étranges qu'ils

puissent paraître, est un outil précieux pour affronter les problèmes arithmétiques, et il est même légitime qu'on l'ait érigé en *principe*.

Nous avons cependant ici tu ce pourquoi nous étudions les modules qui sont au cœur de notre travail. Nous préférons reléguer ceci à plus tard, dans le corps même du premier chapitre ; plutôt donc que d'inviter à se fier à notre parole, nous espérons gagner un début de conviction, en recensant les résultats qui ont précédé les nôtres, et qui semblent indiquer que, non, l'examen des modules dont il est question ici n'est pas une lubie, mais une question bien naturelle.

Résultats connus

L'objet de cette thèse est comme le titre l'indique l'étude de quelques représentations intervenant en théorie de Galois. Fixons les notations : soit $\mathbf{k}$ un corps local tel que $\xi_p \in \mathbf{k}$ et soit $\mathbf{K}/\mathbf{k}$ une extension galoisienne finie de groupe G, où p est évidemment un nombre premier que l'on supposera sauf mention contraire différent de 2. Nous décrivons la structure de G module de $J(\mathbf{K}) = \mathbf{K}^\times/\mathbf{K}^{\times p}$, sous des hypothèses que nous allons progressivement renforcer. Ces préoccupations ne sont cependant pas inédites.

Précisons immédiatement que pour des raisons qui apparaîtront plus tard, tous nos modules sont des modules *à droite*.

D'une part, si G est un groupe cyclique, des résultats complets sur la structure de $J(\mathbf{K})$ ont déjà été fournis : en premier lieu, D. K. Faddeev publia en 1960 un article ([Fad60]) donnant une présentation par générateurs et relations du module $J(\mathbf{K})$, faisant apparaître deux cas.[1].

Théorème (Faddeev)**.** *Soit $\mathbf{K}/\mathbf{k}$ une extension cyclique et soit σ un générateur de $Gal(\mathbf{K}/\mathbf{k})$, où $\mathbf{k}$ est un corps local tel que $\xi_p \in \mathbf{k}$. Posons de plus $n = |\mathbf{k}^\times/\mathbf{k}^{\times p}|$. Alors $J(\mathbf{K})$ admet les présentations par générateurs et relations suivantes*

1. *si $\mathbf{K}$ peut être plongé dans une extension cyclique d'ordre $(n+1)\cdot p$, $\langle \vartheta_1, \dots, \vartheta_{n+1}, \tau | \tau \cdot (\sigma - 1)^2 = 0 \rangle$,*

2. *sinon il s'agit de $\langle \vartheta_1, \dots, \vartheta_n, \tau_1, \tau_2 | \tau_1 \cdot (\sigma - 1) = \tau_2 \cdot (\sigma - 1) = 0 \rangle$.*

Le théorème de Faddeev ne resta pas lettre morte, cependant il s'inscrivit dans une autre histoire ; en effet, cinq ans plus tard Z. I. Borevič sut décrire la structure de $\mathbf{Z}_p[G]$-module des entiers de $\mathbf{K}^\times$, toujours sous l'hypothèse que $\mathbf{k}$ était local et $\mathbf{K}/\mathbf{k}$ cyclique, dans deux papiers : le premier étant [Bor65a] et requérant que $\mathbf{k}$ possède une racine primitive de l'unité ξ_p et le second étant [Bor65b] et supposant le contraire.

Le résultat de Faddeev fut étendu à toutes sortes de corps par J. Mináč, et J. Swallow, au début des années 2000.

Théorème (Mináč et Swallow)**.** *Soit G un groupe cyclique, $\mathbf{L}_0$ un corps tel que $\xi_p \in \mathbf{L}_0$ et soit $\mathbf{L}_1/\mathbf{L}_0$ une extension cyclique d'ordre p. Posons $\mathrm{N} = \sum_{g \in G} g$ la norme de $\mathbf{F}_p G$. Alors $J(\mathbf{L}_1)$ se décompose en tant que $\mathbf{F}_p G$ module comme*

$$J(\mathbf{L}_1) = X \oplus Y \oplus Z \,,$$

où

1. *X est un module indécomposable de dimension 1 si $\xi_p \in \mathbf{L}_1^\times \cdot \mathrm{N}$ et de dimension 2 si $\xi_p \notin \mathbf{L}_1^\times \cdot \mathrm{N}$.*

2. *Y est un module libre,*

3. *Z est un module trivial (ce qui inclut le cas $Z = \{0\}$).*

[1] L'article n'ayant été traduit du russe, nous ne savons pas exactement comment cela fut démontré.

Ce théorème mena à une étude plus fine et plus précise par exemple de la structure de G-module de la K-théorie de Milnor modulo p d'une telle extension : les deux précédents auteurs auquel il convient de joindre A. Schultz et N. Lemire purent en effet donner une description de la K-théorie de Milnor en tant que module sous les hypothèses énoncées plus haut. [LMSS10]

D'autre part, les investigations sur les modules non-cycliques ont connu plusieurs développements au cours des dernières décennies, on peut notamment citer [AGKM01] où l'étude est menée sur la structure de $J(\mathbf{K})$ lorsque $\mathbf{K}$ est la 2-extension élémentaire abélienne maximale. Ces recherches, il nous semble, sont toujours limitées, en dépit même des talents des auteurs, par les outils développés alors pour l'étude des $\mathbf{F}_pG$ modules : en effet, au-delà du cas où G est cyclique ou égal au célèbre groupe de Klein $C_2 \times C_2$, peu de choses sont connues, à part la difficulté du problème (voir par exemple [Ben16]). La cohomologie reste cependant un outil incontournable (cf. [Ben91]) et longuement éprouvé, malgré sa cécité sur certains phénomènes.

Aussi, le développement de la théorie des modules de type de Jordan constant tels que définis dans [CFP08] et développée dans [Ben16] représente une opportunité exceptionnelle pour affronter les problèmes issus de la théorie de Galois et étendre les précédents théorèmes.

Résultats contenus dans ce présent mémoire

C'est ici tout l'enjeu de ce mémoire d'appliquer les techniques d'études des modules de type de Jordan constant aux modules $J(\mathbf{K})$ apparaissant dans l'étude des corps locaux. Notons $\mathcal{G}_{\mathbf{k}}(p)$ le groupe de Galois d'une p-clôture maximale de $\mathbf{k}$, et n le nombre minimal de générateurs topologiques de ce groupe. Nous démontrons ici

Théorème (A)**.** *Soit* $\mathbf{k}$ *un corps local contenant une racine primitive* p*-ième de l'unité, soit* $\mathbf{K}$ *une extension galoisienne finie de* $\mathbf{k}$*, et soit* $G = Gal(\mathbf{K}/\mathbf{k})$*. Supposons que* G *est un* p*-groupe tel que son anneau de cohomologie* $H^\bullet(G, \mathbf{F}_p)$ *est de Cohen-Macaulay ; posons alors* $d_i(G) = \dim_{\mathbf{F}_p} \hat{H}^i(G, \mathbf{F}_p)$*. De surcroît, excluons les cas où* G *serait un des groupes des quaternions généralisés. On a alors l'alternative suivante*

1. *si l'inflation* $\inf\colon H^2(Gal(\mathbf{K}/\mathbf{k}), \mathbf{F}_p) \longrightarrow H^2(\mathcal{G}_{\mathbf{k}}(p), \mathbf{F}_p)$ *est nulle, les isomorphismes suivant sont vérifiés :*

$$\begin{cases} H^s(G, J(\mathbf{K})) & \simeq & \hat{H}^{s+2}(G, \mathbf{F}_p) \oplus H^{s-2}(G, \mathbf{F}_p) \quad s \geq 1 \\ H^0(G, J(\mathbf{K})) & \simeq & \mathbf{F}_p^{d_2(G)+(n-d_1(G))} \end{cases}.$$

2. *si l'inflation* $\inf\colon H^2(Gal(\mathbf{K}/\mathbf{k}), \mathbf{F}_p) \longrightarrow H^2(\mathcal{G}_{\mathbf{k}}(p), \mathbf{F}_p)$ *est non-nulle, les isomorphismes suivant sont vérifiés :*

$$\begin{cases} H^1(G, J(\mathbf{K})) & \simeq & H^3(G, \mathbf{F}_p) \\ H^s(G, J(\mathbf{K})) & \simeq & H^{s+2}(G, \mathbf{F}_p) \oplus H^{s-2}(G, \mathbf{F}_p) \quad s \geq 2 \\ H^0(G, J(\mathbf{K})) & \simeq & \mathbf{F}_p^{d_2(G)-1+(n-d_1(G))} \end{cases}.$$

Ce premier résultat décrit pleinement la cohomologie à coefficients dans $J(\mathbf{K})$; pour ce qui est du type de Jordan et des extensions élémentaires abéliennes, nous prouvons plus loin le théorème suivant :

Théorème (B)**.** *Soit* $\mathbf{k}$ *un corps local tel que* $\xi_p \in \mathbf{k}$ *et soit* $\mathbf{K}/\mathbf{k}$ *une* p*-extension élémentaire abélienne. Si* $\mathbf{K}/\mathbf{k}$ *n'est pas cyclique, alors* $J(\mathbf{K}) = \mathbf{K}^\times/\mathbf{K}^{\times p}$ *est un* $Gal(\mathbf{K}/\mathbf{k})$*-module de type de Jordan constant. De plus, son type de Jordan stable est* $[1]^2$*.*

En vérité, nous démontrerons un peu plus que ce théorème, mais préciser les hypothèses avec exactitude ici-même ferait perdre en élégance l'énoncé pour gagner peu. Les méthodes que nous utilisons nous permettent cependant d'obtenir quelques autres propositions qui ne sont pas indignes d'attention. Tout d'abord, le résultat suivant, valable pour toute p-extension galoisienne finie $\mathbf{K}/\mathbf{k}$, où $\mathbf{k}$ est toujours un corps local contenant une racine primitive p-ième de l'unité, mérite d'être cité :

Proposition (C). *Soit $G = Gal(\mathbf{K}/\mathbf{k})$ où G est un p-groupe. Pour $s \in \{-1, 2\}$, il existe un module $\omega_s(\mathbf{F}_p)$ stablement isomorphe à $\Omega^s(\mathbf{F}_p)$ et une suite exacte :*

$$0 \longrightarrow \omega_{-1}(\mathbf{F}_p) \xrightarrow{\kappa} \omega_2(\mathbf{F}_p) \longrightarrow J(\mathbf{K}) \longrightarrow 0 \ .$$

Cette précédente proposition est l'outil central dans la démonstration des deux théorèmes sus-mentionnés et les conditions figurant dans le théorème (A) sont en fait équivalentes à des conditions plus simples à discuter sur κ.

C'est pourquoi le chapitre 5 se consacre intégralement à l'étude de κ : nous nous y restreignons au cas unique de l'extension p-élémentaire abélienne maximale, certes encore une fois, puisque nous aurons examiné ceci de très près dans le chapitre 4, mais avec des objectifs radicalement différents. Ici, nous tenterons d'étendre notre étude à une classe plus grande de corps, ou plutôt de groupes. Ceci nous amènera à étudier le comportement, relativement au produit libre de deux groupes, de l'application qui étend proprement la définition de κ, ce qui est fait dans la Proposition 5.2.7 (qui requiert trop de notations pour être introduite ici). Cependant, cette proposition sera immédiatement mise à profit pour démontrer l'impossibilité d'étendre le théorème (B), en effet nous aboutissons alors au contre-exemple suivant :

Proposition. *Soit $\mathbf{k}$ un corps (qui ne soit pas local), possédant une racine primitive p-ième de l'unité et tel que $\mathcal{G}_{\mathbf{k}}(p)$ soit le produit libre d'un groupe de Demuškin et d'un groupe libre. Notons alors $\mathbf{K}/\mathbf{k}$ la p-extension abélienne élémentaire maximale de $\mathbf{k}$. Alors $J(\mathbf{K}) = \mathbf{K}^\times/\mathbf{K}^{\times p}$ n'est pas un $Gal(\mathbf{K}/\mathbf{k})$-module de type de Jordan constant.*

La démonstration de ce dernier théorème nous demandera une étude assez précise de la structure de certains modules, ce qui nous contraindra à adopter une stratégie de preuve assez technique, mais conceptuellement simple.

L'approche à partir de calculs explicites, qui nous est permise grâce à la classification effectuée par J. Labute des groupes de Demuškin (cf. [Lab67]), nous offre aussi la possibilité d'obtenir des résultats plus fins, par exemple sur la série socle du module. Ceci n'est pas sans intérêt, en effet, dans le cas où $p = 2$, traité *in extenso* dans [AGKM01], les auteurs introduisent plusieurs invariants liés à cette série. Nous tirons donc profit de nos travaux précédents pour proposer, à partir des corps locaux, comment pourraient s'étendre les-dites formules pour p quelconque. Plus précisément, nous montrons :

Proposition (D). *Soit $\mathbf{K}$ la p-extension élémentaire abélienne maximale d'un corps local $\mathbf{k}$ qui possède une racine primitive p-ième de l'unité. Alors le $Gal(\mathbf{K}/\mathbf{k})$-module $J(\mathbf{K})$ a pour longueur*

$$l(J(\mathbf{K})) = n(p-1) - 1 \, ,$$

où n est la dimension de $\mathbf{k}^\times/\mathbf{k}^{\times p}$ en tant que $\mathbf{F}_p$-espace vectoriel. De plus si p est impair, alors l'égalité suivante est vérifiée :

$$\dim_{\mathbf{F}_p} \mathrm{Soc}^2(J(\mathbf{K}))/\mathrm{Soc}(J(\mathbf{K})) = \frac{n(n-2)(n+2)}{3} \, .$$

Enfin, cette thèse contient quelque petits détours volontaires : au cours de démonstrations plus longues et plus explicites des résultats figurant plus haut, nous avons donné une présentation par générateurs et relations des décalages de Heller du module trivial lorsque G est un groupe élémentaire abélien. Ceci est l'objet du théorème 3.1.2 : il nous faudrait cependant trop nous étendre sur les notations pour en préciser les termes exacts.

Cependant si nous nous autorisons à citer ces résultats, c'est qu'outre l'intérêt qu'ils peuvent avoir en eux-mêmes, ils nous permettront d'étudier dans le cas où $\mathbf{K}/\mathbf{k}$ est l'extension p-élémentaire abélienne maximale. Ces considérations nous amèneront à prouver en fait que la suite exacte courte de la proposition D est en fait à un décalage près *localement exactement scindée*. Ceci permet alors aisément d'étudier le fibré vectoriel associé au module par les foncteurs introduits par E. Friedlander et J. Pevtosva (cf. [FP11]).

Proposition (E)**.** *Soit ℓ la caractéristique du corps résiduel de $\mathbf{k}$ un corps local tel que $\xi_p \in \mathbf{k}$, et soit $\mathbf{K}/\mathbf{k}$ la p-extension élémentaire abélienne maximale de $\mathbf{k}$. Notons $\mathfrak{V}$ le foncteur de Pevtosva et $n = \dim \mathbf{k}^\times/\mathbf{k}^{\times p}$. Si $\ell = p$, l'égalité suivante est vérifiée*

$$\mathfrak{V}(J(\mathbf{K})) = \mathcal{O}(p) \oplus \mathcal{O}(-p)\,,$$

où $\mathcal{O}$ est le faisceau usuel et $\mathcal{O}(j) = \mathcal{O}^{\otimes j}$ de $\mathbf{P}_n(\mathbf{F}_p)$ tandis que si $\ell \neq p$, on a

$$\mathfrak{V}(J(\mathbf{K})) = \mathcal{O} \oplus \mathcal{O}\,.$$

Plan de l'étude

Afin de parvenir aux fins que nous nous sommes fixées, nous allons dans un premier temps rappeler quelques résultats dont nous avons besoin : citons entre autres, la définition des modules de type de Jordan constant ou la définition de la catégorie des modules stables. Au cours de cette partie, nous traduirons le problème qui se pose en théorie de Galois en un problème de théorie des groupes. Ceci est l'objet même du Chapitre 1

Ensuite, dans le chapitre 2, nous démontrerons les théorèmes B, A mentionnés plus haut : au cours de leur démonstration, nous verrons ce en quoi ils peuvent être en fait étendus, au prix d'un énoncé moins élégant.

Nous nous focaliserons par la suite dans le calcul de modules - ici par calcul, nous entendons donner une expression par générateurs et relations - des décalages de Heller du module trivial, dans le chapitre 3, puisqu'il s'agit là de précieux résultats techniques pour aborder les chapitres suivants.

Une fois ceci fait, nous étudierons plus en détails la structure du module $J(\mathbf{K})$ obtenu lorsque $\mathbf{K}/\mathbf{k}$ est la p-extension élémentaire abélienne maximale dans le chapitre 4, ce qui est rendu possible par l'étude précédemment donnée.

Par la suite, dans le chapitre 5, nous traiterons un exemple particulier de sorte à montrer en quoi nos résultats ne peuvent pas s'étendre dans toutes les circonstances que l'on pourrait souhaiter.

Enfin, nous examinerons deux exemples concrets : ces derniers nous permettrons d'une part de constater que la disjonction de cas effectuée sur κ se produit dans les faits, et d'autre part de motiver une étude un peu plus détaillée des extensions p-élémentaires abéliennes. En effet, ni le critère sur κ que nous développerons au cours du chapitre 2, ni celui sur l'inflation ne semblent vérifiables *in concreto* ; de surcroît, ces derniers ne semblent pas liés à l'arithmétique du corps, or ces deux exemples laissent augurer tout-à-fait le contraire. Aussi nous nous permettrons de mentionner très brièvement l'ébauche d'une étude en cours permettant de remédier aux manquements que nous venons de signaler.

Chapter 1

Background material

In this chapter, we shall introduce the notions which are the core of this thesis, namely the modules of constant Jordan type and the Kummer extensions. We will immediately take profit from basic Kummer theory in order to set the stage for our results. Indeed, we shall transform the arithmetical problem into a group-theoretic one, which will enable us to use some famous results from Galois theory.

1.1 Modules of constant Jordan type

Here, we quickly recall some basic facts about modules of constant Jordan type. A more general approach is contained in the fundamental article of J. Carlson, E. Friedlander and J. Pevtosva ([CFP08]), treating the case of group schemes and a more exhaustive one about elementary abelian p-groups in Benson's book ([Ben16]). In this chapter, G is a finite p-group and $\mathbf{F}$ an algebraically closed field of characteristic p. All modules are supposed to be finitely generated.

1.1.1 Modules for the cyclic group

Modules of constant Jordan type were introduced in order to properly extend what was already known for $\mathbf{F}C_p$-modules (here C_p stands for the cyclic group of order p). Indeed, in this case, a module M is completely described by the action of a given generator x_1 of C_p, more precisely we have the following theorem:

Theorem 1.1.1. *The $\mathbf{F}C_p$-modules of dimension n (over $\mathbf{F}$) are in bijection with the partition of n by parts of size no greater than p, up to isomorphism.*

Proof. Let M be an $\mathbf{F}C_p$-module. By a slight but classical abuse of notation, we will write x_1 for a generator of C_p, the associated element in $\mathbf{F}C_p$ and the associated endomorphism in $\mathrm{End}_{\mathbf{F}}(M)$.

Now, remember that, since $\mathbf{F}$ is of characteristic p, the beginner's dream is true in $\mathbf{F}C_p$:

$$x_1^p - 1 = (x_1 - 1)^p \,;$$

however x_1^p is zero in C_p, so that $x_1 - \mathrm{Id}$ is a nilpotent endomorphism; it is commonly known that such morphisms are classified by their Jordan type. The Jordan form of $x_1 - \mathrm{Id}$ gives a decomposition of M into cyclic $\mathbf{F}C_p$-modules. Remark that the Jordan type of $x_1 - \mathrm{Id}$ does not depend upon the choice of x_1, so that this is well defined, and we can state that two $\mathbf{F}C_p$-modules having the same Jordan type are isomorphic. Hence the announced classification.

□

Remark. The Jordan type $[1]^{n_1} \dots [p]^{n_p}$ of the morphism x_1 is called the Jordan type of the module M.

Notation 1.1.2. For such a module M, $n_j(M)$ denotes the number of its blocks of length j, where j verifies the inequalities $1 \leq j \leq p$.

We can easily relate this block decomposition of a cyclic module to the dimension of the cohomology groups, by the following lemma.

Lemma 1.1.3. *Let M be a finitely generated $\mathbf{F}E_1$-module, then*

$$\begin{cases} \dim H^0(E_1, M) &= \sum_{j=1}^{p} n_j(M)\,, \\ \dim H^1(E_1, M) &= \sum_{j=1}^{p-1} n_j(M)\,. \end{cases}$$

The proof of this innocent lemma is left to the reader; despite its simplicity it will be our key argument in the proof of theorem A, and in the treatment of one of our examples.

1.1.2 Generalities

In order to adapt the previous method to non-cyclic groups, we will use the language of π-points. But first, we have to recall some basic facts: let A_1 and A_2 be two $\mathbf{F}$-algebras and let $\beta\colon A_1 \longrightarrow A_2$ be a morphism of $\mathbf{F}$-algebras. The morphism β induces a functor from the category of *right* modules of finite type $\mathfrak{mod}(A_2)$ to the category of *right* modules of finite type $\mathfrak{mod}(A_1)$. It is in fact known by all that every A_2-module M can be turned into an A_1-module using this external law:

$$x \cdot a_1 = x \cdot \beta(a_1)\,, \quad \forall x \in M\,, \forall a_1 \in A_1\,,$$

and it is easily seen that this construction is functorial.

Notation 1.1.4. From now on, β^* will denote the functor induced by a morphism β between two $\mathbf{F}$-algebras.

It should be immediately remarked that this functor verifies multiple properties: it is for instance additive and exact: two small facts we shall make good use of. Keep in mind that we made the choice to study right modules and not the usual left modules: the reason for this rather unconventional choice will be put into light in the second section of Chapter 3.

Definition 1.1.5. A π-point is a morphism of algebra

$$\beta\colon \mathbf{F}[T]/(T^p) \longrightarrow \mathbf{F}G\,,$$

which is flat, that is: $\beta^*(\mathbf{F}G)$ is a projective $\mathbf{F}[T]/(T^p)$-module.

Remarks. Two remarks have to be made.

Module structure It should be noticed that $\mathbf{F}[T]/(T^p)$ is isomorphic to $\mathbf{F}E_1$, where E_1 is the p-elementary abelian group of rank 1. Let us choose a generator γ of E_1 and set $\Gamma = \gamma - 1 \in \mathbf{F}E_1$, so that the isomorphism between $\mathbf{F}[T]/(T^p)$ and $\mathbf{F}E_1$ is simply given by

$$f\colon \Gamma \mapsto T\,.$$

Therefore, according to our previous discussion, every π-point β enables us to give a structure of $\mathbf{F}E_1$-module to every $\mathbf{F}G$-module.

Flatness condition The flatness condition shall not be neglected: indeed, thanks to it, the $\mathbf{F}E_1$-module $\beta^*(P)$ is projective if P is a projective $\mathbf{F}G$-module. This simple fact has major consequences relative to the cohomology: β^* induces a morphism of cohomological functors

$$\mathrm{res}_\beta \colon \hat{H}(G,-) \longrightarrow \hat{H}(E_1,-)\,.$$

Such map is written like a restriction, because it should be thought of as such: indeed, all expected properties of the restriction exposed in any textbook (for instance [Gui18, Part III]) remain true.

Definition 1.1.6. Let β_1, β_2 be two π-points.Then the π-points β_1 and β_2 are said to be equivalent if for every module M, $\beta_1^*(M)$ is projective if and only if $\beta_2^*(M)$ is projective.

Example 1.1.7. Let us consider more closely the case where G is an elementary abelian p-group of rank r, which will be written E_r.

It is well-known that given a basis $x_1, \dots, x_r$ of E_r the elements denoted $X_i = x_i - 1 \in \mathbf{F}E_r$ form a basis of $\mathbf{F}E_r$ as an $\mathbf{F}$-algebra (i is obviously between 1 and r); more precisely, $\mathbf{F}E_r \simeq \mathbf{F}[X_1, \dots, X_r]/(X_i^p)$, where (X_i^p) denotes the ideal generated by the various X_i^p. It could be shown that in this case every π-point is of the form

$$\begin{array}{rccc} \beta\colon & \mathbf{F}[T]/(T^p) & \longrightarrow & \mathbf{F}G \\ & [T] & \longmapsto & \gamma \in \mathrm{Rad}(\mathbf{F}E_r) \end{array}\,.$$

Now, according to [Car83, Lemma 6.4.], two π-points β_1, β_2 on $\mathbf{F}E_r$ are equivalent if and only if the image of $\beta_1 - \beta_2$ lies in $I^2(E_r)$ -where $I(E_n)$ is the augmentation ideal. Thus a π-point -up to equivalence- is simply a morphism

$$\begin{array}{rccc} \beta\colon & \mathbf{F}[T]/(T^p) & \longrightarrow & \mathbf{F}G \\ & [T] & \longmapsto & \sum_{i=1}^{r} b_i X_i \end{array}\,,$$

where $(b_1, \dots, b_r) \neq (0, \dots, 0)$.

Now, it is time to introduce the modules of constant Jordan type.

Definition 1.1.8. A finitely generated $\mathbf{F}G$-module M is said to be of constant Jordan type $[a_1]^{m_1} \dots [a_l]^{m_l}$, if the Jordan type of $\beta^*(M)$ is $[a_1]^{m_1} \dots [a_l]^{m_l}$ for every π-point β. Its Jordan type is called the Jordan type of M. If we omit the block of length p, we speak of *stable* Jordan type.

Remark. If M is an $\mathbf{F}'G$-module where $\mathbf{F}'$ is a field of characteristic p which is *not* algebraically closed, we say that M is of constant Jordan type if $\bar{\mathbf{F}}' \otimes_{\mathbf{F}'} M$ is of constant Jordan type, where $\bar{\mathbf{F}}'$ is of course an algebraic closure of $\mathbf{F}'$.

Examples 1.1.9.

1. Projective modules are a first example; indeed, $\mathbf{F}G$-projective modules are just direct sums of copies of $\mathbf{F}G$. Since a π-point β is flat, if P is a projective $\mathbf{F}G$-module, then $\beta^*(P)$ is a projective $\mathbf{F}E_1$-module: thus, it is a direct sum of copies of $\mathbf{F}E_1$ or, in other words, of blocks of size p. Hence a projective module is of constant Jordan type $[p]^{\frac{\dim P}{p}}$. Note in this case if G is an elementary abelian group, the converse is true: it is the famous Dade's lemma. (see [Ben16, Lemma 1.9.5])

2. Here is an example that foreshadows the proof of theorem B. Let $I(G)^*$ be the dual of the augmentation ideal of $\mathbf{F}G$, and let us show directly that it is a module of constant Jordan type. Indeed, this module is defined by the short exact sequence:

$$0 \longrightarrow \mathbf{F} \longrightarrow \mathbf{F}G \xrightarrow{\varepsilon^*} I(G)^* \longrightarrow 0\ ,$$

where ε is the norm map. Let β-be a π-point. Since β^* is an exact functor and sends projective modules to projective modules, by taking a look at the long exact sequence in cohomology, we have that

$$\dim H^1(E_1, \beta^*(I(G)^*)) = 1\,.$$

Using exactly the same trick, but one degree lower, and the well-known dimension of $I(G)^*$, we can compute the following dimension:

$$\dim H^0(E_1, \beta^*(I(G)^*)) = \frac{|G|}{p}\,.$$

Therefore, according to the lemma 1.1.3, we get

$$n_p(\beta^*(M)) = \dim H^0(E_1, \beta^*(I(G)^*)) - \dim H^1(E_1, \beta^*(I(G)^*)) = \frac{|G|}{p} - 1\,.$$

Furthermore, there is only one block whose size is not p. Because we have the following equality

$$\dim \beta^*(I(G)^*) = \dim I(G)^* = |G| - 1\,,$$

we deduce that the size of this block is $p-1$. Thus the module is of constant Jordan type $[p-1][p]^{\frac{|G|}{p}-1}$. We will later state a proposition (1.6.2), which will make obvious that $I(G)^*$ is of constant Jordan type.

Counter-example 1.1.10. Consider the $\mathbf{F}E_3$-module given by generators and relations:

$$M = \langle \alpha | \alpha \cdot X_1^{p-1} X_2^{p-1} = 0 \rangle\,;$$

this module is not of constant Jordan type. Indeed, consider the following two π-points:

$$\beta_1 \colon \Gamma \mapsto X_1\,, \quad \beta_2 \colon \Gamma \mapsto X_3\,.$$

It is easy to see that $(\beta_1)^*(M)$ has block decomposition $[p-1]^p[p]^{p(p-1)}$, each block of size p being generated by $\alpha \cdot X_2^j X_3^k$ (with $j \neq p-1$ and $0 \leq k \leq p-1$) and the blocks of size $p-1$ by the $r \cdot X_2^{p-1} X_3^k$, whereas $\beta^*(M)$ has block decomposition $[p]^{p^2-1}$, all those blocks being generated by the $\alpha \cdot X_1^j X_2^k$ where $i, j \in \{0, \ldots, p-1\}$ and (j,k) is different from $(p-1, p-1)$. In spite of it simplicity, this counterexample shall later appear in a more interesting context (see 5.3).

Further elementary examples of modules of constant Jordan type will be given later. The following proposition from [CFP08] enables us to build more modules of constant Jordan type.

Proposition 1.1.11. *The full subcategory $\mathfrak{ctJt}(\mathbf{F}G)$ of $\mathfrak{mod}(\mathbf{F}G)$ whose objects are modules of constant Jordan type is closed under direct sums, tensor products and taking the linear dual.*

Remember that if M is an $\mathbf{F}G$-module, the linear dual M^* of M is the module which, as an $\mathbf{F}$-vector space, is isomorphic to $\hom_{\mathbf{F}}(M, \mathbf{F}_p)$ and whose module structure is simply given by the law

$$f \cdot g \colon x \mapsto f(x \cdot g^{-1})\,, \quad \forall f \in M^*\,, \forall g \in G\,.$$

Within only a few lines, it can be proved that the direct sum of two modules of constant Jordan type is of constant Jordan type. It is less obvious that this class is stable under tensor product and taking the linear dual (for a proof, see [CFP08, Prop. 1.8, cor. 4.3]). The latest can even reserve some surprises: M is of constant Jordan type if and only if M^* is so, yet the Jordan type of M is not necessarily the same as the one of M^*!

Counter-example 1.1.12. In [Ben16, Example 1.13.1], for every prime p, Benson gives an example of an E_n-module M of constant Jordan type $[2][1]$, but whose dual M^* is of constant Jordan type $[1]^3$. Furthermore it is not possible to recover the *stable* Jordan type of M^* from the one of M, indeed set $p = 3$ and consider the E_n-module $N = \mathbf{F}_p \oplus I(G)$, where $I(G)$ is the augmentation ideal. The Jordan type of N is $[1][2][3]^{p^{n-1}}$ (according to [Ben16, Theorem 5.4.5]). Always according to the same theorem, the Jordan type of N^* is however similar to the one of N. Hence M and N have exactly the same stable Jordan type but their duals do not.

This first surprise should give an insight about how unusual the behaviour of the modules of constant Jordan type can be. There could be no better commentators of this that their own creators. We quote the introduction of [CFP08]: "The naivety of the approach is somewhat misleading, for underlying many theorems are somewhat difficult cohomological results."

We hope that what follows in this text is sufficient to convince the reader of the importance of group cohomology in the study of modules of constant Jordan type. However, the complexity of modules of constant Jordan type should not be underestimated: we shall only encounter already well-known modules, but many problems about the modules of constant Jordan type remain unsolved. For instance, one does not know if, given a stable Jordan type $[1]^{m_1} \dots [p-1]^{m_{p-1}}$, there exists a module whose stable Jordan type is this peculiar partition. This phenomenon occurs for very simple Jordan type: in his book [Ben16], D. Benson points out that the smallest example of this fact is the stable Jordan type $[4][1]$ for an $\overline{\mathbf{F}}_{11}(C_{11} \times C_{11})$-module.

Yet, as we will soon explain, the theory of modules of constant Jordan type for elementary abelian p-groups may be introduced in fewer words and in an ever more naive way.

1.1.3 An exact structure

The category of modules of constant Jordan type may be seen as an exact category, but not with the usual short exact sequences. We should consider instead the *locally split short exact sequences*.

Definition 1.1.13. A *locally split short exact sequence* of modules of constant Jordan type is a short exact sequence of modules of constant Jordan type

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0 \ ,$$

such that for every π-point β, the short exact sequence

$$0 \longrightarrow \beta^*(L) \xrightarrow{f} \beta^*(M) \xrightarrow{g} \beta^*(N) \longrightarrow 0$$

is split.

We do not give any example yet. Later, there will be however two noteworthy examples: the short exact sequence

$$0 \longrightarrow \omega_{-1}(\mathbf{F}_p) \xrightarrow{\kappa} \omega_2(\mathbf{F}_p) \longrightarrow J(\mathbf{K}) \longrightarrow 0$$

appearing in Proposition C is *not* locally split exact, although every module in this short exact sequence is of constant Jordan type, but if we "shift" it, so that it becomes

$$0 \longrightarrow \omega_3(\mathbf{F}_p) \longrightarrow \omega(J(\mathbf{K})) \longrightarrow \omega_{-1}(\mathbf{F}_p) \longrightarrow 0 \ ,$$

we get a locally split short exact sequence.

As mentioned earlier, one of the main interest of those short exact sequences lies in the fact that we could give a bit more structure to the category of modules of constant Jordan type.

Proposition 1.1.14. *The category* $\mathfrak{ctJt}(G)$ *endowed with the locally split short exact sequences is an exact category.*

As always, the proof can be read in [Ben16, §5.3].

1.1.4 Another point of view

When $G = E_n$, we could have introduced the modules of constant Jordan type in a more elementary way, like D. Benson did in his book ([Ben16]).

Consider $(e_i)_{1 \leq i \leq n}$ a basis of E_n. An $\mathbf{F}E_n$ module V is but an $\mathbf{F}$-vector space V endowed with a group homomorphism $\psi \colon E_n \longrightarrow \mathrm{Gl}(V)$. Since ψ is a group homomorphism, $\psi(e_i)^p = \mathrm{Id}$,

hence $\psi(e_i) - \mathrm{Id}$ is nilpotent of order at most p. Furthermore this morphism is perfectly defined by its image on the basis $(e_i)_{1\leq i\leq n}$, thus an E_n-module V is just the data of n nilpotent matrices $X_1, \dots, X_n$ whose order is at most p and which commute. Put this together with the description of π-points that we gave earlier (see the example in §1.1.7), we could have used this definition instead:

Proposition 1.1.15. *The couple $(V, \{X_1, \dots, X_n\})$ is a module of constant Jordan type if and only if the Jordan type of the matrix*

$$X_\beta = \sum_{i=1}^{n} \beta_i X_i\,, \quad \beta = (\beta_1, \dots, \beta_n) \in \bar{\mathbf{F}}^n \backslash (0, \dots, 0)$$

is independent from the choice of β.

It should be pointed out, that the proposition is not so obvious as one could think at first glance: indeed numerous choices were made, and it should be proved that they do not affect the definition at all, which is not trivial. For a complete proof of this, see [Ben16].

Example 1.1.16. Consider $V = \bar{\mathbf{F}}_2^{10}$ on which $G = C_2^3$ acts, let us call X_i the matrix of the action of $e_i - 1$ in a peculiar basis. Those matrices commute and are nilpotent. We then get that the 10×10 matrix

$$aX_1 + bX_2 + cX_3 = \begin{pmatrix} & & & & & & & & & \\ & & & & & & & & & \\ & & & & & & & & & \\ & & & & & & & & & \\ & & & & & & & & & \\ b & c & & & a & & & & & \\ & a & & & b & & & & & \\ c & & & b & & & a & & & \\ & & & & & c & b & & & \\ & & & & a & & c & & & \end{pmatrix},$$

where a, b, c are in an algebraic closure of $\mathbf{F}_2$ has constant rank 4, as long as $(a, b, c) \neq (0, 0, 0)$ and therefore the module $(V, \{X_1, X_2, X_3\})$ is of constant Jordan type.

In fact, this module arise in Galois theory: let $\mathbf{K} = \mathbf{Q}_2(\sqrt{2}, \sqrt{-1}, \sqrt{5})$, then the module $(V, \{X_1, X_2, X_3\})$ is isomorphic to the $Gal(\mathbf{K}/\mathbf{Q}_2)$-module $\mathbf{K}^\times/\mathbf{K}^{\times 2}$.

1.1.5 Associated vector bundles

In [FP11], J. Pevtosva and E. Friedlander associated to every module of constant Jordan type a vector bundle in a functorial way. Introducing those functors would require a lot of work, and since they do not play a major role in our study, exhibiting this construction does not seem useful to the understanding of our results. Therefore we will not explain how they arise, nor define them: the curious reader may consult [Ben16, Chapter 8], where the functor called here $\mathfrak{V}$ is called $\mathcal{F}_{0,1}$.

In this section, we set $G = E_r$ for a peculiar $r \in \mathbf{N}$. Let $\mathbf{P}_{\mathbf{F}}^{r-1}$ be the projective space corresponding to the affine space $\mathbf{F}[Y_1, \dots, Y_r]$, and let $\mathcal{O}$ be its structural sheaf (see [EH01, §I.2.4]). We set $\mathcal{O}(j) = \mathcal{O}^{\otimes j}$, and if $\mathfrak{F}$ is an $\mathcal{O}$-module, we write $\mathfrak{F}(j) = \mathfrak{F} \otimes_{\mathcal{O}} \mathcal{O}(j)$.

Theorem 1.1.17. *There exists a functor $\mathfrak{V}$ from the category of $\mathbf{F}E_r$-modules of constant Jordan type to the category of vector bundles over $\mathbf{P}_{\mathbf{F}}^{r-1}$. More precisely, if M is a module of constant Jordan type $[p]^{m_p} \dots [1]^{m_1}$, then $\mathfrak{V}(M)$ is a vector bundle of rank m_1. Furthermore, this functor has the following properties:*

1. *$\mathfrak{V}$ is exact,*

2. *it verifies the following relations*

$$\begin{aligned} \mathfrak{V}(M^*) &= \mathfrak{V}(M)^\wedge\,, \\ \mathfrak{V}(\omega_2(M)) &= \mathfrak{V}(M)(-p)\,, \end{aligned}$$

where $\mathfrak{V}(M)^\wedge$ *is the dual bundle of* $\mathfrak{V}(M)$.

Example 1.1.18. It could be showed that

$$\mathfrak{V}(\mathbf{F}) = \mathcal{O}\,.$$

1.2 Some basics about the Frattini subgroup

The structure of the pro-p-groups is at the core of our work, we shall recall some facts without any proof: they will be used along this text, although they will never be explicitly mentioned after this section. We follow closely [DDSMS99, Chapter 1]: the reader might found the lacking proofs in it.

Definition 1.2.1. Let $\mathcal{G}$ be a pro-p-group. The Frattini subgroup of $\mathcal{G}$ is the subgroup

$$\Phi(\mathcal{G}) = \bigcap\{\mathcal{H} \,|\, \mathcal{H} \text{ is a maximal proper open subgroup of } \mathcal{G}\}\,.$$

We mention here some of the main interests of the Frattini subgroup.

Proposition 1.2.2. *Let* $\mathcal{G}$ *be a pro-p-group. Then its Frattini subgroup verifies the following properties:*

1. *the subgroup* $\Phi(\mathcal{G})$ *is normal and closed in* $\mathcal{G}$.
2. *if* $\mathcal{K}$ *is a closed normal subgroup of* $\mathcal{G}$ *contained in* $\Phi(\mathcal{G})$, *then* $\Phi(\mathcal{G}/\mathcal{K}) = \Phi(\mathcal{G})/\mathcal{K}$.
3. *let* X *be a subset of* $\mathcal{G}$ *then, the following conditions are equivalent:*
   (a) X *generates* $\mathcal{G}$ *topologically;*
   (b) $X \bigcup \Phi(\mathcal{G})$ *generates* $\mathcal{G}$ *topologically;*
   (c) $X\Phi(\mathcal{G})/\Phi(\mathcal{G})$ *generates* $\mathcal{G}/\Phi(\mathcal{G})$ *topologically.*

The definition above is of little help, we will rather use this useful characterisation:

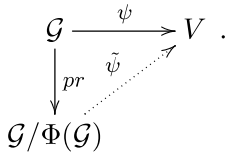
Proposition 1.2.3. *Let* $\mathcal{G}$ *be a pro-p-group, then*

$$\Phi(\mathcal{G}) = \overline{\mathcal{G}^p(\mathcal{G},\mathcal{G})}\,,$$

where $(\mathcal{G},\mathcal{G})$ *is the derived subgroup of* $\mathcal{G}$, *which means the normal subgroup generated by the commutators* (x,y), *and* $\mathcal{G}^p$ *is the subgroup generated by the elements* g^p, *where* $g \in \mathcal{G}$. *Furthermore, if* $\mathcal{G}$ *is finitely generated, then* $\mathcal{G}^p(\mathcal{G},\mathcal{G})$ *is already closed.*

From now on, we shall only consider finitely generated pro-p-groups $\mathcal{G}$, which means that $\mathcal{G}/\Phi(\mathcal{G})$ is finite.

Remark. Let $\mathcal{G}$ be a finitely generated pro-p-group. The subgroup $\Phi(\mathcal{G})$ verifies the following universal property: let $\psi\colon \mathcal{G} \longrightarrow V$ a morphism of pro-p-groups where V is an $\mathbf{F}_p$-vector space, then there exists a map $\tilde{\psi}\colon \mathcal{G}/\Phi(\mathcal{G}) \longrightarrow V$ making the following diagram commutative:



In other words, $\mathcal{G}/\Phi(\mathcal{G})$ is *the* biggest quotient which is a vector space. Biggest meaning here that it is of maximal dimension.

1.3 Local fields

Now, it is time to introduce the extensions which are at the heart of this dissertation. Let $\mathbf{k}$ be a local field which contains a primitive p-th root of unity and let us fix $\bar{\mathbf{k}}$ an algebraic closure of $\mathbf{k}$. We set $\mathbf{K}$ a Galois p-extension of finite type of $\mathbf{k}$ whose Galois group called G verifies that its cohomology ring (with coefficients in $\mathbf{F}_p$) is Cohen-Macaulay. Bear in mind that, because of J. Duflot's theorem ([Duf81]), if G is an elementary abelian p-group which is not cyclic, this assumption holds. In spite of their ingenuity, such groups play a major role in field theory.

The study of $J(\mathbf{K}) = \mathbf{K}^\times/\mathbf{K}^{\times p}$ will lead us to the study of some other extensions, as we shall see hereafter. Let us put $\mathcal{R} = \{x \in \bar{\mathbf{k}} | x^p \in \mathbf{K}\}$ and $\mathbf{K}^{(2)} = \mathbf{K}[\mathcal{R}]$, so that we have the following diagram of extensions.

$$\begin{array}{c} \mathbf{K}^{(2)} \\ | \\ \mathbf{K} \\ | \\ \mathbf{k} \end{array}$$

According to the previous diagram we have the following exact sequence

$$0 \longrightarrow Gal(\mathbf{K}^{(2)}/\mathbf{K}) \longrightarrow Gal(\mathbf{K}^{(2)}/\mathbf{k}) \longrightarrow Gal(\mathbf{K}/\mathbf{k}) \longrightarrow 0 \ .$$

Therefore it is abundantly clear that $G := Gal(\mathbf{K}/\mathbf{k})$ acts on $Gal(\mathbf{K}^{(2)}/\mathbf{K})$ by conjugation. Furthermore, as an $\mathbf{F}_pG$-module $Gal(\mathbf{K}^{(2)}/\mathbf{K})$ is related to $J(\mathbf{K})$ via *Kummer theory*. Let us recall the basics.

Remember first that a field extension $\mathbf{L}/\mathbf{L}_0$ is an *n-Kummer extension* if it is simply a Galois extension such that $Gal(\mathbf{L}/\mathbf{L}_0)$ is an abelian group of exponent dividing n, and if $\mathbf{L}_0$ contains a primitive n-th root of unity. Like in Galois theory, there is a correspondence theorem.

Theorem 1.3.1 (Kummer theory)**.** *Let $\mathbf{L}_0$ be a field containing a primitive n-th root of unity and fix an algebraic closure $\bar{\mathbf{L}}_0$ of $\mathbf{L}_0$. The n-Kummer extensions $\mathbf{L}$ of $\mathbf{L}_0$ contained in $\bar{\mathbf{L}}_0$ are in 1-to-1 correspondence with the subgroups of $\mathbf{L}_0^\times/\mathbf{L}_0^{\times n}$; moreover the correspondence maps the subgroup H to the field $\mathbf{L}_0[x^{\frac{1}{n}}, [x] \in H]$, and is thus order-preserving. Finally, if a field $\mathbf{L}$ and a subgroup H are in correspondence, then* $\hom(Gal(\mathbf{L}/\mathbf{L}_0), \mathbf{Z}/n\mathbf{Z}) \cong H$.

See [Gui18, Theorem 1.25]. From this theorem and the previous considerations we can deduce two key facts (with $n = p$ in both cases).

First, the group $Gal(\mathbf{K}^{(2)}/\mathbf{K})$ is simply an elementary abelian p-group and in particular an $\mathbf{F}_p$-vector space.

Secondly, the theorem applied to the base field $\mathbf{K}$ implies, by maximality, that $\mathbf{K}^{(2)}$ is in correspondence with $J(\mathbf{K})$ (note that all p-Kummer extensions of $\mathbf{K}$ are contained in $\mathbf{K}^{(2)}$). It follows that $\hom(Gal(\mathbf{K}^{(2)}/\mathbf{K}), \mathbf{F}_p)$ is isomorphic to $J(\mathbf{K})$, and this is really an isomorphism of $\mathbf{F}_pG$ *modules*: indeed this is the refinement brought by equivariant Kummer theory (see [Gui18, Theorem 1.26]).

A more elaborate result, which we call Tate duality (cf. [Gui18, Theorem 13.21]), states that $J(\mathbf{K})$ is self-dual, as a module, as long as $\mathbf{k}$ contains a primitive p-th root of unity, which is fortunately the case here.

We summarize this discussion in the following lemma:

Lemma 1.3.2. *There is an isomorphism of $\mathbf{F}_pG$-modules between $Gal(\mathbf{K}^{(2)}/\mathbf{K})$, $J(\mathbf{K})$ and $J(\mathbf{K})^*$.*

Notation 1.3.3. From now on, we set $J = J(\mathbf{K}) = \mathbf{K}^\times/\mathbf{K}^{\times p}$.

According to the previous lemma and Proposition 1.1.11, instead of trying to study J, we can turn our attention to its dual namely $Gal(\mathbf{K}^{(2)}/\mathbf{K})$ and use techniques from group theory.

Let us write $\mathbf{L}(p)$ for the largest pro-p extension of the field $\mathbf{L}$, and put $\mathcal{G}_{\mathbf{L}}(p) = Gal(\mathbf{L}(p)/\mathbf{L})$. Let $\mathcal{H}$ the subgroup of $\mathcal{G}_{\mathbf{k}(p)}$ in Galois correspondence with $\mathbf{K}$. It is not hard to see that $\mathbf{K}^{(2)}$ is in correspondence with $\Phi(\mathcal{H})$, using the maximality condition defining this extension and the one defining the Frattini subgroup. We can therefore state the following lemma:

Lemma 1.3.4. *There is an isomorphism $J^* \cong \mathcal{H}/\Phi(\mathcal{H})$, as modules over $\mathbf{F}_pG$ where $G = \mathcal{G}_{\mathbf{k}}(p)/\mathcal{H}$.*

1.4 The main theorems

Thanks to the previous lemma, we have completely translated the problem arising from Galois theory into a group-theoretic one; not only does this formulation enable us to solve the problem, but we can now rephrase all major results of this dissertation in the two following theorems. But before we set the following notation.

Notation 1.4.1. For any p-group G, we set $d_i(G) = \dim H^i(G, \mathbf{F}_p)$.

Theorem 1.4.2 (First main theorem)**.** *Let $\mathbf{k}$ be a local field and let $\mathcal{G}_{\mathbf{k}}(p)$ be the Galois group of a maximal pro-p-extension. Consider a closed normal subgroup of finite index $\mathcal{H}$ of $\mathcal{G}_{\mathbf{k}}(p)$ and put $J = \hom(\mathcal{H}/\Phi(\mathcal{H}), \mathbf{F}_p)$ and $G = \mathcal{G}_{\mathbf{k}}(p)/\mathcal{H}$.*

We have the following possibilities for the cohomology of G with coefficients in J.

1. *If $\mathbf{k}$ does not contain a primitive p^{th} root of unity, then for all $s \in \mathbf{Z}$:*

$$\begin{cases} \hat{H}^s(G, J) & = & \hat{H}^{s+2}(G, \mathbf{F}_p) \\ H^0(G, J) & \simeq & \mathbf{F}_p^{d_2(G)+n-d_1(G)} \end{cases}.$$

2. *Suppose that $\xi_p \in \mathbf{k}$ and $H^\bullet(G, \mathbf{F}_p)$ is a Cohen-Macaulay ring, then we have to distinguish between two cases*

   (a) *if the inflation map* $\inf\colon H^2(Gal(\mathbf{K}/\mathbf{k}), \mathbf{F}_p) \longrightarrow H^2(\mathcal{G}_{\mathbf{k}}(p), \mathbf{F}_p)$ *is zero, the following isomorphisms hold:*

$$\begin{cases} H^s(G, J) & \simeq & \hat{H}^{s+2}(G, \mathbf{F}_p) \oplus H^{s-2}(G, \mathbf{F}_p), \quad s \geq 1 \\ H^0(G, J) & \simeq & \mathbf{F}_p^{d_2(G)+(n-d_1(G))} \end{cases}.$$

   (b) *if the inflation map* $\inf\colon H^2(Gal(\mathbf{K}/\mathbf{k}), \mathbf{F}_p) \longrightarrow H^2(\mathcal{G}_{\mathbf{k}}(p), \mathbf{F}_p)$ *is non-zero then*

$$\begin{cases} H^1(G, J) & \simeq & H^3(G, \mathbf{F}_p) \\ H^s(G, J) & \simeq & H^{s+2}(G, \mathbf{F}_p) \oplus H^{s-2}(G, \mathbf{F}_p), \quad s \geq 2 \\ H^0(G, J) & \simeq & \mathbf{F}_p^{d_2(G)-1+(n-d_1(G))} \end{cases}.$$

Theorem 1.4.3 (Second main theorem)**.** *Under the same hypothesis over $\mathbf{k}$ and using the same notation, the G-module J^**

- *is of constant Jordan type, and its stable Jordan type is $[1]$, if $\mathbf{k}$ does not contain a primitive p^{th}-root of unity,*
- *is of constant Jordan type, and its stable Jordan type is $[1]^2$, if $\mathbf{k}$ does contain a primitive p^{th}-root of unity and G is an elementary abelian p-group.*

Note that in the case where $\mathbf{k}$ does not contain a primitive p^{th}-root of unity, there is no such thing as Kummer theory; therefore there is no isomorphism between $\mathbf{K}^\times/\mathbf{K}^{\times p}$ and $\mathcal{H}/\Phi(\mathcal{H})$, so that this formulation of the theorem is the only one available. It should be remarked that J reflects some differences between those fields and their arithmetic. By the bye, note that we have introduced the following notation:

Remember that for any p-group G, we set $d_i(G) = \dim H^i(G, \mathbf{F}_p)$ (see Notation 1.4.1).

The next chapter of the dissertation is devoted to the proof of those theorems (which implies, in particular, the statements of Theorems A and B from the introduction, of course). Before we turn to this however, we need to continue with more background material.

1.5 Demuškin groups

The Galois groups of maximal pro-p-extensions of local fields are explicitly known: indeed if $\mathbf{L}$ is a local field such that $\xi_p \in \mathbf{L}$, then $\mathcal{G}_\mathbf{L}(p)$ is a *Demuškin group*. A presentation by generators and relations of such groups was given by J. Labute (see [Lab67]), which we recall first for $p \neq 2$:

$$\mathcal{D}_{k,2s} = \langle x_1, \dots, x_{2s} | x_1^{p^k}(x_1, x_2)(x_3, x_4)\dots(x_{2s-1}, x_{2s}) = 1 \rangle ,$$

where k is the maximal integer such that $\xi_{p^k} \in \mathbf{L}$ and $2s$ is the dimension of $J(\mathbf{L})$.

When $p = 2$, the relation in the Demuškin group changes. If the number of generators is odd, it becomes

$$\mathcal{D}_{f,n=2s+1} = \langle x_1, \dots, x_{2s+1} | x_1^2 x_2^f (x_2, x_3)(x_4, x_5)\dots(x_{2s}, x_{2s+1}) = 1 \rangle .$$

However, if the number of generators is even, the relation is either

$$\mathcal{D}_{f,n=2s} = \langle x_1, \dots, x_{2s} | x_1^{2+2^f}(x_1, x_2)(x_3, x_4)\dots(x_{2s-1}, x_{2s}) = 1 \rangle ,$$

or

$$\mathcal{D}'_{f,n=2s} = \langle x_1, \dots, x_{2s} | x_1^2(x_1, x_2)x_3^{2^f}(x_3, x_4)\dots(x_{2s-1}, x_{2s}) = 1 \rangle .$$

In each case f is an integer such that $f \geq 2$.

We complete this review of the possible descriptions for $\mathcal{G}_\mathbf{L}(p)$ with the case when $\mathbf{L}$ does not contain a primitive p^{th}-root of unity: in this situation $\mathcal{G}_\mathbf{L}(p)$ is just a free prop-p-group ([Ser94, Theorem 3, II, §5]).

1.6 The stable module category and Heller shifts

We have to introduce some new modules: our key argument is yet very simple (it is just a short exact sequence), but we have to explain some classical notation and objects. Here we just follow [CTVEZ03, §2.5 sq.], so we consider a finite group G and a field $\mathbf{F}$ (whose characteristic p typically divides the order of G).

Let M be an $\mathbf{F}G$-module of finite type, let $\pi\colon P \longrightarrow M$ an epimorphism from a projective module onto M. Its kernel denoted $\Omega(M)$ is called the *Heller shift* of M; it always exists, however it is only defined up to a projective summand. That is why we have to introduce the *stable* module category $\underline{\mathfrak{mod}}(\mathbf{F}G)$ whose objects are but $\mathbf{F}G$-modules, and whose hom sets, written $\underline{\hom}$, are defined by

$$\underline{\hom}(M, N) = \hom_{\mathbf{F}G}(M, N)/P_{M,N} ,$$

where $P_{M,N}$ is the subspace of morphisms which factor through a projective. Then Ω becomes a well-defined functor on the stable category.

We should immediately remark that we can iterate Ω and set without ambiguity $\Omega^{i+1}(M) = \Omega(\Omega^i(M))$ and so on. Dualizing this construction (i.e. taking the cokernel of a monomorphism from M into a projective module) gives birth to $\Omega^{-1}(M)$ and then we can again iterate such a

construction. We would like to emphasize the fact that $\Omega(M)$ is not well-defined in the category of modules but in the stable category; usually $\omega(M)$ will be our notation for *some* module whose image in $\underline{\mathfrak{mod}}(\mathbf{F}G)$ is isomorphic to $\Omega(M)$, though we will repeat this for emphasis.

Furthermore the previous construction is natural: Ω is an endo-functor of $\underline{\mathfrak{mod}}(\mathbf{F}G)$ and an equivalence of category whose quasi inverse is, as expected, Ω^{-1}. We may hope that it adds a little bit of structure to $\underline{\mathfrak{mod}}(\mathbf{F}G)$. In fact $(\underline{\mathfrak{mod}}(\mathbf{F}G), \Omega^{-1})$ is a triangulated category: given a short exact sequence in $\mathfrak{mod}(\mathbf{F}G)$

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0 \ ,$$

it is possible to build maps $(\tilde{\alpha}, \tilde{\beta}, \gamma)$ in the stable module category in such a way the class of α (resp.β) is $\tilde{\alpha}$ (resp. $\tilde{\beta}$) and $\gamma\colon N \longrightarrow \Omega^{-1}(L)$, so that the distinguished triangles are all the triangles isomorphic to one of the form:

$$L \xrightarrow{\tilde{\alpha}} M \xrightarrow{\tilde{\beta}} N \xrightarrow{\gamma} \Omega^{-1}(L) \ . \tag{1.1}$$

We summarize in the following proposition :

Proposition 1.6.1. *The additive category $\underline{\mathfrak{mod}}(\mathbf{F}G)$, equipped with the functor Ω^{-1} and whose distinguished triangles are the ones described above, is a triangulated category.*

Remarks.

1. One of the main interests of Ω is the fact that it may give a new definition of Tate cohomology, namely

$$\hat{H}^k(G, M) \simeq \underline{\hom}(\Omega^{s+k}(\mathbf{F}_p), \Omega^s(M)) \, , \quad \forall s,\, k \in \mathbf{Z} \, .$$

2. Let us consider the following exact sequence in $\mathfrak{mod}(\mathbf{F}G)$:

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0 \ .$$

Since the cone of a map in a triangulated category is unique up to isomorphism, the module N is stably isomorphic to the cone of α.

We will consider in particular the stable modules $\Omega^{-1}(\mathbf{F})$ and $\Omega^2(\mathbf{F})$ when G is a p-group, indeed, when $\mathcal{G}_{\mathbf{k}}(p)$ is a Demuškin group, the crucial statement will be the existence of a short exact sequence of modules

$$0 \longrightarrow \omega_{-1}(\mathbf{F}_p) \longrightarrow \omega_2(\mathbf{F}_p) \longrightarrow J^* \longrightarrow 0 \ , \tag{*}$$

which will enable us to compute the cohomology groups $H^i(E_1, \beta^*(J^*))$ for every π-point β. The precise description of those modules will be detailed hereafter (see the discussion in §2.1.) Indeed it is worth noting that $\beta^*\colon \mathfrak{mod}(\mathbf{F}_pG) \longrightarrow \mathfrak{mod}(\mathbf{F}_pE_1)$ induces a functor of triangulated categories between $\underline{\mathfrak{mod}}(\mathbf{F}_pG)$ and $\underline{\mathfrak{mod}}(\mathbf{F}_pE_1)$, since it is flat.

It is also noteworthy that the category of constant Jordan type modules is stable under Heller shifts: to be more precise, we can state the following theorem:

Theorem 1.6.2. *A module M is of constant Jordan type, if and only if any module which is stably isomorphic to $\Omega(M)$ is of constant Jordan type.*

A proof can be found -as for everything dealing with modules of constant Jordan type- in [CFP08]. Since the trivial module $\mathbf{F}_p$ is obviously of constant Jordan type, the modules $\omega_2(\mathbf{F}_p)$ and $\omega_{-1}(\mathbf{F}_p)$ which appear in the previous exact sequence are also of constant Jordan type: even better, we know their Jordan type, such as stated in the following remark.

Remark. Every module which is stably isomorphic to $\omega_2(\mathbf{F}_p)$ is of constant Jordan type and its stable Jordan type is [1] (see [CFP08, Theorem 5.6]).

For what concerns the module $\omega_{-1}(\mathbf{F}_p)$, it is already known to the reader: as it shall be proved later, it is $I(G)^*$ whose stable constant Jordan type is $[p-1]$ (see Example 1.1.9).

As pointed out earlier, for an object M in $\underline{\mathfrak{mod}}(\mathbf{F}G)$, there are many modules in $\mathfrak{mod}(\mathbf{F}G)$ whose equivalence class in the stable category is isomorphic to $\Omega(M)$. Yet, there exists a module without any projective summand in it and which is stably isomorphic to $\Omega(M)$. By a very slight abuse of notation, we denote such a (*usual*) module verifying *both* conditions $\Omega(M)$: indeed asking the absence of projective summand ensures the uniqueness of a representative (see[Car96, p.14]). To be precise, in this dissertation if we speak about the module (and not the stable module) $\Omega^1(\mathbf{F}_p)$ we refer to the augmentation ideal of G written $I(G)$ (and $\Omega^{-1}(\mathbf{F}_p)$ its dual), moreover $\Omega^2(\mathbf{F}_p)$ will be the kernel of the application

$$\begin{array}{rcl}(\mathbf{F}_pG)^{|G|} = \langle e_g, g \in G\rangle & \longrightarrow & I(G) \\ e_g & \longmapsto & X_g = g-1\end{array}.$$

We will encounter this module later (see Chapter 3).

1.7 A first half of the theorem

Now we can prove half of the theorems, which is in fact a simple rephrasing of a a well-known theorem, so well-known among the specialists, that it is hard to know who should take credit for it. A reader interested by this case in the history of a theorem could refer to one article from W. Magnus ([Mag39]), a note on this article by N. Blackburn ([Bla69]), a letter in J.-P. Serre's correspondence and an article of W. Gaschütz ([Gas54]).

Proposition 1.7.1. *Let $\mathcal{F}_n$ be the free pro-p-group of rank n and $\tilde{\mathcal{H}}$ be a closed subgroup of $\mathcal{F}_n$. Let $G = \mathcal{F}_n/\tilde{\mathcal{H}}$, then $\tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}})$ is stably isomorphic as a G-module to $\Omega^2(\mathbf{F}_p)$.*

A conceptual proof of this fact can be found in [Fri95] and a more down-to-earth using Fox derivatives is implicitly present in [Bla69]. Here, the word "implicitly" means that the reader has just to add "pro-p" every where it makes sense and read "Frattini subgroup" instead of "derived subgroup". Later in Chapter 3, we will give a very elementary proof, not exactly of this proposition, but only of a case covered by it. Yet this peculiar one will be quite useful, especially in Chapter 4.

This proves the main theorem when $\mathcal{G}_{\mathbf{k}}(p)$ is a free pro-p-group. Indeed, by definition

$$\hat{H}^s(G, \Omega^2(\mathbf{F}_p)) \simeq \hat{H}^{s-2}(G, \mathbf{F}_p)\,;$$

moreover such module is of constant Jordan type and its stable Jordan type is [1], as pointed out in the remark above (in §1.6, after Theorem 1.6.2). Only one piece of information is missing: the dimension of the fixed points of $(\tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}}))^*$ under the action of G. Thanks to the spectracl sequence associated to the short exact sequence

$$1 \longrightarrow \mathcal{H} \longrightarrow \mathcal{F}_n \longrightarrow G \longrightarrow 1$$

we have the following five term exact sequence ([NSW08, Cor. 2.4.2]):

$$0 \longrightarrow H^1(G, \mathbf{F}_p) \longrightarrow H^1(\mathcal{F}_n, \mathbf{F}_p) \longrightarrow H^1(\tilde{\mathcal{H}}, \mathbf{F}_p)^G \longrightarrow H^2(G, \mathbf{F}_p) \longrightarrow H^2(\mathcal{F}_n, \mathbf{F}_p)\ .$$

It is well known that $\hat{H}^2(\mathcal{F}_n, \mathbf{F}_p) = 0$ ([Ser94]) and that $H^1(G, \mathbf{F}_p) = d_1(G)$ by definition, because we set $d_i(G) = \dim H^i(G, \mathbf{F}_p)$ (see Theorem 1.4.2). Now, let us inspect $H^1(\tilde{\mathcal{H}}, \mathbf{F}_p)^G$, we have indeed

$$\begin{array}{rcll} H^1(\tilde{\mathcal{H}}, \mathbf{F}_p)^G & \simeq & (\hom(\tilde{\mathcal{H}}, \mathbf{F}_p))^G & (\mathbf{F}_p \text{ is a trivial module}) \\ & \simeq & \hom(\tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}}), \mathbf{F}_p)^G & (\text{by the property of the Frattini subgroup}) \end{array}$$

This litany of isomorphisms will be often used in this dissertation. Therefore we can state the following equality

$$\dim H^0(G, (\tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}}))^*) = d_2(G) + (n - d_1(G))\,.$$

We then need this basic lemma:

Lemma 1.7.2. *Let G be a finite p-group, and let M be a finitely generated $\mathbf{F}_pG$-module. Now set*

$$n = \dim H^0(G, M) - \dim \hat{H}^0(G, M)\,,$$

then $M = M_1 \oplus (\mathbf{F}_pG)^n$ where M_1 is an $\mathbf{F}_pG$-module without any projective summand.

Proof. Let us decompose M as

$$M = M_1 \oplus P\,,$$

where P is a projective module and M_1 has no projective summand: such decomposition may always be found, since P is a projective $\mathbf{F}G$-module, hence an injective one. In fact, we may suppose that $P = (\mathbf{F}_pG)^m$, since projective $\mathbf{F}_pG$-modules are free. We would like to show that $m = n$. To this end, let us remark

$$\hat{H}^0(G, M) = \hat{H}^0(G, M_1)\,.$$

Since $\dim \hat{H}^0(G, M_1) + m = \dim H^0(G, M)$, it remains to prove that

$$\dim H^0(G, M_1) = \dim \hat{H}^0(G, M_1)\,.$$

If this were not the case, there would be an element $x \in M_1$ such that $x \cdot \mathrm{N} \neq 0$ (where N is the norm) so that there would be a projective summand in M_1 (see [Gui18, Lemma 1.31], which is absurd. □

Now, we can properly compute $H^0(G, \tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}}))$. Indeed, since $\tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}})$ is stably isomorphic to $\Omega^2(\mathbf{F}_p)$, its dual is stably isomorphic to $\Omega^{-2}(\mathbf{F}_p)$, hence

$$\dim H^0(G, (\tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}}))^*) - \dim \hat{H}^0(G, (\tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}}))^*) = n - d_1(G)\,,$$

where $d_i(G) = \dim_{\mathbf{F}_p} \hat{H}^i(G, \mathbf{F}_p)$. According to the previous lemma

$$(\tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}}))^* = \Omega^{-2}(\mathbf{F}_p) \oplus (\mathbf{F}_pG)^{n-d_1(G)}\,,$$

where $\Omega^{-2}(\mathbf{F}_p)$ is a module without any projective summand and stably isomorphic to $\Omega^{-2}(\mathbf{F}_p)$, hence its dual is isomorphic to $\Omega^2(\mathbf{F}_p)$. Since there is no projective summand

$$\dim H^0(G, \Omega^{-2}(\mathbf{F}_p)^*) = \dim \hat{H}^0(G, \Omega^{-2}(\mathbf{F}_p)^*) = \dim \hat{H}^{-2}(G, \mathbf{F}_p) = d_1(G)\,.$$

Now, we can easily conclude:

$$\dim H^0(G, \tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}})) = n - d_1(G) + \dim H^0(G, \Omega^{-2}(\mathbf{F}_p)^*)$$

Hence we obtain the expected result:

$$\dim H^0(G, \tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}})) = n\,.$$

Alternatively, we could have used [Gas54, Satz 2].
It now remains to confront the case where $\mathcal{G}_{\mathbf{k}}(p)$ is a Demuškin group.

Chapter 2

Proof of the main theorems

In this chapter, as in the previous one, p is a prime number, $\mathbf{k}$ is a local field and $\mathcal{G}_{\mathbf{k}}(p)$ is the Galois group of a maximal pro-p-extension of $\mathbf{k}$. From now on, we assume that $\mathcal{G}_{\mathbf{k}}(p)$ is a Demuškin group. In order to simplify our proofs, we will assume below that $p \neq 2$, unless we explicitly write otherwise. All results in this chapter do still remain true when $p = 2$, with some slight changes which we will indicate along the text. Let us fix then n and k such that

$$\mathcal{G}_{\mathbf{k}}(p) = \mathcal{D}_{k,n}\,.$$

We treat this as an equality rather than an isomorphism, which is tantamount to choosing generators for the group once and for all.

Our objective is the proof of Theorem 1.4.2 and Theorem 1.4.3, in the case when $\xi_p \in \mathbf{k}$, so that the above group-theoretical hypotheses are in force. As previously mentioned, our key argument is a short exact sequence: we shall prove it first, and then draw the consequences from it. No mention of Galois theory will be made, since we have already translated the problem of studying $J(\mathbf{K}) = \mathbf{K}^\times/\mathbf{K}^{\times p}$ into a problem of group theory.

Throughout this chapter, we fix a finite p-Galois extension $\mathbf{K}/\mathbf{k}$, and we denote by G its Galois group. We assume that G is a quotient of $\mathcal{D}_{k,n}$ and we denote by $\mathcal{H}$ the normal subgroup of $\mathcal{D}_{k,n}$ such that $G = \mathcal{D}_{k,n}/\mathcal{H}$. In section 2.2, we suppose that G is non-cyclic, whereas we assume the converse in section 2.3.

2.1 The short exact sequence...

As previously recalled, the Demuškin group $\mathcal{D}_{k,n}$ is but a quotient of the free pro-p-group on n generators $x_1, \ldots, x_n$, denoted here $\mathcal{F}_n$, by the normal subgroup generated by $x_1^{p^k}(x_1, x_2)\ldots(x_{n-1}, x_n)$. This element will be denoted δ and we set

$$\pi\colon \mathcal{F}_n \longrightarrow \mathcal{D}_{k,n}\,,$$

the canonical projection. If $p = 2$, then δ should be changed, and we have to distinguish multiple cases (see 1.5), however what follows remains true without any change.

Now, let us construct the epimorphism in the short exact sequence appearing in Proposition C, which means a map from a module $\omega_2(\mathbf{F}_p)$ (stably isomorphic to $\Omega^2(\mathbf{F}_p)$) onto J^*. Remember that $J^* = \mathcal{H}/\Phi(\mathcal{H})$. So we set

$$\tilde{\mathcal{H}} = \pi^{-1}(\mathcal{H})\,.$$

According to Proposition 1.2.3, there exists an $\mathbf{F}_p$-linear map from $\tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}})$ onto $\mathcal{H}/\Phi(\mathcal{H})$. Moreover, this map is a morphism of G-modules.

Indeed, first, note that $\mathcal{F}_n/\tilde{\mathcal{H}}$ is isomorphic to G: since $\ker\pi$ is equal to the normal subgroup generated by δ, denoted here by $\mathrm{Gr}(\delta)$, and δ lies in $\tilde{\mathcal{H}}$, we have that $\pi\colon \mathcal{F}_n \longrightarrow \mathcal{D}_{k,n}$ induces an epimorphism from $\mathcal{F}_n/\tilde{\mathcal{H}}$ onto $\mathcal{D}_{k,n}/\mathcal{H}$, and by definition of $\tilde{\mathcal{H}}$ it is obviously a monomorphism, hence it is an isomorphism of groups.

Furthermore, the induced map from $\tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}})$ onto $\mathcal{H}/\Phi(\mathcal{H})$, which is written $\pi_{\mathcal{H}}$, is G-equivariant, since the action on those modules is but the action by conjugation. Thus $\pi_{\mathcal{H}}$ is an epimorphism of modules from $\tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}})$, which is stably isomorphic to $\Omega^2(\mathbf{F}_p)$ according to Proposition 1.7.1, onto J^*.

Notation 2.1.1. Since we have fixed an extension $\mathbf{K}/\mathbf{k}$, we have fixed the subgroup $\mathcal{H}$ (and consequently $\tilde{\mathcal{H}}$). Therefore from now on, when we speak of *the* module $\omega_2(\mathbf{F}_p)$ we mean $\tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}})$ as an $\mathcal{F}_n/\tilde{\mathcal{H}}$-module, unless we explicitly say so.

In order to prove the short exact sequence, it remains to study the kernel of $\pi_{\mathcal{H}}$: it is done in the following lemma.

Lemma 2.1.2. *There exists a unique cyclic $\mathbf{F}_pG$-module of dimension $|G|-1$ (up to isomorphism). It is stably isomorphic to $\Omega^{-1}(\mathbf{F}_p)$, and in fact isomorphic to the following module given by generators and relations*

$$\langle \alpha | \alpha \cdot \mathrm{N} = 0 \rangle \,,$$

where N *denotes the norm*

$$\mathrm{N} := \sum_{g \in G} g \,.$$

Proof. Let us translate one by one the hypothesis of this lemma: suppose M is a module verifying the conditions of the lemma; since M is cyclic, there exists an epimorphism $\mathbf{F}_pG \longrightarrow M$. Because of the dimension of M, its kernel is of dimension 1, it is of course $\mathbf{F}_p$, both as a vector space and as a module. Therefore the following sequence is exact

$$0 \longrightarrow \mathbf{F}_p \longrightarrow \mathbf{F}_pG \longrightarrow M \longrightarrow 0 \ ,$$

which, by definition, means

$$M \simeq \Omega^{-1}(\mathbf{F}_p) \,.$$

Now, note that the monomorphisms from $\mathbf{F}_p$ into $\mathbf{F}_pG$, are just the $f_c \colon 1 \mapsto c\,\mathrm{N}$, where $c \in \mathbf{F}_p$ and N is the norm. Hence the lemma. □

This module, which is simply $I(G)^*$, will be denoted by $\omega_{-1}(\mathbf{F}_p)$ in the rest of the paper. Now, we would like to verify step by the step the lemma on $\ker \pi_{\mathcal{H}}$. Let us first address the first hypothesis of this latter.

Lemma 2.1.3. *The kernel of the map from $\tilde{\mathcal{H}}/\Phi(\tilde{\mathcal{H}})$ onto $\mathcal{H}/\Phi(\mathcal{H})$ is monogenous and it is generated by $[\delta]$, the class of δ modulo $\Phi(\tilde{\mathcal{H}})$.*

Proof. Consider the canonical projection $pr \colon \mathcal{H} \longrightarrow \mathcal{H}/\Phi(\mathcal{H})$ and set $\tilde{\pi} \colon \tilde{\mathcal{H}} \longrightarrow \mathcal{H}/\Phi(\mathcal{H})$ such that $\tilde{\pi} = pr \circ \pi$. We claim that $\ker \tilde{\pi}$ is the normal subgroup of $\mathcal{H}$ generated by δ and $\Phi(\mathcal{H})$.

Take $x \in \ker \tilde{\pi}$, then we have $\tilde{\pi}(x) \in \Phi(\mathcal{H})$. Now consider a lift $\overline{x}$ of this element in $\mathcal{H}$. If it is zero, since $\ker \pi = \mathrm{Gr}(\delta)$, then $x \in \mathrm{Gr}(\delta)$. If this is not the case, then $\overline{x}$ can be written as a product of h_i^p and (h_j, h_s) where $h_i, h_j, h_s \in \mathcal{H}$, hence x can be written as a product of elements of the form $\tilde{h}_i^p$, $(\tilde{h}_j, \tilde{h}_s)$ and δ, where $\tilde{h}_i, \tilde{h}_j, \tilde{h}_k$ are in $\tilde{\mathcal{H}}$. Hence we have proved the claim.

Note now that $\ker \pi_{\mathcal{H}} = \ker \tilde{\pi}/\Phi(\tilde{\mathcal{H}})$, therefore it is generated by $[\delta]$.

□

We then have to compute the dimension of J^*.

For every finitely generated pro-p-group $\mathcal{U}$, $d_1(\mathcal{U})$ denotes the minimal number of topological generators of $\mathcal{U}$, or equivalently the dimension of $H^1(\mathcal{U}, \mathbf{F}_p)$ or the one of $\mathcal{U}/\Phi(\mathcal{U})$ (see [Ser94, 4.2]).

According to [Koc02, Example 6.3] and to [Ser94, Exercice 6 p.41], the following formulae hold:

$$\begin{cases} d_1(\tilde{\mathcal{H}}) &= (\mathcal{F}_n : \tilde{\mathcal{H}})(n-1)+1 \\ d_1(\mathcal{H}) &= (\mathcal{D}_{k,n} : \mathcal{H})(n-2)+2 \end{cases} \tag{2.1}$$

Since we have that $(\mathcal{F}_n : \tilde{\mathcal{H}}) = |G| = (\mathcal{D}_{k,n} : \mathcal{H})$, the dimension of $\ker \pi_{\mathcal{H}}$ is exactly $|G|-1$, therefore we can use the lemma and conclude. Thus the following proposition holds:

Proposition 2.1.4. *The following sequence is exact:*

$$0 \longrightarrow \omega_{-1}(\mathbf{F}_p) \xrightarrow{\kappa} \omega_2(\mathbf{F}_p) \xrightarrow{\pi_{\mathcal{H}}} J^* \longrightarrow 0 \ . \tag{2.2}$$

Remark. It should be pointed out that, in the previous exact sequence, $\omega_2(\mathbf{F}_p)$ does not necessarily verify the minimality condition we have set in §1.6, whereas $\omega_{-1}(\mathbf{F}_p)$ always does so.

From now on, we fix κ to be the map in the previous short exact sequence: it will play a major role, before disappearing at the end of this chapter.

2.2 ...and its consequences

Now, we are in possession of the required tools to show the main theorems. We will have to distinguish between two cases, according as the morphism κ in the short exact sequence of Proposition 2.1.4 is stably zero or not.

2.2.1 When κ is stably zero

In $\underline{\mathfrak{mod}}(\mathbf{F}_pG)$ the triangle

$$\Omega^{-1}(\mathbf{F}_p) \xrightarrow{\kappa} \Omega^2(\mathbf{F}_p) \longrightarrow J^* \longrightarrow \Omega^{-2}(\mathbf{F}_p) \ ,$$

is distinguished according to [HJ10, 3.1.]

If κ is stably zero, then, according to [HJ10, 4.4.], in the stable category the following isomorphism stands

$$J^* \simeq \Omega^2(\mathbf{F}_p) \oplus \Omega^{-2}(\mathbf{F}_p) \, .$$

Thus J^* is of constant Jordan type and its stable Jordan type is $[1]^2$, without any condition on the group G. Furthermore, since $\kappa = 0$ stably, the beginning of the long exact sequence of cohomology is but

$$0 \longrightarrow H^0(G, \omega_{-1}(\mathbf{F}_p)) \longrightarrow H^0(G, \omega_2(\mathbf{F}_p)) \longrightarrow H^0(G, J^*(\mathbf{K})) \longrightarrow H^1(G, \omega_{-1}(\mathbf{F}_p)) \longrightarrow 0 \ ,$$

hence we get

$$\dim H^0(G, J(\mathbf{K})^*) = d_2(G) + (n - d_1(G)) \, ,$$

where $d_i(G) = \dim H^i(G, \mathbf{F}_p)$.

We have therefore shown a little more that we announced:

Proposition 2.2.1. *Remember* $\mathbf{K}/\mathbf{k}$ *is a finite Galois extension of a local field* $\mathbf{k}$ *such that* $\xi_p \in \mathbf{k}$. *If the map* κ *is stably zero, then* $J(\mathbf{K})$ *is isomorphic in the stable module category to*

$$J(\mathbf{K}) \simeq \Omega^2(\mathbf{F}_p) \oplus \Omega^{-2}(\mathbf{F}_p) \, .$$

Hence $J(\mathbf{K})$ *is of constant Jordan type* $[1]^2$ *and the cohomology groups of* G *with coefficients in* $J(\mathbf{K})$ *are in fact*

$$\begin{cases} \hat{H}^s(G, J(\mathbf{K})) & \simeq & \hat{H}^{s+2}(G, \mathbf{F}_p) \oplus \hat{H}^{s-2}(G, \mathbf{F}_p) \\ H^0(G, J(\mathbf{K})) & \simeq & \mathbf{F}_p^{d_2(G)+d_1(G)+(n-2d_1(G))} \end{cases}$$

So we have proved (2)(a) of Theorem 1.4.2, and a little more than the second statement of Theorem 1.4.3 under the current assumption on κ. Remark that we did not need to make further assumptions on G in order to prove this proposition: it is an improvement of both main theorems.

Let us discuss a bit more the structure of $J(\mathbf{K})$. We certainly know that in the category of (not stable) modules, we have

$$J(\mathbf{K}) \simeq \Omega^2(\mathbf{F}_p) \oplus \Omega^{-2}(\mathbf{F}_p) \oplus P\,,$$

where P is a projective module. Bear in mind that we write $\Omega^k(\mathbf{F}_p)$ for a module which is stably isomorphic to $\Omega^k(\mathbf{F}_p)$ and not containing any projective summand. It is possible to compute the number of copies of $\mathbf{F}_pG$ contained in P:

Proposition 2.2.2. *When κ is zero, the G-module $J(\mathbf{K})$ can be decomposed in the following way*

$$J(\mathbf{K}) \simeq \Omega^2(\mathbf{F}_p) \oplus \Omega^{-2}(\mathbf{F}_p) \oplus (\mathbf{F}_pG)^{n-2d_1(G)}\,.$$

Proof. As previously proved, we have a stable isomorphism

$$J(\mathbf{K}) \simeq \Omega^2(\mathbf{F}_p) \oplus \Omega^{-2}(\mathbf{F}_p)\,,$$

it is therefore sufficient to compute the number of copies of the free module in $J(\mathbf{K})$. Using lemma 1.7.2, we get that this number is equal to

$$\dim H^0(G, J(\mathbf{K})) - \dim \hat{H}^0(G, J(\mathbf{K})) = d_2(G) + n - d_1(G) - d_2(G) - d_1(G)\,,$$

because we have clearly set that

$$\begin{array}{rcccl} H^0(G, \Omega^2(\mathbf{F}_p)) & \simeq & \hat{H}^0(G, \Omega^2(\mathbf{F}_p)) & \simeq & \mathbf{F}_p^{d_1(G)} \\ H^0(G, \Omega^{-2}(\mathbf{F}_p)) & \simeq & \hat{H}^0(G, \Omega^{-2}(\mathbf{F}_p)) & \simeq & \mathbf{F}_p^{d_2(G)} \end{array}$$

Which concludes the proof. □

It should be remarked that this proposition gives us a necessary - but not sufficient - condition on G in order for κ to be zero: as it is quite convenient, we promote this small remark to a corollary.

Corollary 2.2.3. *If κ is stably zero, then $2d_1(G) \leq n$.*

For example, note that if $\mathbf{K}/\mathbf{k}$ is the *maximal* p-elementary abelian extension, then $d_1(G)$ is equal to n the minimal number of generators of $\mathcal{G}_{\mathbf{k}}(p) = \mathcal{D}_{k,n}$. According to the previous corollary, it is not possible for κ to be stably zero; hence $\mathbf{K}^\times/\mathbf{K}^{\times p}$ is never stably isomorphic to $\Omega^2(\mathbf{F}_p) \oplus \Omega^{-2}(\mathbf{F}_p)$, as will be clear from the study of the alternative case, to which we turn now.

2.2.2 When κ is stably non-zero

If κ does not vanish in the stable module category, we will proceed in two steps: first, we shall draw the consequences of the short exact sequence of Proposition 2.1.4 in cohomology, secondly we shall prove that $J(\mathbf{K})$ is of constant Jordan type. Let us suppose from now on that κ is not stably zero.

Proposition 2.2.4. *We have the following equality*

$$\dim H^0(G, J(\mathbf{K})) = d_2(G) + (n - d_1(G)) - 1\,.$$

Proof. Note that in the long exact sequence in cohomology, the map

$$H^1(G, \omega_{-1}(\mathbf{F}_p)) \longrightarrow H^1(G, \omega_2(\mathbf{F}_p))$$

is not zero. Indeed, remark that the following diagram is commutative

$$\begin{array}{ccc} H^1(G, \omega_{-1}(\mathbf{F}_p)) & \longrightarrow & H^1(G, \omega_2(\mathbf{F}_p)) \\ \| & & \| \\ \hat{H}^2(G, \mathbf{F}_p) & \xrightarrow{\smile[\kappa]} & \hat{H}^{-1}(G, \mathbf{F}_p) \end{array}$$

However, by Tate duality [Bro94, §VI.7], the pairing given by

$$\begin{array}{ccc} \hat{H}^i(G,\mathbf{F}_p)\otimes\hat{H}^{-i-1}(G,\mathbf{F}_p) & \longrightarrow & \hat{H}^{-1}(G,\mathbf{F}_p)\simeq\mathbf{F}_p \\ a\otimes b & \longmapsto & a\smile b \end{array}$$

is non-degenerate. Therefore the previous map is non-zero, and consequently it is an epimorphism, for $H^1(G,\omega_2(\mathbf{F}_p))\simeq\mathbf{F}_p$. Thus the beginning of the long exact sequence of cohomology is just but

$$0\longrightarrow H^0(G,\mathbf{F}_p)\longrightarrow H^0(G,\omega_2(\mathbf{F}_p))\longrightarrow H^0(G,\mathbf{F}_p)\longrightarrow H^2(G,\mathbf{F}_p)\longrightarrow\hat{H}^{-1}(G,\mathbf{F}_p)\longrightarrow 0$$

Hence we obtain the announced equality. □

Now, we have to make further assumptions in order to compute the cohomology groups.

From now on, in this chapter G is a p-group such that $H^\bullet(G,\mathbf{F}_p)$ is a Cohen-Macaulay ring: since this hypothesis is - as far as we know - quite uncommon among the literature in Galois theory, we shall sometimes recall this hypothesis in order to lay emphasis on it. Moreover, in this section, we only study $J(\mathbf{K})$ under the hypothesis that G is not cyclic; when G is cyclic of order p we refer to §2.3.

Lemma 2.2.5. *Let $s,j\in\mathbf{Z}$ such that $j-s>0$ and let $\gamma\colon\omega_s(\mathbf{F}_p)\longrightarrow\omega_j(\mathbf{F}_p)$ a map of modules, where $\omega_s(\mathbf{F}_p)$ and $\omega_j(\mathbf{F}_p)$ are* any *modules stably isomorphic to $\Omega^s(\mathbf{F}_p)$ and $\Omega^j(\mathbf{F}_p)$. Then consider the distinguished triangle in the stable module category*

$$\Omega^s(\mathbf{F}_p)\xrightarrow{\gamma}\Omega^j(\mathbf{F}_p)\longrightarrow C_\gamma\longrightarrow\Omega^{s-1}(\mathbf{F}_p)\ . \tag{2.3}$$

If G is not cyclic and such that $H^\bullet(G,\mathbf{F}_p)$ is a Cohen-Macaulay ring, then in the long exact sequence of cohomology the following maps

$$\hat{H}^l(G,\omega_s(\mathbf{F}_p))\longrightarrow\hat{H}^l(G,\omega_j(\mathbf{F}_p)),\quad l\geq j+1\quad or\quad l\leq s-1$$

are zero.

Proof. Three things shall be remembered. First, bear in mind that $\omega_l(\mathbf{F}_p)$ denotes *a* module which is stably isomorphic to *the* object $\Omega^l(\mathbf{F}_p)$ in the stable category.

Secondly, for every pair of integers n_1,n_2, there exists an isomorphism between $\hat{H}^{n_1}(G,\mathbf{F}_p)$ and $\underline{\hom}(\Omega^{n_1+n_2}(\mathbf{F}_p),\Omega^{n_2}(\mathbf{F}_p))$. If κ is an element of $\underline{\hom}(\Omega^{n_1+n_2}(\mathbf{F}_p),\Omega^{n_2}(\mathbf{F}_p))$, by $[\kappa]$ we mean the corresponding class of cohomology in $\hat{H}^{n_1}(G,\mathbf{F}_p)$.

Thirdly, if a,b are two cohomology classes respectively of degree n_1 and n_2 such that $a=[\alpha]$ and $b=[\beta]$ where $\alpha\colon\Omega^{n_1+n_2+n_3}(\mathbf{F}_p)\longrightarrow\Omega^{n_2+n_3}(\mathbf{F}_p)$ and $\beta\colon\Omega^{n_2+n_3}(\mathbf{F}_p)\longrightarrow\Omega^{n_3}(\mathbf{F}_p)$, then $a\smile b=[\alpha\circ\beta]$. ([CTVEZ03, §4.5])

Now, the short exact sequence (2.3) gives birth to a long exact sequence in the stable-module category ([HJ10, Prop. 4.2]), which is but the long exact sequence in cohomology. Let us take a closer look to it:

$$\ldots\longrightarrow\underline{\hom}(\mathbf{F}_p,\Omega^{s-l}(\mathbf{F}_p))\xrightarrow{m_\gamma}\underline{\hom}(\mathbf{F}_p,\Omega^{j-l}(\mathbf{F}_p))\longrightarrow\underline{\hom}(\mathbf{F}_p,\Omega^{-l}(C_\gamma))\longrightarrow$$

$$\longrightarrow\underline{\hom}(\mathbf{F}_p,\Omega^{s-1-l}(\mathbf{F}_p))\longrightarrow\underline{\hom}(\mathbf{F}_p,\Omega^{j-1-l}(\mathbf{F}_p))\longrightarrow\ldots$$

However the application defined by

$$\begin{array}{rccc} m_\gamma\colon & \underline{\hom}(\mathbf{F}_p,\Omega^{s-l}(\mathbf{F}_p)) & \longrightarrow & \underline{\hom}(\mathbf{F}_p,\Omega^{j-l}(\mathbf{F}_p)) \\ & f & \longmapsto & f\circ\gamma \end{array}$$

is simply the cup product by $[\gamma] \in \hat{H}^{s-j}(G, \mathbf{F}_p)$ from $\hat{H}^{l-s}(G, \mathbf{F}_p)$ to $\hat{H}^{l-j}(G, \mathbf{F}_p)$. Now, it is known [BC92, Thm. 3.1 and Lemma 2.1], under the assumption that $H^\bullet(G, \mathbf{F}_p)$ is a Cohen-Macaulay ring, that such cup products are zero, as soon as $l < s$ ([BC92, Thm. 3.1]) or $l > j$ ([BC92, Lemma 2.1]). Hence we get the proposition.

□

Remarks.

1. If $p = 2$, in order to apply [BC92, Thm. 3.1 and lemma 2.1], we have to assume that G is not a generalized quaternion group.
2. Note that we had to suppose that $H^\bullet(G, \mathbf{F}_p)$ was a Cohen-Macaulay ring in order to control the behaviour of the cup product by $[\kappa]$.

Corollary 2.2.6. *Let G be as in the lemma. If M is an $\mathbf{F}_pG$-module fitting in the following exact sequence*

$$0 \longrightarrow \omega_{-1}(\mathbf{F}_p) \longrightarrow \omega_2(\mathbf{F}_p) \longrightarrow M \longrightarrow 0 \ , \tag{2.4}$$

then the Tate cohomology groups with coefficients in M verify

$$\hat{H}^s(G, M) = \hat{H}^{s+2}(G, \mathbf{F}_p) \oplus \hat{H}^{s-2}(G, \mathbf{F}_p) \quad \forall s,\ s \geq 2,\ \textit{or}\ s \leq -3\,.$$

Proof. It is sufficient to take a look on the long exact sequence in cohomology and apply the previous lemma. □

Therefore, we have already proved another big part of our theorem: the computation of the cohomology groups of degree higher than 2 (and lower than -4) is done and conform to what was announced in case (2)(b) of Theorem 1.4.2. Let us now address the case of the first cohomology group.

Proposition 2.2.7. *The groups $H^1(G, J^*)$ and $H^3(G, \mathbf{F}_p)$ are isomorphic.*

Proof. Let us again look at the long exact sequence in cohomology. Remember that

$$H^1(G, \omega_{-1}(\mathbf{F}_p)) \longrightarrow H^1(G, \omega_2(\mathbf{F}_p))$$

is an epimorphism according to Tate duality, since we have supposed that κ is not stably zero ([Bro94, §VI.7]). Therefore we may write

$$0 \longrightarrow H^1(G, J(\mathbf{K})) \longrightarrow H^2(G, \omega_{-1}(\mathbf{F}_p)) \longrightarrow H^2(G, \omega_2(\mathbf{F}_p)) \longrightarrow \dots$$

and as stated in lemma 2.2.5 the arrow

$$H^2(G, \omega_{-1}(\mathbf{F}_p)) \longrightarrow H^2(G, \omega_2(\mathbf{F}_p))\,,$$

is zero, hence the long exact sequence in cohomology gives us

$$0 \longrightarrow H^1(G, J(\mathbf{K})) \longrightarrow H^2(G, \omega_{-1}(\mathbf{F}_p)) \longrightarrow 0$$

which concludes the proof.

□

Now the proof of Theorem 1.4.2 is finally complete, in all cases. It is time to address the proof of Theorem 1.4.3. Let us recall a proposition due to D. Benson [Ben16, Proposition 8.12.1]

Proposition 2.2.8. *Let β be a π-point and $G = E_r$, where $r \geq 2$. If $\zeta \in \hat{H}^{-l}(E_r, \mathbf{F}_p)$ with $l > 0$, then $\mathrm{res}_\beta(\zeta)$ is zero.*

Now, we can prove the promised theorem.

Theorem 2.2.9. *Let $\mathbf{K}/\mathbf{k}$ be an elementary abelian p-extension. If $\mathbf{K}/\mathbf{k}$ is not cyclic, then $J(\mathbf{K})^* = \mathbf{K}^\times/\mathbf{K}^{\times p}$ is a $Gal(\mathbf{K}/\mathbf{k})$-module of constant Jordan type. Furthermore, its stable Jordan type is $[1]^2$.*

Proof. We recall that if M is an E_1-module, $n_j(M)$ denotes the number of blocks of size j in the decomposition of M (see Notation 1.1.2), furthermore it is known that $\dim J(\mathbf{K}) = 2+|G|(n-2)$ (see (2.1)), where n is the minimal number of generators of $\mathcal{G}_\mathbf{k}(p) = \mathcal{D}_{k,n}$. Therefore our goal is to prove that $n_1(\beta^*(J^*)) = 2$ and $n_p(\beta^*(J^*)) = (n-2)\frac{|G|}{p}$ for every π-point β.

Now, remember that in the exact sequence

$$0 \longrightarrow \omega_{-1}(\mathbf{F}_p) \xrightarrow{\kappa} \omega_2(\mathbf{F}_p) \longrightarrow J^* \longrightarrow 0 \ ,$$

the map κ is in fact a cohomology class in $\hat{H}^{-3}(E_k, \mathbf{F}_p)$. We have previously remarked that in the long exact sequence of cohomology the maps

$$\hat{H}^l(G, \omega_{-1}(\mathbf{F}_p)) \longrightarrow \hat{H}^l(G, \omega_2(\mathbf{F}_p)) \quad \forall l \in \mathbf{Z}\,,$$

is the cup product by $[\kappa] \in \hat{H}^{-3}(E_k, \mathbf{F}_p)$.

So, let β be a π-point. Since $\mathrm{res}_\beta([i])$ is zero according to the previous proposition, numerous morphisms are zero in the long exact sequence in cohomology. To be more precise, it leads to the following short exact sequence for all $l \in \mathbf{Z}$:

$$0 \longrightarrow \hat{H}^l(E_1, \beta^*(\omega_2(\mathbf{F}_p))) \longrightarrow \hat{H}^l(E_1, \beta^*(J^*)) \longrightarrow \hat{H}^{l+1}(E_1, \beta^*(\omega_{-1}(\mathbf{F}_p))) \longrightarrow 0 \ .$$

Since a π-point induces a morphism of triangulated category, $\beta^*(\Omega(M)) = \Omega(\beta^*(M))$, so that the leftmost and rightmost groups in the previous short exact sequence are but $\mathbf{F}_p$. Hence we deduce this precious piece of information:

$$H^1(E_1, \beta^*(J^*)) = \hat{H}^1(E_1, \beta^*(J^*)) = \mathbf{F}_p^2\,.$$

Thus by Lemma 1.1.3, we know that for every π-point β, $\beta^*(J^*)$ has in its decomposition exactly two blocks whose size is not p. It remains to prove that their size is exactly 1. To this end, let us compute the dimension of $H^0(E_1, \beta^*(J^*))$.

Knowing the nullity of the map $H^2(E_1, \beta^*(\Omega^{-1}(\mathbf{F}_p))) \longrightarrow H^2(E_1, \Omega^2(\mathbf{F}_p))$, the long exact sequence in cohomology gives us the following exact sequence:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0(E_1, \beta^*(\omega_{-1}(\mathbf{F}_p))) & \longrightarrow & H^0(E_1, \beta^*(\omega_2(\mathbf{F}_p))) & \longrightarrow & H^0(E_1, \beta^*(J^*)) \\ & & & & & & \downarrow \\ & & & & 0 & \xleftarrow[a_1]{} & H^1(E_1, \beta^*(\omega_{-1}(\mathbf{F}_p))) \end{array}$$

Since we know both the dimension of $\omega_{-1}(\mathbf{F}_p)$ and $\omega_2(\mathbf{F}_p)$ and their stable constant Jordan type (resp. $[p-1]$ and $[1]$), we deduce

$$\begin{cases} \dim H^0(E_1, \beta^*(\omega_{-1}(\mathbf{F}_p)) & = & \frac{|G|}{p} \\ \dim H^0(E_1, \beta^*(\omega_2(\mathbf{F}_p)) & = & (n-1)\cdot\frac{|G|}{p} + 1 \\ \dim H^1(E_1, \beta^*(\omega_{-1}(\mathbf{F}_p)) & = & 1 \end{cases}$$

Injecting these piece of information in the previous exact sequence we obtain

$$\dim H^0(E_1, \beta^*(J^*)) = 1 + ((n-1)\frac{|G|}{p} + 1 - \frac{|G|}{p}) = 2 + (n-2)\frac{|G|}{p}\,,$$

hence we get the following equality:

$$n_p(\beta^*(J^*)) = (n-2)\frac{|G|}{p}\,.$$

As previously remarked, we know that in the decomposition there are two blocks whose size is not p. Let ℓ_1 and ℓ_2 be their size; of course, we have

$$\dim J^* = n_p(\beta^*(J^*)) \cdot p + \ell_1 + \ell_2\,.$$

Because we already know the dimension of J^* (see (2.1)), this leads to

$$2 = \ell_1 + \ell_2\,.$$

We deduce that $\ell_1 = \ell_2 = 1$, hence $n_1(\beta^*(J^*)) = 2$, as expected. □

This completes the proof of Theorem 1.4.3.

Remark. A peculiar case is worth noting: if the absolute Galois group has p-rank two, the module J^* is of dimension 2 according to the previous computation of the dimension, and since it is of constant Jordan type $[1]^2$, it is simply isomorphic as a module to $\mathbf{F}_p \times \mathbf{F}_p$!

Furthermore such case is not a pathological made-up one, indeed consider $\mathbf{k} = \mathbf{Q}_\ell(\xi_p)$, with $\ell \neq p$. In this case, according to [Gui18, Theorem 4.8], $\mathbf{k}^\times/\mathbf{k}^{\times p}$ is of dimension 2, hence $\mathcal{G}_\mathbf{k}(p)$ is generated by two elements.

2.2.3 On the vanishing condition

The condition regarding κ, as natural as it can be in this text, is not easy to check nor to express in few words, therefore we will try to find an equivalent condition and give criteria in order to distinguish between the two cases.

Proposition 2.2.10. *When $\mathbf{K}/\mathbf{k}$ is a finite non-cyclic p-Galois extension, such that $Gal(\mathbf{K}/\mathbf{k})$ is not a quaternion group neither a cyclic one and the ring $H^\bullet(Gal(\mathbf{K}/\mathbf{k}), \mathbf{F}_p)$ is Cohen-Macaulay, the map $\kappa\colon \omega_{-1}(\mathbf{F}_p) \longrightarrow \omega_2(\mathbf{F}_p)$ is stably zero if and only if the following inflation map*

$$\inf\colon H^2(Gal(\mathbf{K}/\mathbf{k}), \mathbf{F}_p) \longrightarrow H^2(\mathcal{G}_\mathbf{k}(p), \mathbf{F}_p)\,,$$

is also zero.

Proof. The spectral sequence associated to

$$1 \longrightarrow \mathcal{H} \longrightarrow \mathcal{G}_\mathbf{k}(p) \longrightarrow G \longrightarrow 1$$

yields the five ter exact sequence:

$$0 \longrightarrow H^1(G, \mathbf{F}_p) \longrightarrow H^1(\mathcal{G}_\mathbf{k}(p), \mathbf{F}_p) \longrightarrow H^1(\mathcal{H}, \mathbf{F}_p)^G \longrightarrow H^2(G, \mathbf{F}_p) \longrightarrow H^2(\mathcal{G}_\mathbf{k}(p), \mathbf{F}_p)\ .$$

Remember here that $\mathcal{G}_\mathbf{k}(p) = \mathcal{D}_{k,n}$, where the integers k and n are fixed, so we have that $H^1(\mathcal{G}_\mathbf{k}(p), \mathbf{F}_p) = \mathbf{F}_p^n$ and $H^1(\mathcal{H}, \mathbf{F}_p)^G \simeq H^0(G, J)$. Now, let us suppose that κ is stably 0, in this case $\dim H^0(G, J) = d_2(G) + d_1(G) + (n - 2d_1(G))$ (according to Proposition 2.2.1). Hence by injecting these piece of information, we have in fact that the inflation

$$\inf\colon H^2(G, \mathbf{F}_p) \longrightarrow H^2(\mathcal{G}_\mathbf{k}(p), \mathbf{F}_p)$$

is zero.

The converse is similar.

□

Remark. The previous condition echoes to the one introduced by J. Mináč, J. Swallow and A. Topaz in [MST14, Theorem 2].

2.3 When G is cyclic of order p

We suppose here that $p \neq 2$.

The techniques we used did not really cover an already well-known case: when $\mathbf{K}/\mathbf{k}$ is a cyclic extension. Although the structure of those modules was already described first by D. K. Faddeev ([Fad60]) and then by J. Mináč and J. Swallow ([MS03]), we will give a proof which uses our techniques. Indeed only few details shall be changed in the previous ones, in order to achieve this goal.

Note that if in the short exact sequence

$$0 \longrightarrow \omega_{-1}(\mathbf{F}_p) \xrightarrow{\kappa} \omega_2(\mathbf{F}_p) \longrightarrow J(\mathbf{K}) \longrightarrow 0$$

the map κ is stably zero, then $J(\mathbf{K})$ is stably isomorphic to $\Omega^2(\mathbf{F}_p) \oplus \Omega^{-2}(\mathbf{F}_p)$: since in Proposition 2.2.1, we only had to assume that G was a finite p-group. As remarked, the cohomological condition was first used in the second half of the proof of Proposition 2.2.5.

The only thing which remain unknown is the structure of $J(\mathbf{K})$, when κ is not stably zero. We address this issue in the following proposition.

Proposition 2.3.1. *Let $\mathbf{K}/\mathbf{k}$ be a cyclic extension of degree p. If the map κ is not stably zero, then $J(\mathbf{K})$ has stable Jordan type* $[2]$.

Proof. We shall mimic the previous proofs. We claim that in the long exact sequence in Tate cohomology associated to the short exact sequence

$$0 \longrightarrow \omega_{-1}(\mathbf{F}_p) \longrightarrow \omega_2(\mathbf{F}_p) \longrightarrow J(\mathbf{K}) \longrightarrow 0 \ ,$$

the morphisms

$$f_i \colon \hat{H}^i(C_p, \omega_{-1}(\mathbf{F}_p)) \longrightarrow \hat{H}^i(C_p, \omega_2(\mathbf{F}_p))$$

are isomorphisms. Indeed as pointed out earlier in the proof of 2.2.5, according to [CTVEZ03, §4.5.], those morphisms are but

$$\begin{array}{rccc} f_i \colon & \hat{H}^i(C_p, \omega_{-1}(\mathbf{F}_p)) \simeq \hat{H}^{i+1}(C_p, \mathbf{F}_p) & \longrightarrow & \hat{H}^i(C_p, \omega_2(\mathbf{F}_p)) \simeq \hat{H}^{i-2}(C_p, (\mathbf{F}_p) \\ & \alpha & \longmapsto & [\kappa] \smile \alpha \end{array} .$$

However, since the cohomology is periodic for a cyclic group, the cup-product by a non-zero class is an isomorphism ([Bro94, §VI.9]), hence the claim.

$$\ldots \longrightarrow \hat{H}^1(C_p, \omega_{-1}(\mathbf{F}_p)) \xrightarrow{f_1} \hat{H}^1(C_p, \omega_2(\mathbf{F}_p)) \longrightarrow \hat{H}^1(C_p, J(\mathbf{K})) \longrightarrow \hat{H}^2(C_p, \omega_{-1}(\mathbf{F}_p)) \xrightarrow{f_2} \longrightarrow \ldots \ ,$$

by using the definition of $\omega_{-1}(\mathbf{F}_p)$, $\omega_2(\mathbf{F}_p)$ and the claim above we get that

$$\hat{H}^1(C_p, J(\mathbf{K})) \simeq \hat{H}^3(C_p, \mathbf{F}_p) \simeq \mathbf{F}_p \, ,$$

Now, since for $i \geq 1$, we have that $H^i(C_p, M) \simeq \hat{H}^i(C_p, M)$, we may apply Lemma 1.1.3, as earlier. Thus $J(\mathbf{K})$ has exactly a block whose length is not p, but according to the computation of the dimensions made in (2.1), we have

$$\dim J(\mathbf{K}) = 2 + (n-1) \cdot p \, ,$$

where $n = \dim H^1(\mathcal{G}_{\mathbf{k}}(p), \mathbf{F}_p)$; therefore the block is of size 2.

□

This alternative raises again the question of the inflation.

Proposition 2.3.2. *Let $\mathbf{K}/\mathbf{k}$ be a cyclic Galois extension of degree p. Then $J(\mathbf{K})$ has stable Jordan type $[1]^2$ if and only if* $\inf \colon H^2(Gal(\mathbf{K}/\mathbf{k}), \mathbf{F}_p) \longrightarrow H^2(\mathcal{G}_{\mathbf{k}}(p), \mathbf{F}_p)$ *is zero. Conversely, the inflation is not zero if and only if $J(\mathbf{K})$ has stable Jordan type* $[2]$.

Proof. Fix $\mathbf{K}/\mathbf{k}$ a cyclic extension and set $\mathcal{H} = Gal(\mathbf{k}(p)/\mathbf{K})$. Remember that $\mathbf{k}(p)$ stands for a maximal pro-p-closure of $\mathbf{k}$. We have an obvious short exact sequence

$$1 \longrightarrow \mathcal{H} \longrightarrow \mathcal{D}_{k,n} \longrightarrow C_p \longrightarrow 1 \ .$$

The spectral sequence associated to this short exact sequence yields the five term exact sequence:

$$0 \longrightarrow H^1(C_p, \mathbf{F}_p) \longrightarrow H^1(\mathcal{D}_{k,n}, \mathbf{F}_p) \longrightarrow H^1(\mathcal{H}, \mathbf{F}_p)^{C_p} \longrightarrow H^2(C_p, \mathbf{F}_p) \xrightarrow{\inf} H^2(\mathcal{D}_{k,n}, \mathbf{F}_p) \ .$$

Again, the usual litany of isomorphisms, already seen in the proof of Lemma 1.3.4, leads to $H^1(\mathcal{H}, \mathbf{F}_p)^{C_p} = J(\mathbf{K})^{C_p}$. Therefore, we have the following equality

$$\dim H^1(\mathcal{H}, \mathbf{F}_p)^{C_p} = \sum_{i=1}^{p} n_i(J(\mathbf{K}))\,,$$

where $n_i(J(\mathbf{K}))$ is the number of blocks of size i in $J(\mathbf{K})$.

If κ is stably zero, then there exists 2 blocks of size 1 and $n-2$ blocks of size p, hence $\dim H^1(\mathcal{H}, \mathbf{F}_p)^{C_p} = n$. So, the five term exact sequence is

$$0 \longrightarrow \mathbf{F}_p \longrightarrow \mathbf{F}_p^n \longrightarrow \mathbf{F}_p^n \longrightarrow H^2(C_p, \mathbf{F}_p) \xrightarrow{\inf} H^2(\mathcal{D}_{k,n}, \mathbf{F}_p) \ .$$

A quick inspection shows that inf is zero.

However if κ is stably non-zero, then $\dim H^1(\mathcal{H}, \mathbf{F}_p)^{C_p} = n-1$, so that by looking at the exact sequence

$$0 \longrightarrow \mathbf{F}_p \longrightarrow \mathbf{F}_p^n \longrightarrow \mathbf{F}_p^{n-1} \longrightarrow H^2(C_p, \mathbf{F}_p) \xrightarrow{\inf} H^2(\mathcal{D}_{k,n}, \mathbf{F}_p) \ ,$$

we know that $\inf\colon H^2(C_p, \mathbf{F}_p) \longrightarrow H^2(\mathcal{D}_{k,n}, \mathbf{F}_p)$ is a monomorphism, however since $\dim H^2(C_p, \mathbf{F}_p) = \dim H^2(\mathcal{D}_{k,n}, \mathbf{F}_p)$, it is an isomorphism. □

Remark. It should be pointed out that if $J(\mathbf{K})$ has stable Jordan type $[2]$, it has Jordan type $[2][p]^{n-2}$, whereas if $J(\mathbf{K})$ has stable Jordan type $[1]^2$, it has Jordan type $[1]^2[p]^{n-2}$.

Chapter 3

The Heller shifts of the trivial module

In this chapter, p is an odd prime number, E_n is an elementary abelian p-group of rank n, and we write simply $\mathbf{F}_p$ for the trivial E_n-module. We start by giving a presentation by generators and relations of certain modules $\tilde{\Omega}^s(\mathbf{F}_p)$, for $s \in \mathbf{Z}$, which are stably isomorphic to $\Omega^s(\mathbf{F}_p)$ and verify the minimality condition introduced in §1.6. According to our conventions, described right before §1.7, we should have named them $\omega_s(\mathbf{F}_p)$, and subsequently $\Omega^s(\mathbf{F}_p)$: in order to avoid any confusion however, as long as we have not proved that they are stably isomorphic to $\Omega^s(\mathbf{F}_p)$ and that they verify the minimality condition, we call them $\tilde{\Omega}^s(\mathbf{F}_p)$, but as soon as it is done, we will forget the tilde. Then in the second part, we revisit $\Omega^2(\mathbf{F}_p)$ from a completely different viewpoint. Namely, we start from a free pro-p-group of rank n, denoted $\mathcal{F}_n$, and consider $M_n = \Phi(\mathcal{F}_n)/\Phi^{(2)}(\mathcal{F}_n)$ as a module over $E_n = \mathcal{F}_n/\Phi(\mathcal{F}_n)$, where we have set $\Phi^{(2)}(\mathcal{F}_n) = \Phi(\Phi(\mathcal{F}_n))$; working directly with commutators, we find a presentation for M_n which turns out to be precisely the presentation for $\Omega^2(\mathbf{F}_p)$ considered earlier. As a result, M_n is of course isomorphic to $\Omega^2(\mathbf{F}_p)$. Note that this is a particular case of Proposition 1.7.1.

Thus we do not make any mention of Galois theory in the next paragraphs. Yet, the material in this chapter paves the way for a closer study of $J(\mathbf{K})$.

3.1 The modules $\Omega^s(\mathbf{F}_p)$

We start with the case $n = 1$. It is well known that there is a projective resolution of $\mathbf{F}_p$ as an $\mathbf{F}_pE_1 = \mathbf{F}_pC_p$ module which is periodic, and indeed of the form

$$\cdots \longrightarrow \mathbf{F}_pE_1 \xrightarrow{x\mapsto x\cdot X_1} \mathbf{F}_pE_1 \xrightarrow{x\mapsto x\cdot X_1^{p-1}} \mathbf{F}_pE_1 \xrightarrow{x\mapsto x\cdot X_1} \mathbf{F}_pE_1 \longrightarrow \cdots$$

Let us be more precise. In degree $s \geq 0$ we take a copy P_s of the free module of rank 1, we take $P_{-1} = \mathbf{F}_p$, and define $D_s\colon P_s \longrightarrow P_{s-1}$ by $D_s(x) = x \cdot X_1$ if s is odd, and $D_s(x) = x \cdot X_1^{p-1}$ if s is even and positive, while D_0 is the augmentation.

By definition, we see that for $s \geq 1$, $\tilde{\Omega}^s(\mathbf{F}_p) := \ker(D_{s-1}) = \mathrm{Im}(D_s) \cong P_s/\ker(D_s)$ is a model for $\Omega^s(\mathbf{F}_p)$. So $\tilde{\Omega}^s(\mathbf{F}_p)$ is a submodule of P_{s-1}, but more importantly for us, it is a quotient of P_s. It is thus "presented" as having one generator (the generator for P_s), and one relation (the image of the generator of P_{s+1} under D_{s+1}, which generates all of $\mathrm{Im}(D_{s+1}) = \ker(D_s)$).

We need some notation. It may appear surprising at first, but will generalize well to other values of n. So we consider the graded commutative ring $P_* = \mathbf{F}_pE_1[\zeta, \eta]$, where the subring $\mathbf{F}_pE_1$ is concentrated in degree 0, the degrees of ζ and η are 2 and 1 respectively, and there are no relations apart from those imposed by graded-commutativity, that is $\eta^2 = 0$ and $\eta\zeta = \zeta\eta$. In other words, we have

$$P_* = H^*(E_1, \mathbf{F}_p) \otimes_{\mathbf{F}_p} \mathbf{F}_pE_1\,.$$

From topological practice, we have acquired the habit of writing either xy or $x \smile y$ for the product of two elements x and y of P_*.

The degree s summand in P_* is free of rank 1 over $\mathbf{F}_pE_1$, generated by ζ^k if $s = 2k$ and by $\eta\zeta^k$ if $s = 2k+1$. So we may take it as the module written P_s above, and thus we can consider the combined map

$$D\colon P_* \longrightarrow P_*$$

obtained from the various boundary maps D_s. We caution that D is not a derivation of the ring P, as can be verified with the formulae

$$D(\zeta^k) = \eta\zeta^{k-1} \cdot X_1^{p-1}\,, \tag{3.1}$$

and

$$D(\eta\zeta^k) = \zeta^k \cdot X_1\,. \tag{3.2}$$

The point of this is to come up with reasonable names for the generators of the modules $\tilde{\Omega}^s(\mathbf{F}_p)$. Thus to finish with the case $n = 1$, we see that $\tilde{\Omega}^{2k}(\mathbf{F}_p)$ is generated by ζ^k; as the module of relations $\ker(D_{2k})$ is also $\mathrm{Im}(D_{2k+1})$, it is generated by $D_{2k+1}(\eta\zeta^k) = \zeta^k \cdot X_1$. Using the isomorphism $\tilde{\Omega}^{2k}(\mathbf{F}_p) \cong P_{2k}/\ker(D_{2k})$ induced by D_{2k}, we conclude that we have the following presentation by generators and relations:

$$\tilde{\Omega}^{2k}(\mathbf{F}_p) \cong \langle \zeta^k \mid \zeta^k \cdot X_1 = 0 \rangle\,. \tag{3.3}$$

A similar reasoning leads to

$$\tilde{\Omega}^{2k+1}(\mathbf{F}_p) \cong \langle \eta\zeta^k \mid \eta\zeta^k \cdot X_1^{p-1} = 0 \rangle\,. \tag{3.4}$$

We can turn to an arbitrary value of n. Tensoring the resolution P_* previously given with itself n times (over $\mathbf{F}_p$), we obtain a resolution A_* of $\mathbf{F}_p$, by the Künneth theorem. Moreover, the usual formula for the differential in a tensor product of complexes shows, by an immediate induction on n, that we really have a resolution by $\mathbf{F}_pE_n$-modules.

We can identify $A_* = \bigoplus_s A_s$ with the graded ring $\mathbf{F}_pE_n[\zeta_1, \ldots, \zeta_n, \eta_1, \ldots, \eta_n]$. It is equipped with a self-map D, obtained from the differentials. The module $\tilde{\Omega}^s(\mathbf{F}_p) := A_s/D(A_{s+1})$ is stably isomorphic to $\Omega^s(\mathbf{F}_p)$, by definition. Moreover, the $\mathbf{F}_pE_n$-module A_s is free, its generators being the monomials in the ζ_i and η_j of the appropriate degree. Thus we have a presentation

$$A_{s+1} \xrightarrow{D_{s+1}} A_s \xrightarrow{D_s} \tilde{\Omega}^s(\mathbf{F}_p) \longrightarrow 0\,.$$

Hence $\tilde{\Omega}^s(\mathbf{F}_p)$ has a presentation, with generators indexed by the monomials in A_s, and relations indexed by the monomials in A_{s+1}. The technical point will be to compute the effect of the map D_{s+1}, and this is the object of the proposition below. We point out that, in the sequel, the ring A_* will be essentially forgotten, but what will survive is a system of names for the generators and relations of various modules.

Definition 3.1.1. A *multi-index* is a tuple $\nu = (\nu_1, \nu_2, \ldots)$ of nonnegative integers (in this paper, most multi-indices will be of length n, the rank of E_n). The *weight* of ν is then $|\nu| = \nu_1 + \nu_2 + \cdots$. We define a *$C$-index of weight s* to be a pair (h, z) of multi-indices of the same length verifying the following conditions:

1. $h_i \in \{0, 1\}$ for each i,
2. $2|z| + |h| = s$.

Further, if ν is a multi-index, we define $\mathrm{supp}(\nu) = \{i \mid \nu_i \neq 0\}$.

As elements of A do not commute, we have to specify the following notation

$$\eta^h \smile \zeta^z = \eta_1^{h_1} \ldots \eta_n^{h_n} \zeta_1^{z_1} \ldots \zeta_n^{z_n}\,.$$

We shall introduce some simple notation, classical in the free differential calculus of Fox (see [Fox53]). Taking into account the weight of each generator, a basis of A is given by the monomial

$\eta^h \smile \zeta^z$ where (h,z) is a C-index. Let m be such a monomial, we define the following linear map:

$$\begin{array}{rccl} \frac{\partial}{\partial\eta_i}: & A & \longrightarrow & A \\ & m' & \longmapsto & \frac{\partial m'}{\partial\eta_i} = \left\{ \begin{array}{ll} 0 & \text{if there is no } \eta_i \text{ in } m', \\ m & \text{if } m' = \eta_i m. \end{array} \right. \end{array}$$

Note those are well defined, since we have defined these $\mathbf{F}_p$-linear applications on an $\mathbf{F}_p$-basis of A. In the same fashion, we introduce the following operators for every $i \in \{1,\dots,n\}$,

$$\begin{array}{rccl} \zeta_i^{-1}: & A_{s+2} & \longrightarrow & A_s \\ & m & \longmapsto & \zeta_i^{-1}(m) = \left\{ \begin{array}{ll} m' & \text{if } m = \zeta_i m' \text{ for a monomial } m', \\ 0 & \text{otherwise.} \end{array} \right. \end{array}$$

It will be easier to write simply $\zeta_i^{-1}m$ or $m\zeta_i^{-1}$ for $\zeta_i^{-1}(m)$. It should be remarked that ζ_i^{-1} is *not* an isomorphism. Indeed we have for instance

$$\zeta_1^{-1}(\eta_1) = 0\,,$$

hence its kernel is not reduced to $\{0\}$: it may be identified to $\mathbf{F}[\eta_1,\dots,\eta_n,\zeta_1,\dots,\hat{\zeta}_i,\dots,\zeta_n]$, where $\hat{\zeta}_i$ means that we have omitted ζ_i. With this notation, the action of D for $n=1$ described above (see (3.1),(3.2)) can be recast as

$$D(\zeta_1^k) = \eta_1\zeta_1^k\zeta_1^{-1}\cdot X_1^{p-1} \quad (k\neq 0) \quad \text{and} \quad D(\eta_1\zeta_1^k) = \frac{\partial(\eta_1\zeta_1^k)}{\partial\eta_1}\cdot X_1\,,$$

and thus for any monomial $m \neq 1$ in η_1 and ζ_1 we may state :

$$D(m) = \frac{\partial(m)}{\partial\eta_1}\cdot X_1 + \eta_1 m\zeta_1^{-1}\cdot X_1^{p-1}\,.$$

The next proposition generalizes this to any value of n.

Theorem 3.1.2. *Let $s \geq 0$. The module $\tilde{\Omega}^s(\mathbf{F}_p)$, which is stably isomorphic to $\Omega^s(\mathbf{F}_p)$, has a presentation of the form*

$$\tilde{\Omega}^s(\mathbf{F}_p) \cong \langle \eta^h \smile \zeta^z \mid \mathrm{Rel}^{s+1}(h',z') \rangle$$

with generators $\eta^h \smile \zeta^z$ indexed by the C-indices (h,z) of weight s, and one relation $\mathrm{Rel}^{s+1}(h',z')$ for each C-index (h',z') of weight $s+1$, given by

$$\sum_{i=1}^{n}\left(\frac{\partial(\eta^{h'}\smile\zeta^{z'})}{\partial\eta_i}\cdot X_i + (\eta_i\eta^{h'}\smile\zeta^{z'}\zeta_i^{-1})\cdot X_i^{p-1}\right) = 0\,.$$

Moreover, for $s \geq 1$ there is an $\mathbf{F}_pE_n$-module $\tilde{\Omega}^{-s-1}(\mathbf{F}_p)$, which is stably isomorphic to $\Omega^{-s-1}(\mathbf{F}_p)$, and has a presentation of the form

$$\tilde{\Omega}^{-s-1}(\mathbf{F}_p) \cong \langle \eta^h \smile \zeta^z \mid \mathrm{Rel}_{s-1}(h',z') \rangle$$

with generators $\eta^h \smile \zeta^z$ indexed by the C-indices (h,z) of weight s, and one relation $\mathrm{Rel}_{s-1}(h',z')$ for each C-index (h',z') of weight $s-1$, given by

$$\sum_{i=1}^{n}\left((\eta^{h'}\smile\zeta^{z'}\eta_i)\cdot X_i + \zeta_i\frac{\partial(\eta^{h'}\smile\zeta^{z'})}{\partial\eta_i}\cdot X_i^{p-1}\right) = 0\,.$$

Finally, there is a module $\tilde{\Omega}^{-1}(\mathbf{F}_p)$, stably isomorphic to $\Omega^{-1}(\mathbf{F}_p)$, with presentation

$$\tilde{\Omega}^{-1}(\mathbf{F}_p) \cong \langle \alpha \mid \alpha\cdot\prod_{1\leq i\leq n} X_1^{p-1} = 0\rangle\,.$$

Proof. Assume $s \geq 1$ first. Let us find an expression of the differential D by induction on the rank n of the elementary abelian group. It is clear that the proposition holds for $n = 1$ according to the equations (3.3) and (3.4).

Let us assume that for every element of the form $c = \eta_1^{h_1} \dots \eta_{n-1}^{h_{n-1}} \zeta_1^{z_1} \dots \zeta_{n-1}^{z_{n-1}} = \eta^h \zeta^z$, where (h, z) is a C-index, we have

$$D(c) = \sum_{i=1}^{n-1} \left(\eta_i c \zeta_i^{-1} \cdot X_i^{p-1} + \frac{\partial c}{\partial \eta_i} \cdot X_i \right) . \tag{3.5}$$

We now establish that the same formula holds with $n-1$ replaced by n.

Continue with the element c, and let $(h_n, z_n) \in (\{0,1\} \times \mathbf{N}) - \{(0,0)\}$, by using the classical definition of the differential of the tensor product of two resolutions, and the fact that ζ_n is of degree 2 we get:

$$\begin{aligned} D(\eta^h \zeta^z \zeta_n^{z_n} \eta_n^{h_n}) &= D(c \eta_n^{h_n} \zeta_n^{z_n}) \\ &= D(c) \eta_n^{h_n} \zeta_n^{z_n} + (-1)^{\sum_{i=1}^{n-1} h_i} c D(\eta_n^{h_n} \zeta_n^{z_n}) \end{aligned}$$

Since $h_n \in \{0,1\}$, we shall distinguish two cases according to the possible values of h_n.

If $h_n = 0$, since ζ_n is of weight 2, and using first that $D(\zeta_n^{z_n}) = \eta_n \zeta_n^{z_n} \zeta_n^{-1} \cdot X_n^{p-1}$, second the equation (3.5), we obtain

$$D(\eta^h \eta_n^{h_n} \zeta^z \zeta_n^{z_n}) = D(c \zeta_n^{z_n}) = D(c) \zeta_n^{z_n} + (-1)^{\sum_{i=1}^{n-1} h_i} \eta^h \eta_n \zeta^z \zeta_n^{z_n} \zeta_n^{-1} \cdot X_n^{p-1} .$$

Again, since ζ_n commutes with all elements, the following relations implying the above operators are immediate, on every monomial m:

$$\left\{ \begin{array}{rcccc} \zeta_n \frac{\partial m}{\eta_i} & = & \frac{\partial(\zeta_n m)}{\partial \eta_i} & = & \frac{\partial(m \zeta_n)}{\partial \eta_i} \\ \zeta_n \zeta_j^{-1}(m) & = & \zeta_j^{-1}(\zeta_n m) & = & \zeta_j^{-1}(m \zeta_n) \end{array} \right.$$

where $i \in \{1, \dots, n\}$ and $j \neq n$. Now, let us reorder the term $(-1)^{\sum_{i=1}^{n-1} h_i} (\eta^h \eta_n \zeta^z \zeta_n^{z_n} \zeta_n^{-1}) \cdot X_n^{p-1}$:

$$\begin{aligned} (-1)^{\sum_{i=1}^{n-1} h_i} (\eta^h \eta_n \zeta^z \zeta_n^{z_n} \zeta_n^{-1}) \cdot X_n^{p-1} &= (-1)^{\sum_{i=1}^{n-1} h_i} (\eta_1^{h_1} \dots \eta_{n-1}^{h_{n-1}} \eta_n \zeta^z \zeta_n^{z_n} \zeta_n^{-1}) \cdot X_n^{p-1} \\ &= (-1)^{\sum_{i=1}^{n-1} h_i} (-1)^{h_{n-1}} (\eta_1^{h_1} \dots \eta_{n-2}^{h_{n-2}} \eta_n \eta_{n-1}^{h_{n-1}} \zeta^z \zeta_n^{z_n} \zeta_n^{-1}) \cdot X_n^{p-1} \quad (\eta_{n-1}\eta_n = -\eta_n \eta_{n-1}) \\ &= \dots \\ &= (-1)^{\sum_{i=1}^{n-1} h_i} (-1)^{\sum_{i=1}^{n-1} h_i} (\eta_n \eta^h \zeta^z \zeta_n^{z_n}) \cdot X_n^{p-1} \\ &= (\eta_n c \zeta_n^{z_n} \zeta_n^{-1}) \cdot X_n^{p-1} . \end{aligned}$$

Therefore we have the expected formula:

$$D(c \zeta_n^{z_n}) = \eta_n c \zeta_n^{z_n} \zeta_n^{-1} \cdot X_n^{p-1} + \sum_{i=1}^{n-1} \left(\frac{\partial c \zeta_n^{z_n}}{\partial \eta_i} \cdot X_i + \eta_i c \zeta_n^{z_n} \zeta_i^{-1} \cdot X_i^{p-1} \right) ,$$

which is what we expected according to (3.5).

If $h_n = 1$, some slight changes have to be made:

$$D(c \eta_n \zeta_n^{z_n}) = D(c) \eta_n \zeta_n^{z_n} c + (-1)^{\sum_{i=1}^{n-1} h_i} c \zeta_n^{z_n} \cdot X_n .$$

Furthermore, we have the following equalities:

$$\left\{\begin{array}{rcl} \frac{\partial m}{\partial \eta_i}\eta_n & = & \frac{\partial m\eta_n}{\partial \eta_i} \\ \eta_n\zeta_i^{-1}(m) & = & \zeta_i^{-1}(\eta_n m) \end{array}\right.$$

Again, if we set $(h', z') = ((h, 1), (z, z_n))$, then, on one hand, we clearly have:

$$\frac{\partial(\eta^{h'} \smile \zeta^{z'})}{\partial \eta_i} = \frac{\partial c}{\partial \eta_i}\eta_n\zeta_n^{z_n} \quad i \neq n\,,$$

so that $D(c)\zeta_n^{z_n}$ is equal to

$$\sum_{i=1}^{n-1} \frac{\partial(\eta^{h'} \smile \zeta^{z'})}{\partial \eta_i} \cdot X_i + \sum_{i=1}^{n-1}(\eta_i\eta^{h'} \smile \zeta^{z'}\zeta_i^{-1}) \cdot X_i^{p-1}\,.$$

Now, using the graded-commutativity, we obtain

$$\eta^{h'} \smile \zeta^{z'} = (-1)^{\sum_{i=1}^{n-1} h_i}\eta_n c\zeta_n^{z_n}\,.$$

Therefore, it is clear that

$$\frac{\partial(\eta^{h'} \smile \zeta^{z'})}{\partial \eta_n} = (-1)^{\sum_{i=1}^{n-1} h_i} c\zeta^{z_n}\,,$$

hence the expected formula.

Since $\tilde{\Omega}^s(\mathbf{F}_p)$ is just but the kernel of D_s, we can deduce the proposition.

Now, what happens vis-à-vis $\tilde{\Omega}^{-s-1}(\mathbf{F}_p)$ is quite similar to our argument: we can consider the dual resolution of the initial one. Using again the Künneth formula and doing the same computation, we can obtain an expression of the differential D; but rather than considering the kernel of the differential, we compute the cokernel.

We have not given yet a description of $\Omega^{-1}(\mathbf{F}_p)$ and $\Omega^0(\mathbf{F}_p)$. In fact we can extend our description to $\Omega^0(\mathbf{F}_p)$, because our formulae still make sense in this situation and they give

$$\Omega^0(\mathbf{F}_p) = \langle \zeta^0 \smile \eta^0 \mid (\zeta^0 \smile \eta^0) \cdot X_i = 0, \quad \forall i \in \{1, \ldots, n\}\rangle\,,$$

which is only but a pompous notation for $\mathbf{F}_p$.

Finally, it is a well-known fact that I^* is stably isomorphic to $\Omega^{-1}(\mathbf{F}_p)$, where I is the augmentation ideal in the group algebra $\mathbf{F}_pE_n$, and it is generated by one element, which should logically be denoted by $\zeta^0 \smile \eta^0$, but in order to emphasize its specificity we will call it α. Furthermore it verifies the only relation $\alpha \cdot \coprod_{1\leq i\leq n} X_1^{p-1} = 0$, and this concludes the proof. □

Examples 3.1.3. We shall give a precise description of two modules of those families: $\tilde{\Omega}^1(\mathbf{F}_p)$ and $\tilde{\Omega}^{-2}(\mathbf{F}_p)$. (The reader who wants a third example can have a glimpse at the last corollary to Lemma 3.2.11 at the very end of this chapter: its proof starts with a description of $\tilde{\Omega}^2(\mathbf{F}_p)$.)

The generators of $\tilde{\Omega}^1(\mathbf{F}_p)$ are simply the η_i for $i \in \{1, \ldots, n\}$, and the relations are in fact of two kinds. The first kind consists in the relations $\mathrm{Rel}^2(0, z_i = 1)$ (by $(0, z_i = 1)$ we mean in the obvious way the C-index $((0, ..., 1, ..., 0), (0, ..., 0))$ where the 1 is in i-th position), which are (for $i \in \{1, \ldots, n\}$)

$$\mathrm{Rel}^2(0, z_i = 1): \qquad \eta_i \cdot X_i^{p-1} = 0\,;$$

and then, using the same abbreviation, the second kind of relation is in fact (for $1 \leq i < j \leq n$)

$$\mathrm{Rel}^2(h_i = h_j = 1): \qquad \eta_j \cdot X_i - \eta_i \cdot X_j = 0\,.$$

It should be noticed that $\tilde{\Omega}^1(\mathbf{F}_p)$ is in fact I, the augmentation ideal: a clear isomorphism is in fact given by the map sending η_i to X_i.

What about $\tilde{\Omega}^{-2}(\mathbf{F}_p)$? The generators are elements of the form η_i and there is a unique relation denoted $\mathrm{Rel}_{-1}(0, 0)$ which is

$$\mathrm{Rel}_{-1}(0, 0): \qquad \eta_1 \cdot X_1 + \ldots + \eta_n \cdot X_n = 0\,.$$

Remarks. The following facts are noteworthy.

1. Remember that $d_s(E_n) = \dim_{\mathbf{F}_p} H^s(E_n, \mathbf{F}_p)$ (see Notation 1.4.1). Then $d_s(E_n)$ is also the number of generators in our presentation of $\tilde{\Omega}^s(\mathbf{F}_p)$. It follows that this system of generators is minimal, which can also be deduced from the fact that all the relations belong to the radical (of the free module covering $\tilde{\Omega}^s(\mathbf{F}_p)$); one has

$$\hat{H}^s(E_n, \mathbf{F}_p) \cong \tilde{\Omega}^s(\mathbf{F}_p)/\operatorname{Rad}(\tilde{\Omega}^s(\mathbf{F}_p)) \cong \hom_{\mathbf{F}_p E_n}(\tilde{\Omega}^s(\mathbf{F}_p), \mathbf{F}_p)\,.$$

   Therefore from now on, we will refer to them as $\Omega^s(\mathbf{F}_p)$ and conversely if we speak about *the* ("unstable") module $\Omega^s(\mathbf{F}_p)$, we mean $\tilde{\Omega}^s(\mathbf{F}_p)$.

2. The dimensions of the modules verify

$$\dim_{\mathbf{F}_p} \Omega^{s+1}(\mathbf{F}_p) = d_s(E_n)p^n - \dim_{\mathbf{F}_p} \Omega^s(\mathbf{F}_p)\,. \tag{3.6}$$

3. The description of $\Omega^{-1}(\mathbf{F}_p)$ is exactly similar to the one given in Lemma 2.1.2.

3.2 The module M_n

We shall rediscover the module $\Omega^2(\mathbf{F}_p)$ in a completely different way. In this section p is an odd prime.

3.2.1 Notation & conventions.

If $\mathcal{G}$ is a finitely generated pro-p-group, $\Phi(\mathcal{G})$ denotes its Frattini subgroup, which means, according to Proposition 1.2.3, that $\Phi(\mathcal{G}) = \mathcal{G}^p(\mathcal{G}, \mathcal{G})$. By $(\mathcal{G}, \mathcal{G})$ we mean of course the derived subgroup which is generated by the commutators

$$(g_1, g_2) = g_1^{-1} g_2^{-1} g_1 g_2\,, \forall g_1, g_2 \in G\,. \tag{3.7}$$

Whenever $\mathcal{H} \lhd \mathcal{G}$, the group $\mathcal{G}$ acts by conjugation on $\mathcal{H}$, and we write

$$h^g = g^{-1} h g, \quad \forall h \in \mathcal{H}, \forall g \in \mathcal{G}\,.$$

Thus $\mathcal{G}$ acts on $M_{\mathcal{G}} = \Phi(\mathcal{G})/\Phi^{(2)}(\mathcal{G})$ by conjugation, and since the action of $\Phi(\mathcal{G})$ is trivial modulo $\Phi^{(2)}(\mathcal{G}) = \Phi(\Phi(\mathcal{G}))$, we will study the action of $\mathcal{G}/\Phi(\mathcal{G}) \cong E_r$ for some r. As $M_{\mathcal{G}}$ is an $\mathbf{F}_p$ vector space, it is, all in all, an $\mathbf{F}_p E_r$-right module, with the elementary abelian group E_r identified as above.

On $M_{\mathcal{G}}$ we shall use an additive notation, i.e. we write

$$[\alpha\beta] = [\alpha] + [\beta]\,, \forall \alpha, \beta \in \Phi(G)\,,$$

where $[\alpha]$ denotes the class of α modulo $\Phi^{(2)}(\mathcal{G})$. However, usually the additive notation makes it unnecessary to use brackets, and we may simply write $\alpha + \beta$ for $\alpha, \beta \in \Phi(\mathcal{G})$.

As for the action, our convention is to write $[\alpha] \cdot x$ for $[\alpha^x]$ (where $\alpha \in \Phi(\mathcal{G})$ and $x \in \mathcal{G}$), and more generally we write $[\alpha] \cdot \lambda$ where $\lambda \in \mathbf{F}_p E_r$. Moreover, we extend the convention we introduced in §1.1: if we have used a letter, say x, to denote an element of G, then we shall usually use the same letter x for its image in $\mathcal{G}/\Phi(\mathcal{G})$ and the capitalized letter X for $x - 1 \in \mathbf{F}_p[\mathcal{G}/\Phi(\mathcal{G})]$.

Here is an example of computation with all our conventions at work :

$$\alpha \cdot X = \alpha^x - \alpha = x^{-1}\alpha x \alpha^{-1} = (x, \alpha^{-1})\,,$$

for $\alpha \in \Phi(\mathcal{G})$ and $x \in \mathcal{G}$.

This applies in particular to $\mathcal{G} = \mathcal{F}_n$, the free pro-$p$-group on n generators. In this case we write $M_n := \Phi(\mathcal{F}_n)/\Phi^{(2)}(\mathcal{F}_n)$. We shall give a presentation by generators and relations of M_n as an $\mathbf{F}_p E_n$-module, where $E_n = \mathcal{F}_n/\Phi(\mathcal{F}_n)$, and then remark that it coincides with the presentation previously given of $\Omega^2(\mathbf{F}_p)$.

3.2.2 Some classical relations

Let $\mathcal{G}$ be a finitely generated pro-p-group. Let us recall some classical formulae about commutators, translated into relations about $\Phi(\mathcal{G})/\Phi^{(2)}(\mathcal{G})$ as a module with an action of $\mathcal{G}$. When we specialize to $\mathcal{G} = \mathcal{F}_n$ below, we shall see that we have in fact described *all* the relations, in the sense that we have a presentation.

Lemma 3.2.1. *Let x, y, z be three elements of $\mathcal{G}$, then the following relation holds in $\Phi(\mathcal{G})/\Phi^{(2)}(\mathcal{G})$:*

$$(y,x)\cdot Z + (x,z)\cdot Y + (z,y)\cdot X = 0\,, \tag{3.8}$$

where $X = x - 1$ (similarly for y and z). Furthermore we have:

$$y^p \cdot X = (x,y)\cdot Y^{p-1}\,. \tag{3.9}$$

Proof. We recall the Hall-Witt formula (cf. [DDSMS99] or [Laz54]). Let x, y, z be three elements of a pro-p-group G, then

$$((x,y^{-1}),z)^y((y,z^{-1}),x)^z((z,x^{-1}),y)^x = 1\,.$$

Indeed it is clear that

$$\begin{aligned}(x,y^{-1})^y &= y^{-1}x^{-1}yxy^{-1}y\\ &= y^{-1}x^{-1}yx = (y,x)\,.\end{aligned}$$

We can deduce the following well-known relation, similar to the Jacobi relation in the realm of Lie algebras:

$$(y,x)\cdot Z + (x,z)\cdot Y + (z,y)\cdot X = 0 \pmod{\Phi^2(\mathcal{G})}\,.$$

Indeed using the Hall-Witt relation and the previous remark, we have:

$$\begin{aligned}1 &\equiv ((x,y^{-1}),z)^y((y,z^{-1}),x)^z((z,x^{-1}),y)^x && \pmod{\Phi^{(2)}(\mathcal{G})}\\ &\equiv ((x,y^{-1})^{-1}(x,y^{-1})^z)^y((y,z^{-1})^{-1}(y,z^{-1})^x)^z((z,x^{-1})^{-1}(z,x^{-1})^y)^x && \pmod{\Phi^{(2)}(\mathcal{G})}\\ &\equiv ((y,x)^{-1}(y,x)^z)((z,y)^{-1}(z,y)^x)((x,z)^{-1}(x,z)^y) && \pmod{\Phi^{(2)}(\mathcal{G})}\,.\end{aligned}$$

The following equalities, which could be found in [DDSMS99], will be useful:

$$\begin{cases}(x,yz) &= (x,z)(x,y)^z\\ (xy,z) &= (x,z)^y(y,z)\\ (y^n,x) &= (x,y)^{y^{n-1}}(x,y)^{y^{n-2}}\dots(x,y)\,,\end{cases} \tag{3.10}$$

hence

$$(y^k,x) = \sum_{i=0}^{k-1}(x,y)\cdot y^i = (x,y)\cdot\sum_{i=0}^{k-1}y^i \pmod{\Phi^2(\mathcal{G})}\,.$$

Since in $\mathbf{F}_p[T]$ the following polynomial identity holds

$$\sum_{i=0}^{p-1}T^i = (T-1)^{p-1}\,,$$

we get for $k = p$ the following formula:

$$(y^p,x) = (x,y)\cdot Y^{p-1}\,.$$

Given that

$$y^p\cdot X = (y^p)^x - y^p = x^{-1}y^px - y^p = y^{-p}x^{-1}y^px = (y^p,x)\,,$$

we obtain the expected relation:

$$y^p\cdot X = (x,y)\cdot Y^{p-1}\,.$$

□

3.2.3 The free group

Now we specialize to $\mathcal{G} = \mathcal{F}_n$, the free pro-$p$ group on n generators, which will be called $\chi_1, \ldots, \chi_n$. The images of these in $E_n = \mathcal{F}_n/\Phi(\mathcal{F}_n)$ will be called $x_1, \ldots, x_n$. We write $X_i = x_i - 1 \in \mathbf{F}_p E_n$.

According to the previous relations (3.10), the 2-commutators (i.e. the (χ_i, χ_j)) and the χ_i^p form a generating system for M_n as $\mathbf{F}_p E_n$-module. The first thing we note is that

$$(\chi_i, \chi_j) = -(\chi_j, \chi_i)\,. \tag{3.11}$$

Simply because χ_i commutes with χ_i^p, we certainly have

$$\chi_i^p \cdot X_i = 0\,. \tag{3.12}$$

Next, from the relation (3.9) of the lemma, we have

$$\chi_j^p \cdot X_i = (\chi_i, \chi_j) \cdot X_j^{p-1}\,. \tag{3.13}$$

And finally, from (3.8), we obtain :

$$(\chi_k, \chi_j) \cdot X_i + (\chi_j, \chi_i) \cdot X_k + (\chi_i, \chi_k) \cdot X_j = 0\,. \tag{3.14}$$

Ultimately, we shall prove that the four types of relations just given between the generators provide a presentation for M_n, ie they generate the module of relations.

The strategy is as follows. First we note that it is enough to include the 2-commutators with $i < j$, of course, so we have $\binom{n}{2}$ commutators and n elements of the form χ_i^p.

Notation 3.2.2. Let $F_{n,p}$ be the free $\mathbf{F}_p E_n$-module on elements called $e_1, \ldots, e_n$ and $e_{i,j}$ for $i < j$.

There is a short exact sequence

$$0 \longrightarrow K \longrightarrow F_{n,p} \xrightarrow{\psi} M_n \longrightarrow 0\,,$$

where

$$\psi(e_i) = \chi_i^p\,, \quad \psi(e_{i,j}) = (\chi_i, \chi_j)\,. \tag{3.15}$$

We want to show that $K = \ker(\psi)$ is generated by the elements above. For this, we shall determine the dimension of M_n (which is easy), so that we will know the dimension of K over $\mathbf{F}_p$. The work will consist in exhibiting carefully selected elements of K, all obtained from the above using the $\mathbf{F}_p E_n$ action, which are linearly independent over $\mathbf{F}_p$ and numerous enough for us to conclude that they span K.

3.2.4 A basis for K

The dimension of M_n is well-known: we have already given it in (2.1), but now we make a lemma of this fact:

Lemma 3.2.3. *With our notation:*

$$\dim_{\mathbf{F}_p} M_n = 1 + (n-1) \cdot p^n\,.$$

Proof. According to [Koc02, Example 6.3], we have that the minimal number of topological generators of $\Phi(\mathcal{F}_n)$ - denoted $d(\Phi(\mathcal{F}_n))$ - is equal to $p^n(n-1)+1$, therefore we can conclude by definition of the Frattini subgroup. □

When $\nu = (\nu_1, \ldots, \nu_n)$ is a multi-index, we set

$$X^\nu = X_1^{\nu_1} X_2^{\nu_2} \ldots X_n^{\nu_n}\,.$$

Note that the family $(X^\nu)_{\nu \in \mathcal{I}}$, where $\mathcal{I} = \{0, \ldots, p-1\}^n$ is an $\mathbf{F}_p$ basis of the group algebra $\mathbf{F}_p E_n$. We will write $\mathcal{E}$ for this basis. Now we proceed to introduce distinguished elements of K.

- *The relations $R(i,m)$ and $R(i,j,m)$.*

Notation 3.2.4. For each $1 \leq i \leq n$ and $m \in \{0,\dots,p-1\}^n - \{(0,\dots,0)\}$, we introduce

$$R(i,m) = \begin{cases} e_i \cdot X_i^{m_i} \prod\limits_{s\neq i} X_s^{m_s}, & \text{if } m_i \neq 0\,, \\ e_i \cdot X_j^{m_j} \prod\limits_{\substack{s\neq i \\ s<j}} X_s^{m_s} + e_{(i,j)} \cdot X_i^{p-1} X_j^{m_j-1} \prod\limits_{s\neq i,j} X_s^{m_s}, & \text{if } i < j = \max(\mathrm{supp}(m))\,, \\ e_i \cdot X_j^{m_j} \prod\limits_{\substack{s\neq i \\ s<j}} X_s^{m_s} - e_{(j,i)} \cdot X_i^{p-1} X_j^{m_j-1} \prod\limits_{s\neq i,j} X_s^{m_s}, & \text{if } i > j = \max(\mathrm{supp}(m))\,, \end{cases} \tag{3.16}$$

In the second and in the third case, we also assumed $m_i = 0$.

Lemma 3.2.5. *The elements $R(i,m)$, where $1 \leq i \leq n$ and $m =\in \{0,\dots,p-1\}^n - \{(0,\dots,0)\}$, are in $\ker\psi$ and their number is*

$$n \cdot (p^n - 1)\,. \tag{3.17}$$

Proof. Let us prove that $R(i,m)$ is in the kernel of ψ for $i \in \{1,\dots,n\}$ and $m \in \{0,\dots,p-1\}^n - \{(0,\dots,0)\}$. First suppose $m_i \neq 0$, then $R(i,m) = e_i \cdot X_i^{m_i} \prod\limits_{s\neq i} X_s^{m_s}$ according to (3.16). Let us apply then ψ to it. We get

$$\begin{aligned} \psi(R(i,m)) &= \chi_i^p \cdot X_i^{m_i} \prod_{s\neq i} X_s^{m_s} \quad \text{(because of (3.15))} \\ &= 0 \cdot X_i^{m_i-1} \prod_{s\neq i} X_s^{m_s} \quad \text{(because of (3.12))} \\ &= 0\,. \end{aligned}$$

Second assume that $i < \max(\mathrm{supp}(m))$. In this case, the computation is as follow

$$\begin{aligned} \psi(R(i,m)) &= \chi_i^p \cdot X_j^{m_j} \prod_{\substack{s\neq i \\ s<j}} X_s^{m_s} + (\chi_i,\chi_j) \cdot X_i^{p-1} X_j^{m_j-1} \prod_{s\neq i,j} X_s^{m_s} \quad \text{(because of (3.15))} \\ &= (\chi_i^p \cdot X_j^{m_j} + (\chi_i,\chi_j) \cdot X_i^{p-1} X_j^{m_j-1}) \prod_{\substack{s\neq i \\ s<j}} X_s^{m_s} \\ &= 0 \cdot \prod_{\substack{s\neq i \\ s<j}} X_s^{m_s} \quad \text{(because of (3.13))} \\ &= 0\,. \end{aligned}$$

Third assume that $i > \max(\mathrm{supp}(m))$. We shall proceed in this way

$$\begin{aligned} \psi(R(i,m)) &= \chi_i^p \cdot X_j^{m_j} \prod_{\substack{s\neq i \\ s<j}} X_s^{m_s} - (\chi_j,\chi_i) \cdot X_i^{p-1} X_j^{m_j-1} \prod_{s\neq i,j} X_s^{m_s} \quad \text{(because of (3.15))} \\ &= (\chi_i^p \cdot X_j^{m_j} - (\chi_j,\chi_i) \cdot X_i^{p-1} X_j^{m_j-1}) \prod_{s\neq i,j} X_s^{m_s} \\ &= 0 \prod_{s\neq i,j} X_s^{m_s} \quad \text{(because of (3.13))} \\ &= 0 \end{aligned}$$

Hence by virtue of (3.9), we have deduced that $R(i,m)$ is in the kernel of ψ. We have therefore found exactly

$$n \cdot (p^n - 1)$$

vectors in the kernel of ψ so far.

□

By virtue of the same relation, we obtain that

$$-(\chi_i,\chi_j) \cdot X_i^{p-1} X_j^{p-1} = \chi_i^p \cdot X_j^p = 0\,. \tag{3.18}$$

Thus, the following lemma is obvious:

Lemma 3.2.6. *Vectors of the form*

$$R(i,j,m) = e_{(i,j)} \cdot X_j^{p-1} X_i^{p-1} \prod_{k<i} X_k^{m_k}$$

where

$$\max \operatorname{supp}(m) < i\,, \quad 1 \leq i < j \leq n \tag{3.19}$$

are in the kernel of ψ, for a total amount of

$$\sum_{i=1}^{n} (n-i) \cdot p^{i-1} \tag{3.20}$$

vectors of this form.

Proof. Let us apply ψ to $R(i,j,m)$.

$$\begin{aligned}
\psi(R(i,j,m)) &= \psi(e_{(i,j)} \cdot X_j^{p-1} X_i^{p-1} \prod_{k<i} X_k^{m_k}) \\
&= (\chi_i, \chi_j) \cdot X_j^{p-1} X_i^{p-1} \prod_{k<i} X_k^{m_k} \quad \text{(because of (3.15))} \\
&= 0 \cdot \prod_{k<i} X_k^{m_k} \quad \text{(because of (3.18))} \\
&= 0
\end{aligned}$$

Hence, $R(i,j,m)$ is in $\ker \psi$. Furthermore if we fix i, we have p^{i-1} choices for m, since $\max(\operatorname{supp}(m)) < i$, and $n-i$ choices for j, because this latter is strictly greater than i, so that we have the announced amount of vectors.

□

- *Relations of Jacobi type.*

Let χ_i, χ_j, χ_k be three elements of our generating system of $\mathcal{F}_n$ with $i \leq j \leq k$. Because of (3.8) and the elementary properties on the commutators, we get:

$$(\chi_i, \chi_j) \cdot X_k = (\chi_i, \chi_k) \cdot X_j - (\chi_j, \chi_k) \cdot X_i\,. \tag{3.21}$$

Thus elements of the form $e_{(i,j)} \cdot X_k - e_{(i,k)} \cdot X_j + e_{(j,k)} \cdot X_i$, where $1 \leq i < j < k \leq n$, lie in the kernel of ψ. More generally, by multiplying the previous relation by X^m, where m is such that

$$k = \max(\operatorname{supp}(m))\,, \quad m_k \neq p-1\,, \tag{3.22}$$

we deduce that vectors of the following form lie also in the kernel of ψ:

$$e_{(i,j)} \cdot X_k^{m_k+1} \prod_{s<k} X_s^{m_s} + e_{(j,k)} \cdot X_i^{m_i+1} \prod_{\substack{s\neq i \\ s\leq k}} X_s^{m_s} - e_{(i,k)} \cdot X_j^{m_j+1} \prod_{\substack{s\neq j \\ s\leq k}} X_s^{m_s}\,. \tag{3.23}$$

Notation 3.2.7. Such vectors are denoted $jac_1(i,j,k,m)$, for $1 \leq i < j < k \leq n$ and $k = \max(\operatorname{supp}(m))$.

Lemma 3.2.8. *The number of vectors $jac_1(i,j,k,m)$ is*

$$(p-1) \cdot \sum_{k=0}^{n} \binom{k-1}{2} \cdot p^{k-1}\,.$$

Proof. Indeed if we fix the integer k, then there is $(p-1) \cdot p^{k-1}$ possible choices for m, because $m_k \neq p-1$ and $k = \max(\operatorname{supp}(m))$. Furthermore, there is $\binom{k-1}{2}$ choices for $\{i,j\}$, since we have supposed $1 \leq i < j < k$. □

By multiplying (3.21) by X_k^{p-1}, we obtain the relation

$$(\chi_i, \chi_k) \cdot X_k^{p-1} X_j = (\chi_j, \chi_k) \cdot X_k^{p-1} X_i \tag{3.24}$$

Therefore, by multiplying by X^m where m is such that

$$m_j \neq p-1\,, \quad j = \max(\mathrm{supp}(m)), \tag{3.25}$$

we get again vectors of the form

$$e_{(i,k)} \cdot X_k^{p-1} X_j^{m_j+1} \prod_{s<j} X_s^{m_s} - e_{(j,k)} \cdot X_k^{p-1} X_i^{m_i+1} \prod_{\substack{s<j \\ s\neq i}} X_s^{m_s} \quad \text{where } i<j<k\,,$$

which are in the kernel of ψ: they are denoted by $jac_2(i,j,k,m)$.

Lemma 3.2.9. *We claim that we have added in the kernel of ψ a total amount of*

$$(p-1) \cdot \sum_{j=1}^{n} (j-1)(n-j) p^{j-1}$$

vectors of this form

Proof. Fix j. Since we have required that $k > j$, we have $n-j$ possible choices for k. Furthermore the condition on i implies that there is $(j-1)$ possible choices for i. Now, consider m, note that the condition on m implies that $m_j \neq 0$, hence there is $p-1$ choices for it. Moreover we have required that $j = \max(\mathrm{supp}(m))$, thus we have $(p-1)p^{j-1}$ choices for m. □

Notation 3.2.10. From now on, we set

$$F = \{R(i_1, m), R(i_2, j_2, m'), jac_1(i_3, j_3, k_3, m''), jac_2(i_4, j_4, k_4, m''')\}\,,$$

with the conditions on $i_s, j_s, k_s, m, m', m'', m'''$ given in (3.16), (3.19), (3.22) and (3.25).

Lemma 3.2.11. *The system F is a basis of* $\ker \psi$.

Proof. All vectors contained in F are in $\ker \psi$ by definition; we shall prove that they are linearly independent and that their number is equal to $\dim F_{n,p} - \dim M_n$.

Linear independence. Bear in mind that $\mathcal{E}$ is the basis of $F_{n,p}$ consisting of the $e_i \cdot X^\nu$ and the $e_{(i,j)} \cdot X^\mu$ where ν and μ are elements of $\{0, \ldots, p-1\}^n$. Let us define an $\mathbf{F}_p$-linear map $f\colon F_{n,p} \to F_{n,p}$ given on the vectors of $\mathcal{E}$ by

$$\begin{cases} f(e_i \cdot X^m) &= R(i,m)\,, & \text{if } m \neq (0,\ldots,0) \\ f(e_{(i,j)} \cdot X^m) &= jac_1(i,j,k,m)\,, & \text{if } 1 \leq i < j < k = \max(\mathrm{supp}(m)) \leq n \\ f(e_{(i,k)} \cdot X^m) &= jac_2(i,j,k,m)\,, & \text{if } 1 \leq i < j < k = \max \mathrm{supp}(m) \leq n\,, \\ & & \text{and } m_k = p-1,\ m_j \neq 0,\ m_i \neq p-1 \\ f(v) &= v & \text{otherwise} \end{cases} \tag{3.26}$$

Note that among the fixed vectors of $\mathcal{E}$ are the $R(i,j,m)$'s for instance, or e_i's. In order to number the vectors of the basis, we will use an order relation rather than cumbersome formulae from combinatorics.

We define a total order relation on the vectors of $\mathcal{E}$ by imposing the following conditions:

1. $e_i \cdot \prod_{s=1}^{n} X_s^{\nu_s} \leq e_j \cdot \prod_{s=1}^{n} X_s^{\mu_s}$ if and only if $i < j$ or $i = j$ and either $|\nu| < |\mu|$ or if $|\nu| = |\mu|$ then we use the lexicographic order.

2. $e_{(i,j)} \cdot \prod_{s=1}^{n} X_s^{\nu_s} \leq e_{(k,l)} \cdot \prod_{s=1}^{n} X_s^{\mu_s}$ if and only if one of the following condition is true

   (a) $i < k$

(b) if $i = k$ then one of the following must be true:

i. $j < l$,

ii. $|\nu| < |\mu|$,

iii. $\nu \preceq \mu$ where $\preceq$ is the lexicographic order

3. $e_i \cdot \prod_{s=1}^{n} X_s^{\nu_s} \leq e_{(j,k)} \cdot \prod_{s=1}^{n} X_s^{\mu_s}$.

The matrix associated to f in the basis $\mathcal{E}$, thus ordered, is lower triangular with 1's on the diagonal, as is readily checked (when defining the elements of F, we have always given the formulae so that the leftmost term is the lowest for the order relation).

So f is invertible, and the image of the canonical basis under f is another basis for $F_{n,p}$. This proves in particular that the elements of F are linearly independent.

Cardinality. By using the formula previously given, we can get: $\dim_{\mathbf{F}_p} \ker \psi = \binom{n}{2} p^n - 1$.

However

$$(p-1) \cdot \sum_{k=0}^{n-1} \binom{k}{2} p^k = \binom{n-1}{2} p^n - \sum_{k=1}^{n-1} (k-1) \cdot p^k \,, \tag{3.27}$$

in the same fashion

$$(p-1) \cdot \sum_{j=1}^{n} (n-j)(j-1) p^{j-1} = \sum_{j=1}^{n-1} (2j-n) p^j \,, \tag{3.28}$$

by adding the previous equalities we get:

$$\begin{aligned}
(3.20) + (3.27) + (3.28) &= \binom{n-1}{2} p^n + \sum_{k=0}^{n-1} k p^k - \sum_{k=0}^{n-1} k p^{k-1} + n \sum_{i=1}^{n-1} p^{i-1} - n \sum_{i=1}^{n-1} p^i + \sum_{k=0}^{n-1} p^k \\
&= \binom{n-1}{2} p^n + \sum_{k=0}^{n-1} k p^k - \sum_{k=0}^{n-2} (k+1) p^k + n(1-p) \sum_{k=0}^{n-2} p^k + \sum_{k=0}^{n-1} p^k \\
&= \binom{n-1}{2} p^n + n(1-p^{n-1}) + \sum_{k=1}^{n-1} p^k - \sum_{k=0}^{n-2} p^k \\
&= \binom{n-1}{2} p^n + n - 1 \,.
\end{aligned}$$

If we add this to (3.17), we obtain the desired cardinality. □

From this lemma we can deduce the following proposition.

Proposition 3.2.12. *The system formed by the vectors $(\chi_i^p)_{i \in \{1,\dots,n\}}$ and the vectors $(\chi_i, \chi_j) \cdot X^\nu$ such that ν verifies the following conditions*

1. *$\nu_i \neq p-1$ or $\nu_j \neq p-1$*
2. *$\max(\mathrm{supp}(\nu)) = \max\{s | \nu_s \neq 0\} \leq j$*
3. *if $\nu_j = p-1$, then $\nu_k = 0$ for $k \in \{i+1, \dots, j-1\}$.*

forms a basis of M_n.

Proof. Let

$$\mathcal{B} = f(\mathcal{E}) - F \,,$$

where $\mathcal{E}$ is our usual basis for $F_{n,p}$ and f is the endomorphism defined in the proof of the Lemma 3.2.11. Then $\psi(\mathcal{B})$ is a basis for M_n, where ψ is the morphism defined in (3.15). However, a vector of $v \in \mathcal{E}$ is in $f^{-1}(F)$ if and only if one of the following condition is true:

1. if v is equal to

$$e_i \cdot X^\nu \,, \quad \nu \neq (0, \dots, 0) \,, \tag{3.29}$$

because $f(e_i \cdot X^\nu) = R(i, \nu)$ according to (3.26).

2. if v is equal to
$$e_{(i,j)} \cdot X_i^{p-1} X_j^{p-1} \prod_{s \notin \{i,j\}} X_s^{m_s}\,, \tag{3.30}$$
because $f(v) = R(i,j,m)$ according to (3.19) and (3.26).

3. if v is equal to
$$e_{(i,j)} \cdot X_k^{m_k} \prod_{s<k} X_s^{m_s}\,, \tag{3.31}$$
where $m_k \neq 0$, because $f(v) = jac_1(i,j,k,m = (m_1,\dots,m_{k-1},m_k-1))$ according to (3.26).

4. if v is equal to
$$e_{(i,k)} \cdot X_k^{p-1} X_j^{m_j} \prod_{s \leq i<j} X_s^{m_s}\,, \quad 1 \leq i < j < k \leq n \tag{3.32}$$
where $m_j \neq 0$, because $f(v) = jac_2(i,j,k,m = (m_1,\dots,m_{j-1},m_j-1))$

Let us negate this conditions and prove how they imply the corollary:

1. thanks to (3.29),we get that $\psi(f(e_i \cdot X^\nu))$ is in the basis $\psi(\mathcal{B})$ if and only if $\nu = (0,\dots,0)$, hence only remains the $\psi(e_i)$'s which are the χ_i^p's according to (3.15).

2. thanks to (3.30) and the definition of ψ (see (3.15)) which sends $e_{i,j}$ to (χ_i,χ_j), we get the first condition on ν, which means $\nu_i \neq p-1$ or $\nu_j \neq p-1$.

3. thanks to (3.31), we get the second condition on ν, which means $\max \mathrm{supp}(\nu) \leq j$.

4. thanks to (3.32), we get the third condition on ν, which means: if $\nu_j = p-1$, then $\nu_k = 0$ for $k \in \{i+1,\dots,j-1\}$.

□

Notation 3.2.13. From now on, the above basis will be denoted $\mathcal{B}_{M_n}$.

Corollary 3.2.14. *The module M_n admits the following presentation by generators and relations:*

- *its generators are the χ_i^p and the (χ_i,χ_j) where i and j are in $\{1,\dots,n\}$ and $i<j$.*
- *The relations are given by*
  1. $\chi_i^p \cdot X_i = 0$,
  2. $\chi_i^p \cdot X_j = (\chi_j,\chi_i) \cdot X_i^{p-1}$ *if* $i>j$,
  3. $\chi_i^p \cdot X_j = -(\chi_i,\chi_j) \cdot X_i^{p-1}$ *if* $i<j$,
  4. $(\chi_i,\chi_j)\cdot X_k + (\chi_j,\chi_k)\cdot X_i - (\chi_i,\chi_k)\cdot X_j = 0$, *where* $i<j<k$.

Notice that, alternatively, we could have used generators (χ_i,χ_j) for $i \neq j$ (rather than just $i<j$), add the relation $(\chi_i,\chi_j) = -(\chi_j,\chi_i)$, and then delete relation (3) which is now redundant with (2). Also (4) can then be re-written in a more symmetrical form.

Proof. Let R_n be the module defined by the presentation of the corollary. It should be remarked that there exists an obvious map of modules from R_n onto M_n, for the relations verified in R_n are verified in M_n too: therefore it is clear that
$$\dim_{\mathbf{F}_p} M_n \leq \dim_{\mathbf{F}_p} R_n\,.$$
By looking closer to the proof of Propositon 3.2.12, we see that we only used the relations mentioned in the corollary in order to construct F, therefore we can show exactly by re-writing the proof of Proposition 3.2.12 that
$$\dim_{\mathbf{F}_p} R_n \leq \dim_{\mathbf{F}_p} M_n\,.$$
So the dimensions are equal, and the obvious epimorphism is an isomorphism. □

Corollary 3.2.15. *The module M_n is isomorphic to $\Omega^2(\mathbf{F}_p)$.*

Proof. The presentations of these two modules are in fact the same. Indeed, $\Omega^2(\mathbf{F}_p)$, as introduced in the previous chapter, is generated (Proposition 3.1.2) by elements of the form

1. $\eta_i \smile \eta_j$ for $1 \leq i < j \leq n$
2. ζ_i for $i \in \{1, \dots, n\}$.

The relations which are verified are in fact

1. If $0 \leq i \leq n$ then $Rel(h_i = 1, z_i = 1)$: $\zeta_i \cdot X_i = 0\,,$
2. If $j < i$ then $\mathrm{Rel}(h_j = 1, z_i = 1)$: $\zeta_i \cdot X_j - (\eta_j \smile \eta_i) \cdot X_i^{p-1} = 0\,,$
3. If $j > i$, then $\mathrm{Rel}(h_j = 1, z_i = 1)$: $\zeta_i \cdot X_j + (\eta_i \smile \eta_j) \cdot X_i^{p-1} = 0\,,$
4. If $i < j < k$, then $\mathrm{Rel}(h_i = h_j = h_k = 1)$: $(\eta_i \smile \eta_j)\cdot X_k + (\eta_j \smile \eta_k)\cdot X_i - (\eta_i \smile \eta_k)\cdot X_j = 0\,.$

Therefore the map sending ζ_i on χ_i^p and $\eta_i \smile \eta_j$ on (χ_i, χ_j) is a map of modules and in fact an isomorphism. □

Notation 3.2.16. This isomorphism will be used silently: from now on, we denote by $\mathcal{B}_{\Omega^2(\mathbf{F}_p)}$ the image of the basis $\mathcal{B}_{M_n}$ by the isomorphism introduced in the previous proof. Note that it is sufficient to read ζ_i instead of χ_i^p and $(\eta_i \smile \eta_j) \cdot X^\nu$ instead of $(\chi_i, \chi_j) \cdot X^\nu$ in Proposition 3.2.12, in order to describe this basis.

3.3 $\Omega^2(\mathbf{F}_p)$ and its restrictions

Notation 3.3.1. Let G be a finite group and H be a subgroup of G. If V is an $\mathbf{F}_pG$-module, we denote by $V \downarrow_H^G$ the module obtained by restriction of scalars from $\mathbf{F}_pG$ to $\mathbf{F}_pH$. (see [Bro94, §III.5]) If there is any ambiguity about the subgroup H (and there will be), we shall rather consider the inclusion

$$0 \longrightarrow H \xrightarrow{\psi} G$$

and write $V \downarrow_\psi$, instead of $V \downarrow_H^G$.

It is well-known that if P is a projective $\mathbf{F}_pG$-module and H is a subgroup of G, then $P \downarrow_H$ is again a projective module. Therefore it is not hard to see that for every $\mathbf{F}_pG$-module M, we have

$$\Omega(M) \downarrow_H = \Omega(M \downarrow_H) \oplus P\,,$$

where P is a projective module.

Notation 3.3.2. As we are going to work with restrictions, we would like to keep track of the groups with which we are working, therefore we will write $\Omega_n^2(\mathbf{F}_p)$ for the E_n-module previously described in Theorem 3.1.2.

Let r be an integer (with $r \leq n$): our goal here is, not only to find the copy of the E_r-module $\Omega_r^2(\mathbf{F}_p)$ inside the E_n-module $\Omega_n^2(\mathbf{F}_p)$, but to study the action of E_n on this linear subspace of $\Omega_n^2(\mathbf{F}_p)$ and to find another copy of $\Omega_{n-r}^2(\mathbf{F}_p)$ and, again, study the action of E_n-on it.

Notation 3.3.3. For convenience, we will put $r' = n - r$.

Since there are more than one copy of E_r (or $E_{r'}$) in $E_{r+r'}$, we shall specify the ones we are considering. Remember that $(x_i)_{1 \leq i \leq s}$ is the canonical basis of $E_s = C_p^s$.

Notation 3.3.4. We set ${}_r^{r+r'}\psi \colon E_r \longrightarrow E_{r+r'}$, which verifies ${}_r^{r+r'}\psi(x_i) = x_i$ for $i \in \{1, \dots, r\}$ and $\psi_{r'}^{r+r'} \colon E_{r'} \longrightarrow E_{r+r'}$ such that $\psi_{r'}^{r+r'}(x_i) = x_{r+i}$.

It is not hard to see that, in the module $\Omega^2_{r+r'}(\mathbf{F}_p)\downarrow^{r+r'}_{r}{}_{\psi}$, the copy of $\Omega^2_r(\mathbf{F}_p)$ is simply generated as a module by the vectors ζ_i for $1 \leq i \leq r$ and $\eta_k \smile \eta_l$ for $1 \leq k < l \leq r$.

Notation 3.3.5. Therefore let us set N_1 the $E_{r+r'}$-submodule of $\Omega^2_{r+r'}(\mathbf{F}_p)$ generated by these vectors. In a similar fashion, and for the same reasons, put $N_2 = \mathrm{Span}_{\mathbf{F}_p E_{r+r'}}(\zeta_i,\, \eta_k \smile \eta_l)$, where $r+1 \leq i \leq r+r'$ and $r+1 \leq k < l \leq r+r'$.

Lemma 3.3.6. *A basis $\mathcal{B}_{r'}$ of N_2 over $\mathbf{F}_p$ is given by the following vectors*

- *ζ_i for $r+1 \leq i \leq r+r'$,*
- *$(\eta_i \smile \eta_j)\cdot X^\nu$ where $r+1 \leq i < j \leq r+r'$ and $(\eta_i \smile \eta_j)\cdot X^\nu$ is in the basis $\mathcal{B}_{\Omega^2(\mathbf{F}_p)}$ (see Proposition 3.2.12),*
- *$(\eta_i \smile \eta_j)\cdot X^\nu X_j^{p-1}$ where $1 \leq i \leq r$ and $r+1 \leq j$, and such that this vector is in the basis $\mathcal{B}_{\Omega^2(\mathbf{F}_p)}$ (which means $\nu_k = 0$ if $k > j$ or $j > k > i$, and $\nu_i \neq p-1$).*

Proof. Note that those vectors are linearly independent, since they are a subset of the previously found basis. It remains to prove that they do generate N_2 as a vector space. Since N_2 is generated as a module by the union of the families $(\zeta_i)_{r+1\leq i\leq r+r'}$ and $(\eta_k \smile \eta_l)_{r+1\leq k<l\leq r+r'}$, it is sufficient to check that for every multi-index ν (such that $\nu_i < p$), $\zeta_i \cdot X^\nu$ or $(\eta_k \smile \eta_l)\cdot X^\nu$ may be written as a sum of those vectors.

Fix ν. If $\nu_i \neq 0$, then $\zeta_i \cdot X^\nu = 0$, so we may as well suppose that $\nu_i = 0$. Now set $k = \max\{j | \nu_j \neq 0\}$. If $k > i$, then we have according to the relation (3.13)

$$\zeta_i \cdot X^\nu = -(\eta_i \smile \eta_k)\cdot X_i^{p-1} X^{\nu'},$$

where $\nu' = (\nu_1, \ldots, \nu_{k-1}, \nu_k - 1, \nu_k, \ldots, \nu_{r+r'})$. Furthermore if $k < i$, then we have

$$\zeta_i \cdot X^\nu = (\eta_k \smile \eta_i)\cdot X_i^{p-1} X^{\nu'},$$

where $\nu' = (\nu_1, \ldots, \nu_{k-1}, \nu_k - 1, \nu_k, \ldots, \nu_{r+r'})$.

Now, let us look at what happens to the vectors $\eta_i \smile \eta_j$ under the action of $\mathbf{F}_p E_{r+r'}$ (so we do not suppose that $\nu_i = 0$). It is known that if $\nu_i = \nu_j = p-1$, then $(\eta_i \smile \eta_j)\cdot X^\nu = 0$. If $\max\{j | \nu_j \neq 0\} > j$, according to (3.21), we get that

$$(\eta_i \smile \eta_j)\cdot X^\nu = (\eta_i \smile \eta_k)\cdot X^{\nu'} - (\eta_j \smile \eta_k)\cdot X^{\nu''},$$

where $\nu' = (\nu_1, \ldots, \nu_j + 1, \ldots, \nu_k - 1, \ldots, \nu_{r+r'})$ and $\nu'' = (\nu_1, \ldots, \nu_i + 1, \ldots, \nu_k - 1, \ldots \nu_{r+r'})$. □

For N_1, we have a similar lemma.

Lemma 3.3.7. *A basis $\mathcal{B}_r$ (over $\mathbf{F}_p$) of N_1 is given by the following vectors*

- *ζ_i for $1 \leq i \leq r$,*
- *$(\eta_i \smile \eta_j)\cdot X^\nu$ where $1 \leq i < j \leq r$ and ν verifies the conditions of Proposition 3.2.12,*
- *$(\eta_i \smile \eta_k)\cdot X^\nu - (\eta_j \smile \eta_k)\cdot X^{\nu'}$ such that the following conditions are verified*
  1. *$r+1 \leq k \leq r+r'$ and $1 \leq i < j \leq r$,*
  2. *$(\eta_i \smile \eta_k)\cdot X^\nu$ and $(\eta_j \smile \eta_k)\cdot X^{\nu'}$ are in the basis $\mathcal{B}_{\Omega^2_{r+r'}(\mathbf{F}_p)}$ (see Proposition 3.2.12),*
  3. *$\nu'_s - \nu_s = 0$ for all $s \notin \{i, j\}$, but $\nu'_i - \nu_i = -1$ and $\nu'_j - \nu_j = 1$,*
  4. *$\nu_k \leq p-2$*
- *$(\eta_i \smile \eta_j)\cdot X^\nu X_i^{p-1}$ where $1 \leq i \leq r$ and $r+1 \leq j \leq r+r'$, and such that this vector is in the basis $\mathcal{B}_{\Omega^2(\mathbf{F}_p)}$, which excludes the case $\nu_j = p-1$.*

Proof. Because the proof is similar to the previous one, we will only explain how the vectors $(\eta_i \smile \eta_k)\cdot X^{\nu} - (\eta_j \smile \eta_k)\cdot X^{\nu'}$ appear. Consider $(\eta_i \smile \eta_j)\cdot X^{\nu}$ and set again $k = \max\{i|\nu_i \neq 0\}$. If $k > j$, then according to 3.21, we have

$$(\eta_i \smile \eta_j)\cdot X^{\nu} = (\eta_i \smile \eta_k)\cdot X^{\nu'} - (\eta_j \smile \eta_k)\cdot X^{\nu''}\,.$$

Note that in this case $\nu'_k = \nu''_k = \nu_k - 1 \leq p-2$. Furthermore $\nu''_i - \nu'_i = -1$ and $\nu''_j - \nu'_j = 1$. Note that if those vectors are non-zero, they are in the basis of $\mathcal{B}_{\Omega^2_{r+r'}(\mathbf{F}_p)}$. □

Proposition 3.3.8. *In the $E_{r+r'}$-module $\Omega^2(\mathbf{F}_p)$, we have that*

$$N_1 \cap N_2 = \{0\}\,.$$

Proof. Rather than considering N_1, let us consider $W = \mathrm{Span}_{\mathbf{F}_p}(\mathcal{B}')$, for a certain subset $\mathcal{B}'$ of the basis $\mathcal{B}_{\Omega^2(\mathbf{F}_p)}$ introduced in Proposition 3.2.12. Remember that according to our conventions, we write ζ_i instead of χ_i^p and $\eta_i \smile \eta_j$ instead of (χ_i, χ_j) (see Notation 3.2.16).

The subset $\mathcal{B}'$ contains

- the vectors ζ_i for $i \in \{1, \ldots, r\}$,
- the vectors $(\eta_i \smile \eta_k)\cdot X^{\nu}$ where $i \leq r$. Furthermore if $k \geq r+1$, we impose the condition that $\nu_k \neq p-1$. Note that requesting that this vectors be in $\mathcal{B}_{\Omega^2(\mathbf{F}_p)}$ implies some conditions on ν properly described in see Proposition 3.2.12.

It should be remarked that $N_2 \subset \mathrm{Span}_{\mathbf{F}_p}(\mathcal{B}')$, indeed every vector appearing in the basis of N_2 given in Lemma 3.3.6 is a linear combination of vectors in $\mathcal{B}'$.

However, as pointed out earlier the basis of N_1, given in Lemma 3.3.7, written $\mathcal{B}_r$ is also a subset of $\mathcal{B}_{\Omega^2(\mathbf{F}_p)}$. Now, we have that, as subsets of $\mathcal{B}_{\Omega^2(\mathbf{F}_p)}$, $\mathcal{B}_{r'} \cap \mathcal{B}' = \emptyset$. Indeed in $\mathcal{B}_{r'}$, the vectors of the form $(\eta_i \smile \eta_j)X^{\nu}$ where $i \leq r$ are always such that $j \geq r+1$ (of course $j = \max(\mathrm{supp}(\nu))$ according to Proposition 3.2.12) and $\nu_j = p-1$, which is never the case for a vector of $\mathcal{B}'$. Hence as $\mathbf{F}_p$-linear subspaces

$$W = \mathrm{Span}(\mathcal{B}') \oplus_{\mathbf{F}_p} N_2\,.$$

Since $N_1 \subset W$, the Proposition is proved.

□

Chapter 4

More about the maximal elementary abelian extension

Let us now return to the study of Galois-related problems. The maximal p-elementary abelian extension has already drawn attention, such has in [AGKM01], when $p = 2$. Let us resume the notation of the previous chapters:

Notation 4.0.1. $\mathbf{k}$ is a local field, p is an odd prime number, and $\mathbf{k}$ contains a primitive p-th root of unity ξ_p; as usual $\mathcal{G}_{\mathbf{k}}(p)$ is the Galois group of a maximal pro-p-extension of $\mathbf{k}$; the field $\mathbf{K}$ will now be specialized to be the maximal p-Kummer extension of $\mathbf{k}$. Observe that $\mathbf{K}$ is in Galois correspondence with $\Phi(\mathcal{G}_{\mathbf{k}}(p))$, the Frattini subgroup; the Galois group $G = Gal(\mathbf{K}/\mathbf{k})$ is elementary abelian of rank n, and this number is also the number of generators for the Demuškin group $\mathcal{G}_{\mathbf{k}}(p) \cong \mathcal{D}_{k,n}$. We write $J = J(\mathbf{K}) = \mathbf{K}^{\times}/\mathbf{K}^{\times p}$, and recall that $J \cong J^*$, according to Lemma 1.3.2: this isomorphism will be used along the following sections silently (we may prefer to mention J or J^*, depending on the context, mostly for subjective reasons).

Recall the exact sequence of Proposition 2.1.4 :

$$0 \longrightarrow \omega_{-1}(\mathbf{F}_p) \xrightarrow{\kappa} \omega_2(\mathbf{F}_p) \xrightarrow{\pi_{\mathcal{H}}} J^* \longrightarrow 0 \ ,$$

where $\omega_i(\mathbf{F}_p)$ is stably isomorphic to $\Omega^i(\mathbf{F}_p)$. Under our current assumptions however, the module $\omega_i(\mathbf{F}_p)$ is isomorphic to the minimal model $\Omega^i(\mathbf{F}_p)$ which is discussed in §1.6 and explicitly described in Theorem 3.1.2. Indeed, when establishing Proposition 2.1.4, we have used for $\omega_2(\mathbf{F}_p)$ a module which is now none other than M_n, and we can appeal to Corollary 3.2.15. As for $\omega_{-1}(\mathbf{F}_p)$, the proof of Proposition 2.1.4 shows that it is the unique module described in Lemma 2.1.2, and this is $\Omega^{-1}(\mathbf{F}_p)$.

In §4.1, we give a presentation of J by generators and relations, and as a result, we are able to describe an $\mathbf{F}_p$-basis for it. We exploit this and compute some invariants introduced in [AGKM01], in §4.2. Finally, we "shift" the short exact sequence of Proposition 2.1.4, in order to describe the vector bundle associated to J, in §4.3.

4.1 From M_n to J^*

Since we have a presentation by generators and relations of M_n, we can find one for J without any difficulty. In order to simplify the exposition we assume that $\mathbf{k}$ contains a primitive p^2-th root of unity denoted ξ_{p^2}; when it does not, only small changes have to be made, which will be pointed out along the text.

We recall that we have obtained a presentation of M_n in Corollary 3.2.14. The generators are in bijection with a basis of $H^2(E_n, \mathbf{F}_p)$ while the relations are in bijection with a basis of $H^3(E_n, \mathbf{F}_p)$, a phenomenon which was explained at the beginning of Chapter 3. Here we shall employ a simplified notation.

Notation 4.1.1. The generators for M_n are written χ_i^p (for $1 \leq i \leq n$) and (χ_i, χ_j) (for $1 \leq i < j \leq n$), while the relations are labelled in the following way :

$$\begin{array}{rcll} \zeta_i \smile \eta_i & : & \chi_i^p \cdot X_i = 0 & \\ \zeta_i \smile \eta_j & : & \chi_i^p \cdot X_j + (\chi_i, \chi_j) \cdot X_i^{p-1} = 0 & i < j \\ \zeta_i \smile \eta_j & : & \chi_i^p \cdot X_j - (\chi_j, \chi_i) \cdot X_i^{p-1} = 0 & i > j \\ \eta_i \smile \eta_j \smile \eta_s & : & (\chi_i, \chi_j) \cdot X_s + (\chi_j, \chi_s) \cdot X_i - (\chi_i, \chi_s) \cdot X_j = 0 & 1 \leq i < j < s \leq n \end{array}$$

Lemma 4.1.2. *The module J can be presented as:*

$$\begin{aligned} J &\cong \Omega^2(\mathbf{F}_p) / \operatorname{Span}_{\mathbf{F}_p E_n}(\delta') \\ &\cong \langle \chi_i^p, (\chi_i, \chi_j) \mid \zeta_s \smile \eta_l, \eta_{i_0} \smile \eta_{i_1} \smile \eta_{i_2}, \delta' = 0 \rangle \end{aligned}$$

where $1 \leq i < j \leq n$, $s, l \in \{1, \ldots, n\}$ and $1 \leq i_0 < i_1 < i_2 \leq n$; as for δ', it stands for the element

$$\delta' = (\chi_1, \chi_2) + (\chi_3, \chi_4) + \ldots + (\chi_{n-1}, \chi_n)\,.$$

Proof. As pointed out earlier, we shall use the isomorphism $J \cong J^*$: hence our goal is to find this presentation for J^*. Remember that the Demuškin group $\mathcal{G}_{\mathbf{k}}(p) \cong \mathcal{D}_{k,n}$ is the quotient of the free pro-p-group $\mathcal{F}_n$ by the relation $\delta = 1$ where

$$\delta = x_1^{p^k}(x_1, x_2)(x_3, x_4)\ldots(x_{n-1}, x_n)\,,$$

and $k \geq 2$ from our assumption that $\xi_{p^2} \in \mathbf{k}$ (see §1.5). It is clear that $\delta \in \Phi(\mathcal{F}_n)$.

We recall that if $\mathcal{G}$ is a pro-p-group and $\mathcal{K} \subset \Phi(G)$ is a closed subgroup of $\mathcal{G}$, then $\Phi(\mathcal{G}/\mathcal{K})$ can be identified with $\Phi(\mathcal{G})/\mathcal{K}$ according to Proposition 1.2.2. If $\mathrm{Gr}(\delta)$ denotes the smallest closed, normal subgroup containing δ, we have $\mathrm{Gr}(\delta) \subset \Phi(\mathcal{F}_n)$ and so there is an exact sequence

$$1 \longrightarrow \mathrm{Gr}(\delta) \longrightarrow \Phi(\mathcal{F}_n) \longrightarrow \Phi(\mathcal{D}_{k,n}) \longrightarrow 1\,.$$

Now by the same reasoning, we see that $\Phi^{(2)}(\mathcal{F}_n) = \Phi(\Phi(\mathcal{F}_n))$ maps onto $\Phi^{(2)}(\mathcal{D}_{k,n})$; it follows easily that there is another exact sequence

$$1 \longrightarrow \mathrm{Gr}(\delta)/(\mathrm{Gr}(\delta) \cap \Phi^{(2)}(\mathcal{F}_n)) \longrightarrow \Phi(\mathcal{F}_n)/\Phi^{(2)}(\mathcal{F}_n) \longrightarrow \Phi(\mathcal{D}_{k,n})/\Phi^{(2)}(\mathcal{D}_{k,n}) \longrightarrow 1\,.$$

With a different notation, using our identification of M_n with $\Omega^2(\mathbf{F}_p)$ (see Corollary 3.2.15) and the identification of $\Phi(\mathcal{D}_{k,n})/\Phi^{(2)}(\mathcal{D}_{k,n})$ with J^* (see Lemma 1.3.4), this says that the kernel of $\Omega^2(\mathbf{F}_2) \longrightarrow J^*$ is generated, as $\mathbf{F}_p E_n$-module, by δ', the class of δ modulo $\Phi^{(2)}(\mathcal{F}_n)$. □

Remarks.

1. If $\mathbf{k}$ does not contain ξ_{p^2}, then the element δ' becomes

$$\delta' = \chi_1^p + (\chi_1, \chi_2) + (\chi_3, \chi_4) + \ldots + (\chi_{n-1}, \chi_n)\,.$$

2. If $n = 2$, then the module J is simply isomorphic to $\mathbf{F}_p \times \mathbf{F}_p$, because its presentation is just

$$\langle \chi_1^p, \chi_2^p, (\chi_1, \chi_2) \mid \chi_1^p \cdot X_1 = \chi_2^p \cdot X_2 = 0,\ \chi_1^p \cdot X_2 = -(\chi_1, \chi_2) \cdot X_1^{p-1}, \chi_2^p \cdot X_1 = (\chi_1, \chi_2) \cdot X_2^{p-1}, (\chi_1, \chi_2) = 0 \rangle\,,$$

or in a shorter way

$$\langle \chi_1^p,\ \chi_2^p \mid \chi_1^p \cdot X_1 = \chi_1^p \cdot X_2 = \chi_2^p \cdot X_1 = \chi_2 \cdot X_2 = 0 \rangle\,.$$

This occurs when $\mathbf{k}$ has a residue field of characteristic ℓ different from p (see [Gui18, Theorem 4.8]).

We can even go a little deeper into the computations: to achieve our goal of studying some invariants, we would like in fact to find a basis of J^*. Bear in mind that the projection from the free pro-p-group $\mathcal{F}_n$ onto $\mathcal{D}_{k,n}$ induces an epimorphism $\pi_{\Phi(\mathcal{D}_{k,n})}\colon M_n \longrightarrow J^*$ (see §2.1), hence the image of the previously found basis $\mathcal{B}_{M_n}$ of M_n is a generating system of J^* (for a definition of $\mathcal{B}_{M_n}$ see Proposition 3.2.12). Nevertheless we have to get rid of some vectors in order to have a basis: those vectors can be found through the study of the kernel of

$$\pi_{\Phi(\mathcal{F}_n)}\colon \Phi(\mathcal{F}_n)/\Phi^{(2)}(\mathcal{F}_n) \longrightarrow \Phi(\mathcal{D}_{k,n})/\Phi^{(2)}(\mathcal{D}_{k,n})$$

which is generated by δ'. In order to do so, we need to introduce the following two families of maps on multi-indices

$$\begin{array}{rccc} \delta_i\colon & \mathbf{Z}^n & \longrightarrow & \mathbf{Z}^n \\ & (\nu_1,\dots,\nu_n) & \longmapsto & (\nu_1,\dots,\nu_i-1,\dots,\nu_n) \end{array}$$

and

$$\begin{array}{rccc} \gamma_i\colon & \mathbf{Z}^n & \longrightarrow & \mathbf{Z}^n \\ & (\nu_1,\dots,\nu_n) & \longmapsto & (\nu_1,\dots,\nu_i+1,\dots,\nu_n) \end{array}$$

Now we can state a technical lemma - the reader can skip its proof, for it is a silly and tedious computation.

Lemma 4.1.3. *For any multi-index $\nu \in \{0,\dots,p-1\}^n$ with $\nu \neq (0,\dots,0)$, we set*

$$I(\nu) = \left\{1 \leq s \leq \frac{n}{2} \mid \nu_{2s-1} \neq p-1 \text{ or } \nu_{2s} \neq p-1\right\},$$

and

$$\mu(\nu) = \max(\mathrm{supp}(\nu)) = \max\{s \in \mathbf{N} \,|\, \nu_s \neq 0\}.$$

Then the following equality holds in M_n :

$$\delta'\cdot X^\nu = \sum_{\substack{s=1 \\ s\in I(\nu)}}^{\lceil \frac{\mu(\nu)}{2}\rceil -1} \Big((\chi_{2s-1},\chi_{\mu(\nu)})\cdot X^{\gamma_{2s}\circ\delta_{\mu(\nu)}(\nu)} - (\chi_{2s},\chi_{\mu(\nu)})\cdot X^{\gamma_{2s-1}\circ\delta_{\mu(\nu)}(\nu)}\Big) + \sum_{\substack{s=\lceil \frac{\mu(\nu)}{2}\rceil \\ s\in I(\nu)}}^{\frac{n}{2}} (\chi_{2s-1},\chi_{2s})\cdot X^\nu . \tag{4.1}$$

Here the point is that each term on the right hand side either belongs to the basis $\mathcal{B}_{M_n}$, or is zero, as we will point out during the course of the proof.

Proof. First note that, with the understanding that $1 \leq s \leq \frac{n}{2}$, we have

$$\delta'\cdot X^\nu = \sum_{s\in I(\nu)} (\chi_{2s-1},\chi_{2s})\cdot X^\nu + \sum_{s\notin I(\nu)} (\chi_{2s-1},\chi_{2s})\cdot X^\nu ,$$

and since $(\chi_i,\chi_j)\cdot X_i^{p-1}X_j^{p-1} = 0$ according to (3.18), we have the following equality

$$(\chi_{2s-1},\chi_{2s})\cdot X^\nu = 0,$$

if $s \notin I(\nu)$. Therefore, it is sufficient to sum upon the integers which are in $I(\nu)$. Now, let us split the sum in two:

$$\sum_{s\in I(\nu)} (\chi_{2s-1},\chi_{2s})\cdot X^\nu = \sum_{\substack{s\in I(\nu) \\ s<\lceil \frac{\mu(\nu)}{2}\rceil}} (\chi_{2s-1},\chi_{2s})\cdot X^\nu + \sum_{\substack{s\in I(\nu) \\ s\geq\lceil \frac{\mu(\nu)}{2}\rceil}} (\chi_{2s-1},\chi_{2s})\cdot X^\nu .$$

Remark that the vectors in the second sum are all in the basis $\mathcal{B}_{M_n}$, whereas those on the first sum are not. To address this issue, we will use in fact the Jacobi relation (the one denoted $\eta_{2s-1} \smile \eta_{2s} \smile \eta_{\mu(\nu)}$ in (4.1.1)), hence

$$\begin{aligned}(\chi_{2s-1}, \chi_{2s}) \cdot X^{\nu} &= (\chi_{2s-1}, \chi_{2s}) \cdot X_{\mu(\nu)} X^{\delta_{\mu(\nu)}(\nu)} \\ &= (\chi_{2s-1}, \chi_{\mu(\nu)}) \cdot X_{2s} X^{\delta_{\mu(\nu)}(\nu)} - (\chi_{2s}, \chi_{\mu(\nu)}) \cdot X_{2s-1} X^{\delta_{\mu(\nu)}(\nu)}\,.\end{aligned}$$

Note that the vector $(\chi_{2s-1}, \chi_{\mu(\nu)}) \cdot X_{2s} X^{\delta_{\mu(\nu)}(\nu)}$ (resp. $(\chi_{2s}, \chi_{\mu(\nu)}) \cdot X_{2s-1} X^{\delta_{\mu(\nu)}(\nu)}$) is zero if $\nu_{2s} = p-1$ (resp. $\nu_{2s-1} = p-1$). Otherwise, let us check that it belongs to the basis $\mathcal{B}_{M_n}$, because it satisfies the conditions of Proposition 3.2.12.

Indeed, it is easy to see that $\nu_{\mu(\nu)} - 1 \leq p-2 < p-1$, hence the first and the third conditions of Proposition 3.2.12 are verified. Furthermore, by definition of $\mu(\nu) = \max(\mathrm{supp}(\nu))$, the second condition is obviously verified.

The formula in the lemma is now a simple rearrangement. □

Remark. If ξ_{p^2} is not in $\mathbf{k}$, then it is necessary to add a term $\chi_1^p \cdot X^{\nu}$. If the latter is non zero, it is equal to $-(\chi_1, \chi_{\mu(\nu)}) \cdot X_1^{p-1} X^{\delta_{\mu(\nu)}(\nu)}$.

We can now find a basis for J^*. The next proposition holds regardless of whether $\mathbf{k}$ does or does not contain ξ_{p^2}.

Proposition 4.1.4. *Remember that p is an odd prime. Let $\mathcal{B}_{M_n}$ be the basis obtained for $M_n \cong \Omega^2(\mathbf{F}_p)$ in Proposition 3.2.12. A basis $\mathcal{B}'$ of J^* is given by the image (by the projection $\pi_{\Phi(\mathcal{D}_{k,n})}$) of $\mathcal{B}_{M_n} - V$, where V is the set consisting of the vectors $(\chi_i, \chi_n) \cdot X^{\nu}$ verifying one of the following conditions:*

C1. $i = n-1$.

C2. $i \neq n-1$ *and :*

- *(a)* $\nu_n = p-2$,
- *(b) if i is even*
  - *(i)* $\nu_{i-1} \neq 0$.
  - *(ii)* $\nu_i = \nu_{i+1} = \cdots = \nu_{n-1} = p-1$.
- *(c) if i is odd*
  - *(i)* $\nu_{i+1} \neq 0$.
  - *(ii)* $\nu_{i+2} = \nu_{i+3} = \cdots = \nu_{n-1} = p-1$.

Proof. Let us at once count the vectors in the set V. There are $p^n - p^{n-2}$ vectors satisfying C1 (recall that we consider elements of $\mathcal{B}_{M_n}$, so it is required that $\nu_{n-1} \neq p-1$ or $\nu_n \neq p-1$ here). As for C2, when i is even, with of course $1 \leq i \leq n-2$, we count $(p-1)p^{i-2}$ choices, and we may as well record $(p-1)p^i$ choices for each even number i with $0 \leq i \leq n-4$; for i odd, there are $(p-1)p^i$ choices, so in total we have

$$p^n - p^{n-2} + (p-1)\left[\sum_{i=0}^{n-3} p^i\right] = p^n - 1$$

vectors in V. Writing $\pi = \pi_{\Phi(\mathcal{D}_{k,n})}$ and $K = \ker(\pi)$, we note that we also have $\dim_{\mathbf{F}_p} K = p^n - 1$, since $K \cong \Omega^{-1}(\mathbf{F}_p)$.

We claim that for each $v \in V$, it is possible to find b in the $\mathbf{F}_p$-linear span of $\mathcal{B}_{M_n} - V$ such that

$$v \equiv b \bmod K\,. \qquad (*)$$

Clearly, if we can prove the claim, then $\pi(\mathcal{B}_{M_n} - V)$ generates J^*, and comparing dimensions this set will be seen to be a basis, which is what the proposition states.

Our strategy will be to define an order relation $\preceq$ on $\mathcal{B}_{M_n}$, and to establish, using the previous lemma, that for each $v \in V$ there exists an element w which is a linear combination of elements of $\mathcal{B}_{M_n}$ which are *strictly smaller than* v with respect to $\preceq$, and such that

$$v \equiv w \bmod K\,. \tag{**}$$

The claim easily follows from this. Indeed, a *minimal* counter-example v to (*) (again, with respect to $\preceq$) would lead to a contradiction with (**).

We turn to the definition of $\preceq$, first on the vectors of the form $(\chi_i, \chi_j)\cdot X^\nu$ which are in $\mathcal{B}_{M_n}$. We set $(\chi_i, \chi_j)\cdot X^\nu \preceq (\chi_{i'}, \chi_{j'})\cdot X^\mu$ if one of the following conditions is verified:

1. $(\chi_i, \chi_j)\cdot X^\nu = (\chi_{i'}, \chi_{j'})\cdot X^\mu$,
2. $|\nu| = \sum_{i=1}^n \nu_i < |\mu| = \sum_{i=1}^n \mu_i$,
3. if $|\nu| = |\mu|$, but $\nu \neq \mu$, we set $m = \max(\mathrm{supp}(\mu - \nu))$, and the condition is $(\mu-\nu)_m \geq 0$,
4. if $\nu = \mu$ and $(\chi_i, \chi_j) \neq (\chi_{i'}, \chi_{j'})$, we require that $(i,j) \leq (i',j')$ for the lexicographic order.

We complete the definition of our order relation on $\mathcal{B}_{M_n}$ by requiring

$$\chi_1^p \preceq \chi_2^p \preceq \cdots \preceq \chi_n^p \preceq (\chi_1, \chi_2)\,.$$

Let ν' be a multi-index. We shall prove that, if $(\chi_i, \chi_n)\cdot X^{\nu'}$ belongs to V, then it is the largest vector (in the sense of $\preceq$) among the terms on the right hand side of equation (4.1) expressing $\delta'\cdot X^\nu$, for some ν. This technical fact, when established in all cases, will conclude the proof of (**), keeping in mind that $\delta'\cdot X^\nu \in K$, and thus the proposition will be proved as well.

We start with vectors satisfying C1. Note indeed that if $(\chi_{n-1}, \chi_n)\cdot X^{\nu'}$ is in the basis $\mathcal{B}_{M_n}$, then either $\nu'_{n-1} \neq p-1$ or $\nu'_n \neq p-1$, hence we may use Equation (4.1) from Lemma 4.1.3 as

$$\delta'\cdot X^{\nu'} =$$

$$\underbrace{\sum_{\substack{s=1\\ s\in I(\nu')}}^{\lceil \frac{\mu(\nu')}{2}\rceil - 1} \Big((\chi_{2s-1}, \chi_{\mu(\nu')})\cdot X^{\gamma_{2s}\circ\delta_{\mu(\nu')}(\nu')} - (\chi_{2s}, \chi_{\mu(\nu')})\cdot X^{\gamma_{2s-1}\circ\delta_{\mu(\nu')}(\nu')}\Big)}_{A} + \underbrace{\sum_{\substack{s=\lceil \frac{\mu(\nu')}{2}\rceil\\ s\in I(\nu')}}^{\frac{n}{2}-1} (\chi_{2s-1}, \chi_{2s})\cdot X^{\nu'}}_{B}$$

$$+ (\chi_{n-1}, \chi_n)\cdot X^{\nu'}\,.$$

The vector $(\chi_{n-1}, \chi_n)\cdot X^{\nu'}$ is greater than every vector in the sum A because of the third condition introduced for $\preceq$, whereas it is greater than every vector in the sum B because of the fourth condition.

Now we continue with a vector $(\chi_i, \chi_n)\cdot X^{\nu'}$ satisfying C2. We claim that the vector $(\chi_i, \chi_n)\cdot X^{\nu'}$ is the greatest appearing in $\delta'\cdot X^{\gamma_n\circ\delta_{\sigma(i)}(\nu')}$, where σ is the permutation

$$\sigma = (1,2)(3,4)\ldots(n-1,n)\,.$$

First suppose that i is odd, so that $i+1 = \sigma(i)$. Since we have supposed $\nu'_{i+1} \neq 0$, we are allowed to consider $\delta_{\sigma(i)}(\nu')$, and since $\nu'_n = p-2$, we set

$$\nu = \gamma_n \circ \delta_{\sigma(i)}(\nu')\,,$$

so that

$$\nu' = \gamma_{i+1}\circ\delta_n(\nu)\,.$$

Of course we are going to rely on (4.1) expressing $\delta' \cdot X^\nu$, but it is useful to remark that the latter will simplify quite a bit. First, the simple fact that $X_s^p = 0$ removes about half the terms from the first sum. Also, the second sum reduces to a lone term $(\chi_{n-1}, \chi_n) \cdot X^\nu$; however, recall that

$$(\chi_s, \chi_{s'}) \cdot X_s^{p-1} X_{s'}^{p-1} = 0\,,$$

according to (3.18), and note that we have $\nu_{n-1} = \nu_n = p-1$ (since we are considering $\nu = \gamma_n \circ \delta_{\sigma(i)}(\nu')$ where ν' satisfies C2).

In the end what remains is :

$$\begin{aligned}
\delta' \cdot X^\nu &= \sum_{\substack{s=1 \\ s\in I(\nu)}}^{\frac{i+1}{2}} \Big((\chi_{2s-1}, \chi_n) \cdot X^{\gamma_{2s}\circ\delta_n(\nu)} - (\chi_{2s}, \chi_n) \cdot X^{\gamma_{2s-1}\circ\delta_n(\nu)} \Big) \\
&= \sum_{\substack{s=1 \\ s\in I(\nu)}}^{\frac{i-1}{2}} \Big((\chi_{2s-1}, \chi_n) \cdot X^{\gamma_{2s}\circ\delta_n(\nu)} - (\chi_{2s}, \chi_n) \cdot X^{\gamma_{2s-1}\circ\delta_n(\nu)} \Big) + (\chi_i, \chi_n) \cdot X^{\gamma_{i+1}\circ\delta_n(\nu)} \\
&\quad -(\chi_{i+1}, \chi_n) \cdot X^{\gamma_i\circ\delta_n(\nu)}
\end{aligned}.$$

Hence the greatest term in this sum is $(\chi_i, \chi_n) \cdot X^{\gamma_{i+1}\circ\delta_n(\nu)}$, as announced, because of the third condition in the definition of $\preceq$.

In the very final case when i is even, the computation is similar. This concludes the proof. □

Remarks.

1. We start with a computational remark which prepares what follows. We would like to point out a particular case of a formula just obtained. Take $i = 1$, assume as above that $\nu = \gamma_n \circ \delta_2(\nu')$ where $(\chi_1, \chi_n) \cdot X^{\nu'}$ satisfies C2, and assume further that $\nu_1 = p-1$, or equivalently $\nu'_1 = p-1$; now the the last displayed equation, in the above proof, reads

   $$\delta' \cdot X^\nu = (\chi_1, \chi_n) \cdot X^{\nu'}\,.$$

   This shows that the element $(\chi_1, \chi_n) \cdot X^{\nu'}$ belongs to the kernel K in this particular case.

2. We will sketch the argument for case when $\xi_{p^2} \notin \mathbf{k}$. First we note that the strategy of the above proof would be equally sound if we relaxed condition (**) to state that each $v \in V$ satisfies $v \equiv w \bmod K$ with w a linear combination of elements of the basis $\mathcal{B}_{M_n}$, each of which *either* is strictly lower than v *or* does not belong to V. (That is, a minimal counter-example to (*) would again lead to a contradiction with this.)

   Now, when $\xi_{p^2} \notin \mathbf{k}$, the relation δ' becomes

   $$\chi_1^p + (\chi_1, \chi_2) + (\chi_3, \chi_4) + \ldots + (\chi_{n-1}, \chi_n)\,,$$

   and we have to take into account, when computing $\delta' \cdot X^\nu$, the extra term $\chi_1^p \cdot X^\nu$. This term is zero if $\nu_1 \neq 0$. As a result, the observation of remark (1) applies also in the case $\xi_{p^2} \notin \mathbf{k}$.

   However when $\nu_1 = 0$ and $\nu \neq (0, \ldots, 0)$, according to (3.9) the extra term is equal to :

   $$-(\chi_1, \chi_m) X_1^{p-1} X^{\delta_m(\nu)} \quad (m = \max \operatorname{supp}(\nu)).$$

   Now, this term may very well be (up to a sign!) an element of V. However, we are lucky indeed, for this happens only when $m = n$, and in this situation, it is also in K, as follows from remark (1).

   All in all, the extra term is always either in $\mathcal{B}_{M_n} - V$ or in K, and this allows us to establish the amended version of (**). The rest of the proof is identical.

4.2 Computing some invariants

In their article ([AGKM01]), the authors introduce some invariants for various fields, including local fields and C-fields; here we focus only on local fields, and we will show how their results, obtained for $p = 2$, might be extended when p is an odd prime number. Note that the following results mostly depend upon Proposition 4.1.4 which holds in all cases, provided that $p \neq 2$: therefore what follows is true if $\xi_{p^2} \notin \mathbf{k}$. Nevertheless, for simplicity of exposition, we will assume from now on that $\xi_{p^2} \in \mathbf{k}$. The proof in the alternative case only requires minor changes, which are left to the reader.

We recall that the *socle* $\mathrm{Soc}(M)$ of the $\mathbf{F}_pG$-module M is the largest semisimple submodule of M. When G is a finite p-group, the only simple $\mathbf{F}_pG$-module is the trivial one, and it follows easily that $M = M^G$, the submodule of elements fixed under the action of G.

The socle series of M is defined by

$$\begin{cases} \mathrm{Soc}^0(M) &= \{0\} \\ \mathrm{Soc}^j(M)/\mathrm{Soc}^{j-1}(M) &= \mathrm{Soc}(M/\mathrm{Soc}^{j-1}(M)) \end{cases}$$

Therefore we have

$$\mathrm{Soc}^0(M) \subset \mathrm{Soc}^1(M) \subset \mathrm{Soc}^2(M) \subset \cdots$$

If M is of finite type, there exists a minimal integer $\ell(M)$ such that $\mathrm{Soc}^{\ell(M)}(M) = M$ (this is because $\mathrm{Soc}(M)$ is nonzero when M is nonzero, as M certainly contains a simple submodule). This integer is called *the length* of M.

Similarly, the *radical* $\mathrm{Rad}(M)$ is the smallest submodule of M with semisimple quotient. The radical series is defined by $\mathrm{Rad}^{j+1}(M) = \mathrm{Rad}(\mathrm{Rad}^j(M))$, and $\mathrm{Rad}^0(M) = M$. We have

$$\mathrm{Rad}^0(M) \supset \mathrm{Rad}^1(M) \supset \mathrm{Rad}^2(M) \supset \cdots$$

Again, if M is of finite type, then there is a smallest integer, say $\ell'(M)$, such that $\mathrm{Rad}^{\ell'(M)}(M) = \{0\}$.

However, here are a couple of classical facts : first $\mathrm{Soc}^j(M)$ is comprised of the elements of M which are killed by $\mathrm{Rad}^j(\mathbf{F}_pG)$; second, we have $\mathrm{Rad}^j(M) = M \cdot \mathrm{Rad}^j(\mathbf{F}_pG)$. From this, it follows easily that $\ell'(M) = \ell(M)$.

From now on, Notation 4.0.1 is in force again. In particular, the integer n is defined, and the above definitions will be specialized to $G = E_n$. We shall use that $\mathrm{Rad}(\mathbf{F}_pE_n)$ is the augmentation ideal, which is the linear span of our elements X_i. As a result, $\mathrm{Rad}^j(\mathbf{F}_pE_n)$ is the linear span of the elements X^ν with $|\nu| = j$.

In [AGKM01, Theorem 5.2,5.3,5.15], a formula is proved, which relates the length of the module $\Phi(\mathcal{G}_\mathbf{k}(2))/\Phi^2(\mathcal{G}_\mathbf{k}(2))$ to the 2-cohomological dimension $\mathrm{cd}_2(\mathcal{G}_\mathbf{k}(2))$ of $\mathcal{G}_\mathbf{k}(2)$, the Galois group of a maximal 2-closure of the local field $\mathbf{k}$:

$$\ell(\Phi(\mathcal{G}_\mathbf{k}(2))/\Phi^2(\mathcal{G}_\mathbf{k}(2))) + \mathrm{cd}_2(\mathcal{G}_\mathbf{k}(2)) = \dim_{\mathbf{F}_2} H^1(\mathcal{G}_\mathbf{k}(2), \mathbf{F}_2) + 1\,.$$

The authors establish the same formula for C-fields, and indeed ask whether it holds in general. Our goal is to provide a similar expression for p odd, when $\mathbf{k}$ is a local field. Please note that the following proposition does not require $\mathbf{k}$ to contain a primitive p-th root of unity.

Proposition 4.2.1. *When* $\mathbf{k}$ *is a local field, the following identity holds:*

$$\ell(\Phi(\mathcal{G}_\mathbf{k}(p))/\Phi^2(\mathcal{G}_\mathbf{k}(p))) + \mathrm{cd}_p(\mathcal{G}_\mathbf{k}(p)) = (p-1)\dim H^1(\mathcal{G}_\mathbf{k}(p), \mathbf{F}_p) + 1\,,$$

where $\mathrm{cd}_p(\mathcal{G}_\mathbf{k}(p))$ *is the* p*-cohomological dimension of* $\mathcal{G}_\mathbf{k}(p)$*.*

We have stated the formula so that it could be easily compared to its counterpart for $p = 2$. Recall of course that $\Phi(\mathcal{G}_\mathbf{k}(p))/\Phi^2(\mathcal{G}_\mathbf{k}(p))$ is denoted by J^* elsewhere in this thesis, including the following proof.

Proof. Let $n = \dim_{\mathbf{F}_p} H^1(\mathcal{G}_{\mathbf{k}}(p), \mathbf{F}_p)$. There are only two possibilities for $\mathcal{G}_{\mathbf{k}}(p)$: the free pro-$p$-group $\mathcal{F}_n$ (when $\mathbf{k}$ does not contain a primitive p-th root of unity) or a Demuškin group $\mathcal{D}_{k,n}$ (when $\xi_p \in \mathbf{k}$): see §1.5. Let us distinguish between both cases.

First, let us assume that $\mathcal{G}_{\mathbf{k}}(p)$ is a free pro-p-group, so that $\mathrm{cd}_p(\mathcal{G}_{\mathbf{k}}(p)) = 1$ (see [Ser94, §3, Proposition 16]). We must prove that the length of $J^* \cong M_n$ is in fact equal to $n(p-1)$.

On the one hand, remark that $M_n \cdot \mathrm{Rad}^{n(p-1)}(\mathbf{F}_p E_n) = \{0\}$. Bear in mind that $\mathrm{Rad}^{n(p-1)}(\mathbf{F}_p E_n) = \mathrm{Span}_{\mathbf{F}_p}(\mathrm{N})$, where $\mathrm{N} = \sum_{g \in E_n} g = \prod_{i=1}^{n} X_i^{p-1}$. But we have:

$$\begin{array}{rcll} \chi_i^p \cdot \mathrm{N} & = & 0 & \text{(because } \chi_i^p \cdot X_i = 0 \quad (3.12)) \\ (\chi_i, \chi_j) \cdot \mathrm{N} & = & 0 & \text{(because } (\chi_i, \chi_j) \cdot X_i^{p-1} X_j^{p-1} = 0 \quad (3.18)) \end{array}$$

On the other hand, $M_n \cdot \mathrm{Rad}^{n(p-1)-1}(\mathbf{F}_p E_n) \neq \{0\}$, for $(\chi_1, \chi_n) X_n^{p-2} \prod_{i<n-1} X_i^{p-1}$ is non-zero: it is a vector of the basis $\mathcal{B}_{M_n}$, since it verifies all the conditions required in Proposition 3.2.12. This concludes the argument in the first case.

Secondly, let us suppose that $\mathcal{G}_{\mathbf{k}}(p)$ is a Demuškin group (now Notation 4.0.1 is in force, as in the rest of this chapter). By definition $\mathrm{cd}_p(\mathcal{G}_{\mathbf{k}}(p)) = 2$, and we must prove that the length of J is equal to

$$\ell(J) = (p-1)n - 1\,.$$

Remember that we have set

$$\sigma = (1,2)(3,4)\dots(n-1,n) \in \mathfrak{S}_n\,,$$

note that the permutation σ is meant to send an integer i to the integer j such that (x_i, x_j) or (x_j, x_i) appears in the Demuškin relation. Now, let us compute the length of J.

The first step is to remark that $J \cdot \mathrm{Rad}^{(p-1)n-1}(\mathbf{F}_p E_n) = \{0\}$. Consider indeed the presentation that we have given in Lemma 4.1.2. Take $X^\nu \in \mathrm{Rad}^{(p-1)n-1}(\mathbf{F}_p)$, that is, with $|\nu| = (p-1)n-1$: then obviously for every $i \in \{1,\dots,n\}$, we have $\nu_i \geq p-2 \neq 0$ (bear in mind that p is odd).

Therefore, it is easy to see that $\chi_i^p \cdot X^\nu = 0$, since $\nu_i > 0$ and $\chi_i^p \cdot X_i = 0$ (cf (4.1.1)). Furthermore, take (χ_i, χ_j) and set $\nu = (p-1, \dots, \underbrace{p-2}_{s\text{-th position}}, \dots, p-1)$. Note that if $s \notin \{i,j\}$, since $(\chi_i, \chi_j) \cdot X_i^{p-1} X_j^{p-1} = 0$, it is obvious that $(\chi_i, \chi_j) \cdot X^\nu = 0$. We now turn to the cases $s = i$ with j odd.

We have (with the notation of (4.1.1))

$$\begin{array}{rcll} (\chi_i, \chi_j) \cdot X^\nu & = & (\chi_j, \chi_{\sigma(j)}) \cdot X_n^{\gamma_i(\delta_{\sigma(j)}(\nu))} & (\eta_i \smile \eta_j \smile \eta_{\sigma(j)}) \\ & = & -\sum_{\substack{s=0 \\ 2s+1 \neq j}}^{\frac{n}{2}-1} (\chi_{2s+1}, \chi_{2s+2}) \cdot X^{\gamma_i(\delta_{\sigma(j)}(\nu))} & (\delta') \\ & = & 0 & . \end{array}$$

The last equality comes again from the fact that $(\chi_{2s+1}, \chi_{2s+2}) \cdot X_{2s+1}^{p-1} X_{2s+2}^{p-1} = 0$, according to (3.18).

We leave it to the reader to treat similarly the case when j is odd and the case $s = j$. This concludes the first step.

It remains to see that $J \cdot \mathrm{Rad}^{(p-1)n-2}(\mathbf{F}_p E_n) \neq \{0\}$, since for instance $(\chi_1, \chi_n) \cdot X_n^{p-3} \prod_{j=1}^{n-1} X_j^{p-1}$ is in the basis of J described in Proposition 4.1.4: hence it is non-zero.

This finishes the proof. □

Another noteworthy statement of the paper [AGKM01] is the following proposition, which is only proved when $p = 2$, but which could be established *mutatis mutandis* for p odd (although we shall not use this, and mention the result for motivation only).

Proposition 4.2.2 ([AGKM01] 3.10)**.** *In the mod p Lyndon-Hochschild-Serre spectral sequence for the group extension*

$$1 \longrightarrow \Phi(\mathcal{G}_{\mathbf{k}}(p)) \longrightarrow \mathcal{G}_k(p) \longrightarrow E_n \longrightarrow 1 \ ,$$

we have $E_\infty^{1,1} \cong \mathrm{Soc}^2(J)/\mathrm{Soc}(J)$.

After a concrete computation of the dimension of $E_\infty^{1,1}$, the authors deduce the dimension of $\mathrm{Soc}^2(J)/\mathrm{Soc}(J)$, when $p = 2$ ([AGKM01, Example 5.6]). In this case they obtained:

$$\begin{cases} \dim_{\mathbf{F}_2} \mathrm{Soc}^2((\Omega^2(\mathbf{F}_2)^*)/\mathrm{Soc}^1(\Omega^2(\mathbf{F}_2))^*) &= \frac{n(n+1)(n-1)}{3} \\ \dim_{\mathbf{F}_2} \mathrm{Soc}^2(J)/\mathrm{Soc}(J) &= \frac{n(n-2)(n+2)}{3} \end{cases}$$

This is what we propose to generalize for p odd, by direct arguments.

In fact when p is even, a particular phenomenon occurs, as a consequence of the relation

$$\chi_i^2 \cdot X_j = -(\chi_i, \chi_j) \cdot X_i^{2-1=1} \ .$$

As long as p is an odd prime $p-1$ will be different from 1, hence the proof is slightly different from the previous one, because we have to take account of terms $\chi_i^p \cdot X_j$, as we shall soon see.

Proposition 4.2.3. *With the notation as in 4.0.1, we have on the one hand*

$$\dim_{\mathbf{F}_p} \mathrm{Soc}^2(\Omega^2(\mathbf{F}_p)^*)/\mathrm{Soc}(\Omega^2(\mathbf{F}_p)^*) = \frac{n(n+1)(n-1)}{3} \ ,$$

and on the other

$$\dim_{\mathbf{F}_p} \mathrm{Soc}^2(J)/\mathrm{Soc}(J) = \frac{n(n-2)(n+2)}{3} \ ,$$

where the modules considered are $\mathbf{F}_p E_n$*-modules.*

Proof. Rather than working with the socle series, we will study the radical series; recall indeed that

$$(\mathrm{Soc}^k(M)/\mathrm{Soc}^{k-1}(M))^* \cong \mathrm{Rad}^{k-1}(M^*)/\mathrm{Rad}^k(M^*) \ .$$

(For example see [Web16, Exercise 6.7].) Since we seek to compute the dimensions, we may as well work with $\mathrm{Rad}(M^*)/\mathrm{Rad}^2(M^*)$.

Let us put $R^i = \mathrm{Rad}^i(\Omega^2(\mathbf{F}_p))$ for all $i \geq 0$, and compute the dimension of R^1/R^2. We shall use a partition of the basis $\mathcal{B}_{M_n}$ from Proposition 3.2.12 : let us put $S = \{\chi_i^p \mid 1 \leq i \leq n\}$, $T_0 = \{(\chi_i, \chi_j) \mid 1 \leq i < j \leq n\}$, $T_1 = \{(\chi_i, \chi_j) \cdot X_s \mid 1 \leq i < j \leq n, s \leq j\}$, and finally

$$T_2 = \{(\chi_i, \chi_j) \cdot X^\nu \in \mathcal{B}_{M_n} \text{ with } |\nu| \geq 2\} \ .$$

Then $\mathcal{B}_{M_n}$ is the disjoint union $S \cup T_0 \cup T_1 \cup T_2$, and we make a series of observations, culminating with the fact that the dimension of R^1/R^2 is the cardinality of T_1. We shall also see that R^2 is the linear span of T_2.

The first observation is that $T_1 \subset R^1$ and $T_2 \subset R^2 \subset R^1$, so that $S \cup T_0$ generates R^0/R^1. As a result, the elements $x \cdot X_s$ for $x \in S \cup T_0$ and $1 \leq s \leq n$ generate R^1/R^2 as a vector space.

A second observation, however, is that for $\chi_i^p \in S$, the element $\chi_i^p \cdot X_j$ lies in R^2, for all j. Indeed, if $j = i$, we have $\chi_i^p \cdot X_i = 0$, however if $i \neq j$, we have

$$\chi_i^p \cdot X_j = \begin{cases} -(\chi_i, \chi_j) \cdot X_i^{p-1} & \text{if} \quad i < j \\ (\chi_j, \chi_i) \cdot X_i^{p-1} & \text{if} \quad j < i \end{cases} \ .$$

Since $p \geq 3$, we have that $\chi_i^p \cdot X_j \in R^2$ as announced. (In fact $\chi_i^p \cdot X_j$ is in the linear span of T_2, and we use this below.)

We also need to point out that, if $x \in T_0$ and $1 \leq s \leq n$, then $x \cdot X_s \in \langle T_1 \rangle$, the linear span of T_1. While this is clear if $s \leq j$, for $1 \leq i < j < s \leq n$ we use the relation $\eta_i \smile \eta_j \smile \eta_s$, that is

$$(\chi_i, \chi_j) \cdot X_s = (\chi_i, \chi_s) \cdot X_j - (\chi_j, \chi_s) \cdot X_i \ , \tag{4.2}$$

At this point, we deduce that the classes of the elements of T_1 generate R^1/R^2. It remains to show that $\langle T_1\rangle \cap R^2 = \{0\}$.

To see this, we make our final observation: the linear span $\langle T_2\rangle$ is in fact a submodule, that is if $x \in T_2$ and $1 \leq s \leq n$, we have $x \cdot X_s \in \langle T_2\rangle$. In order to establish this, the reader will complete the following sketch. Let $x = (\chi_i, \chi_j) \cdot X^\nu \in T_2$. The element $x \cdot X_s$ satisfies condition (1) from Proposition 3.2.12 unless it is zero, from (3.18); if it does not satisfies condition (3) from the same proposition, apply (3.24) to reduce to the case when it does ; and if it does not satisfies condition (2), apply (4.2) above. These steps allow us to rewrite $x \cdot X_s$ as a linear combination of elements from the basis $\mathcal{B}_{M_n}$, and we check immediately that the terms appearing are actually in T_2. This completes the sketch.

A similar remark is that, if $x \in T_1$ and $1 \leq s \leq n$, then $x \cdot X_s \in \langle T_2\rangle$. Together, the facts we have collected imply that for any $x \in \mathcal{B}_{M_n}$ and any indices i, j, we have $x \cdot X_i X_j \in \langle T_2\rangle$.

We can conclude that $R^2 \subset \langle T_2\rangle$, and thus that $R^2 = \langle T_2\rangle$. As $\mathcal{B}_{M_n}$ is a basis, we certainly know that $\langle T_1\rangle \cap \langle T_2\rangle = \{0\}$, and this concludes the proof of our claim, according to which the dimension of R^1/R^2 is the cardinality of T_1.

Let us count the vectors $(\chi_i, \chi_j) \cdot X_s$ in T_1. If we fix j, we have j choices for s and $j-1$ choices for i, hence

$$\begin{aligned} \dim_{\mathbf{F}_p} \operatorname{Rad}(\Omega^2(\mathbf{F}_p))/\operatorname{Rad}^2(\Omega^2(\mathbf{F}_p)) &= \sum_{j=0}^{n} (j-1)j \\ &= \tfrac{1}{6}n(n+1)(2n+1) - \tfrac{n(n+1)}{2} \\ &= \tfrac{1}{3}n(n+1)(n-1) \end{aligned} \quad .$$

Now, let us address the case of $J \cong J^*$. The homomorphism $\pi = \pi_{\Phi(\mathcal{D}_{k,n})} \colon \Omega^2(\mathbf{F}_p) \longrightarrow J^*$ certainly maps $\operatorname{Rad}^s(\Omega^2(\mathbf{F}_p))$ into $\operatorname{Rad}^s(J^*)$ for all $s \geq 0$, and since π is an epimorphism, we have in fact $\pi(R^s) = \operatorname{Rad}^s(J^*)$ for all s. From the above, we deduce that $\operatorname{Rad}^2(J^*) = \pi(\langle T_2\rangle)$, and that $\operatorname{Rad}^1(J^*)/\operatorname{Rad}^2(J^*)$ is generated by $\pi(\langle T_1\rangle)$. What is more, we certainly have $\pi(\langle T_1\rangle) \cap \pi(\langle T_2\rangle) = \{0\}$, as follows from Proposition 4.1.4 (the latter states that a basis for J^* is obtained from our basis for $\Omega^2(\mathbf{F}_p)$ by discarding some elements and applying π).

We conclude that the dimension of $\operatorname{Rad}^1(J^*)/\operatorname{Rad}^2(J^*)$ is also that of $\pi(\langle T_1\rangle)$. Now the set $\pi(T_1)$ is no longer linearly independent, as follows from the Demuškin relation: we may suppress the vectors $(\chi_{n-1}, \chi_n) \cdot X_k$ for $k \in \{1, \ldots, n\}$. The remaining vectors however, which are

$$(\chi_i, \chi_j) \cdot X_k\,, \quad 1 \leq i < k < j \leq n\,, \quad i < n-1\,,$$

are indeed linearly independent, as follows from Proposition 4.1.4.

Hence

$$\begin{aligned} \dim_{\mathbf{F}_p} \operatorname{Soc}^2(J)/\operatorname{Soc}(J) &= \dim_{\mathbf{F}_p} \operatorname{Rad}(J^*)/\operatorname{Rad}^2(J^*) \\ &= \dim_{\mathbf{F}_p} \operatorname{Rad}(\Omega^2(\mathbf{F}_p))/\operatorname{Rad}^2(\Omega^2(\mathbf{F}_p)) - n \\ &= \tfrac{1}{3}n(n-2)(n+2) \end{aligned}$$

The proof is complete. □

4.3 The associated vector bundle

Since $J(\mathbf{K})$ is of constant Jordan type, we would like to describe the associated vector bundle denoted $\mathfrak{V}(J(\mathbf{K}))$, where $\mathfrak{V}$ is the functor introduced in §1.1.5. In order to do so, we shall work with a module $\omega(J)$ which is stably isomorphic to $\Omega(J)$, and which fits into an exact sequence

$$0 \longrightarrow \Omega^3(\mathbf{F}_p) \xrightarrow{\varphi} \omega(J) \xrightarrow{\psi} \Omega^{-1}(\mathbf{F}_p) \longrightarrow 0\ . \tag{4.3}$$

This has independent interest. Indeed, this exact sequence must be locally split exact, as follows from Remark 5.3.5 in [Ben16]. As a result, we see that $\omega(J)$, and thus J itself, must be of constant Jordan type, and thus we have a completely different, alternative proof of this fact (in the case of the maximal Kummer extension!).

We turn to the definition of $\omega(J)$. Corresponding to the presentation of Lemma 4.1.2 is a short exact sequence

$$1 \longrightarrow \ker \pi_0 \xrightarrow{i_0} F \xrightarrow{\pi_0} J \longrightarrow 1\,,$$

where F is a free $\mathbf{F}_p E_n$ module of rank $d_2(E_n)$ (recall that we write $d_s(E_n) = \dim_{\mathbf{F}_p} H^s(E_n, \mathbf{F}_p)$). By definition, the module $\ker \pi_0$ is stably isomorphic to $\Omega(J)$. The lemma gives a system of generators for $\ker \pi_0$, and our task, of course, is to find the "relations between the relations".

Here is what the answer will be. In order to make the formulae less cumbersome, we recall the following notation for the norm:

$$\mathrm{N} = \prod_{1\le i\le n} X_i^{p-1} = \sum_{x\in E_n} x\,,$$

and the following one for a "restricted" norm:

$$\tilde{\mathrm{N}}^j = \prod_{i\neq j} X_i^{p-1}\,.$$

We then define $\omega(J)$ to be the module

$$\omega(J) = \langle \eta_j \smile \zeta_i, \eta_{i_1} \smile \eta_{i_2} \smile \eta_{i_3}, \delta' \mid \mathrm{Rel}^4(h,z), \delta'\cdot \mathrm{N} = \sum_{1\le i\le \frac{n}{2}} \eta_{2i} \smile \zeta_{2i-1}\cdot \tilde{\mathrm{N}}^{2i-1}\rangle\,,$$

where (h,z) runs through the C-indices of weight 4, the indices i,j are in $\{1,\dots,n\}$, and $1 \le i_1 < i_2 < i_3 \le n$. Here we revert to the notation of Theorem 3.1.2.

As announced, we shall establish that $\omega(J)$ is stably isomorphic to $\Omega(J)$, and we shall accomplish this by showing that $\omega(J)$ is (genuinely) isomorphic to $\ker \pi_0$.

We start by gathering basic information.

Lemma 4.3.1. *Let the modules $\omega(J)$ and $\ker \pi_0$ be as above.*

1. *The dimension of J over $\mathbf{F}_p$ is $2 + (n-2)\cdot p^n$.*
2. *There is an exact sequence*

$$0 \longrightarrow \Omega^3(\mathbf{F}_p) \xrightarrow{\varphi} \omega(J) \xrightarrow{\psi} \Omega^{-1}(\mathbf{F}_p) \longrightarrow 0\ ,$$

   where φ maps $\eta^h \smile \zeta^z \in \Omega^3(\mathbf{F})$ to the element with the same name in $\omega(J)$, while ψ maps $\eta^h \smile \zeta^z \in \omega(J)$ to 0 and maps δ' to α (with notation as in Proposition 3.1.2).
3. *We have*

$$\dim_{\mathbf{F}_p} \omega(J) = \dim_{\mathbf{F}_p} \ker \pi_0 = \dim_{\mathbf{F}_p} \Omega^3(\mathbf{F}_p) + p^n - 1\,.$$

Proof. (1) We have opened the chapter by recalling the existence of an exact sequence

$$0 \longrightarrow \Omega^{-1}(\mathbf{F}_p) \xrightarrow{\kappa} \Omega^2(\mathbf{F}_p) \xrightarrow{\pi_{\mathcal{H}}} J^* \longrightarrow 0\ .$$

The dimension of $\Omega^2(\mathbf{F}_p)$ is $1 + (n-1)p^n$ (see Lemma 3.2.3), and that of $\Omega^{-1}(\mathbf{F}_p)$ is $p^n - 1$, as $\Omega^{-1}(\mathbf{F}_p) \cong I^*$, the dual of the augmentation ideal.

(2) From the definitions of the modules involved, it is clear that φ and ψ are well-defined and that ψ is surjective. That φ is injective follows easily by inspection, as the new relation in $\omega(J)$ involves the new generator δ'. It is clear that $\varphi(\Omega^3(\mathbf{F}_p)) \subset \ker \psi$, and the induced map $\omega(J)/\varphi(\Omega^3(\mathbf{F}_p)) \longrightarrow \Omega^{-1}(\mathbf{F}_p)$ has an inverse mapping α to δ', so $\Omega^3(\mathbf{F}_p) = \ker \psi$.

(3) From (2) we see that the dimension of $\omega(J)$ is $\dim_{\mathbf{F}_p} \Omega^3(\mathbf{F}_p) + \dim_{\mathbf{F}_p} \Omega^{-1}(\mathbf{F}_p)$, and $\dim_{\mathbf{F}_p} \Omega^{-1}(\mathbf{F}_p) = p^n - 1$. On the other hand, (1) shows that $\dim_{\mathbf{F}_p} \ker \pi_0 = \dim_{\mathbf{F}_p} F - \dim_{\mathbf{F}_p} J = \dim_{\mathbf{F}_p} F - (2 + (n-2)p^n)$, and as the rank of the free module F is $d_2(E_n)$, we have $\dim_{\mathbf{F}_p} F = d_2(E_n)p^n$. Now we recall that

$$\dim_{\mathbf{F}_p} \Omega^3(\mathbf{F}_p) = d_2(E_n)p^n - \dim_{\mathbf{F}_p} \Omega^2(\mathbf{F}_p)\,,$$

from equation 3.6 at the end of §3.1; also $\dim_{\mathbf{F}_p} \Omega^2(\mathbf{F}_p) = 1 + (n-1)p^n$ as already mentioned in this proof. Rearranging terms, we get the announced result. □

Proposition 4.3.2. *The module $\omega(J)$ is isomorphic to $\ker\pi_0$, and thus is stably isomorphic to $\Omega(J)$.*

Proof. We return to the surjective map $\pi_0\colon F \longrightarrow J$. Let the generators of the free module F be labelled $\bar{\chi}_i^p$ and $(\bar{\chi}_i, \bar{\chi}_j)$, so that $\pi_0(\bar{\chi}_i^p) = \chi_i$ and $\pi_0((\bar{\chi}_i, \bar{\chi}_j)) = (\chi_i, \chi_j)$. According to Lemma 4.1.2, the module $\ker\pi_0$ is generated by the element $\varepsilon_{\delta'} := \sum_{i=1}^{\frac{n}{2}} (\bar{\chi}_{2i-1}, \bar{\chi}_{2i})$ and the elements which we now call $\varepsilon_{\eta^h\zeta^z}$, obtained from Notation (4.1.1) by "adding bars". For example, as the relation $\zeta_{2i-1} \backsim \eta_{2i}$ reads

$$-\chi_{2i-1}^p \cdot X_{2i} + (\chi_{2i-1}, \chi_{2i}) \cdot X_{2i-1}^{p-1} = 0\,,$$

we have

$$\varepsilon_{\eta_{2i}\zeta_{2i-1}} = -\bar{\chi}_{2i-1}^p \cdot X_{2i} + (\bar{\chi}_{2i-1}, \bar{\chi}_{2i}) \cdot X_{2i-1}^{p-1}\,.$$

We attempt to define a map

$$\theta\colon \omega(J) \longrightarrow \ker\pi_0$$

which satisfies $\theta(\eta^h \backsim \zeta^z) = \varepsilon_{\eta^h\zeta^z}$ and $\theta(\delta') = \varepsilon_{\delta'}$. If we can merely prove that it is well-defined, then it will be surjective, and hence an isomorphism since we have computed above that the dimensions of the two modules are equal. Hence our task is to show that the elements $\varepsilon_{\eta^h\zeta^z}$ and $\varepsilon_{\delta'}$ satisfy the relations described in our definition of $\omega(J)$.

Part of this has already been done, of course, since J is a quotient of $\Omega^2(\mathbf{F}_p)$. More precisely, we have the following commutative diagram :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Omega^3(\mathbf{F}_p) & \longrightarrow & F & \longrightarrow & \Omega^2(\mathbf{F}_p) & \longrightarrow & 0 \\
 & & {\scriptstyle \eta^h\backsim\zeta^z\mapsto\varepsilon_{\eta^h\zeta^z}}\downarrow & & {\scriptstyle =}\downarrow & & \downarrow & & \\
0 & \longrightarrow & \ker\pi_0 & \longrightarrow & F & \xrightarrow{\pi_0} & J = \Omega^2(\mathbf{F}_p)/(\delta') & \longrightarrow & 0\,.
\end{array}$$

We see that the submodule generated by the elements $\varepsilon_{\eta^h\zeta^z}$ is a homomorphic image of $\Omega^3(\mathbf{F}_p)$ within $\ker\pi_0$. Since the relations $\mathrm{Rel}^4(h', z')$ hold in $\Omega^3(\mathbf{F}_p)$, as established in Chapter 3, they must also hold in $\ker\pi_0$.

The nontrivial work occurs with the relation involving δ': we must prove that

$$\varepsilon_{\delta'} \cdot \mathrm{N} - \sum_i \varepsilon_{\eta_{2i}\zeta_{2i-1}} \cdot \tilde{\mathrm{N}}^{2i-1} = 0\,.$$

Indeed:

$$\begin{aligned}
\varepsilon_{\delta'} \cdot \mathrm{N} - \sum_{i=1}^{\frac{n}{2}} \varepsilon_{\eta_{2i}\zeta_{2i-1}} \cdot \tilde{\mathrm{N}}^{2i-1} &= \sum_{i=1}^{\frac{n}{2}} (\bar{\chi}_{2i-1}, \bar{\chi}_{2i}) \cdot \mathrm{N} - \sum_{i=1}^{\frac{n}{2}} (-\bar{\chi}_{2i-1}^p \cdot X_{2i}\tilde{\mathrm{N}}^{2i-1} + (\bar{\chi}_{2i-1}, \bar{\chi}_{2i}) \cdot X_{2i-1}^{p-1}\tilde{\mathrm{N}}^{2i-1}) \\
&= \sum_{i=1}^{\frac{n}{2}} (\bar{\chi}_{2i-1}, \bar{\chi}_{2i}) \cdot \mathrm{N} - \sum_{i=1}^{\frac{n}{2}} (\bar{\chi}_{2i-1}, \bar{\chi}_{2i}) \cdot \mathrm{N} \\
&= 0\,,
\end{aligned}$$

using $X_{2i}\tilde{\mathrm{N}}^{2i-1} = 0$ and $X_{2i-1}^{p-1}\tilde{\mathrm{N}}^{2i-1} = \mathrm{N}$. □

Remember that we have introduced in §1.1.5 a functor $\mathfrak{V}$ from the category of E_n-modules of constant Jordan type to the category of vector bundles over $\mathbf{P}_{\mathbf{F}}^{r-1}$. Furthermore, $\mathcal{O}$ denotes the structural sheaf of $\mathbf{P}_{\mathbf{F}}^{r-1}$ (see [EH01, §I.2.4]), and we have set $\mathcal{O}(j) = \mathcal{O}^{\otimes j}$ and $\mathcal{O}(-j) = (\mathcal{O}^*)^{\otimes j}$ for $j \geq 0$.

Proposition 4.3.3. *Set $\mathbf{K}/\mathbf{k}$ the maximal elementary abelian extension of a local field $\mathbf{k}$. If the characteristic of the residue field of $\mathbf{k}$ is equal to p, we have the following isomorphism:*

$$\mathfrak{V}(J(\mathbf{K})) = \mathcal{O}(p) \oplus \mathcal{O}(-p)\,;$$

however if the residue field of $\mathbf{k}$ is of characteristic prime to p, we have the isomorphism:

$$\mathfrak{V}(J(\mathbf{K})) = \mathcal{O} \oplus \mathcal{O}\,.$$

Proof. If the residue field of $\mathbf{k}$ has characteristic prime to p, then according to the remarks following Lemma 4.1.2, it appears that $J(\mathbf{K}) = \mathbf{F}_p \times \mathbf{F}_p$. Therefore $\mathfrak{V}(J) = \mathcal{O} \oplus \mathcal{O}$.

If the residue field of $\mathbf{k}$ is not prime to p, then we shall remark that $Gal(\mathbf{K}/\mathbf{k})$ is not an elementary abelian p-group of rank 2: its rank is at least 3, according to [Gui18, Theorem 4.8]. Therefore according to [Ben16, Theorem 8.12.2], the sequence that we obtain by applying the exact functor $\mathfrak{V}_{p-1}$ (denoted in [Ben16, §8.4] by $\mathcal{F}_{p-1}$) to the exact sequence (4.3), which is

$$0 \longrightarrow \mathfrak{V}_{p-1}(\Omega^3(\mathbf{F})) \longrightarrow \mathfrak{V}_{p-1}(\omega(J)) \longrightarrow \mathfrak{V}_{p-1}(\Omega^{-1}(\mathbf{F})) \longrightarrow 0 \ ,$$

splits, hence

$$\mathfrak{V}_{p-1}(\omega(J)) = \mathcal{O}(1-2p) \oplus \mathcal{O}(1) \, ,$$

according to [Ben16, Corollary 8.5.3]. Therefore if we apply [Ben16, Theorem 8.5.1], we have that

$$\mathfrak{V}(J) = \mathcal{O}(-p) \oplus \mathcal{O}(p) \, .$$

□

We have therefore established Proposition E.

Chapter 5

Some (non)-results for groups of elementary type

Since it seems the Galois module structure of $J(\mathbf{K}) = \mathbf{K}^\times/\mathbf{K}^{\times p}$, where $\mathbf{K}/\mathbf{k}$ is an elementary abelian extension of a local field $\mathbf{k}$ containing a primitive p^{th}-root of unity, is relatively under control according to Theorems 1.4.2 and 1.4.3, the reader probably wonders whether both theorems hold for an arbitrary field. Unfortunately, this is not the case.

Remember that we have set $\mathcal{G}_\mathbf{k}(p)$ for the Galois group $Gal(\mathbf{k}(p)/\mathbf{k})$, where $\mathbf{k}(p)$ is a maximal p-extension of $\mathbf{k}$. We shall focus here exclusively on the Galois-module structure of the maximal p-elementary abelian extension, in order to provide a counterexample. According to Lemma 1.3.2, this arithmetical question can be rephrased as a group theoretic one: we will in fact consider $\Phi(\mathcal{G}_\mathbf{k}(p))/\Phi^{(2)}(\mathcal{G}_\mathbf{k}(p))$ as an $E_n \simeq \mathcal{G}_\mathbf{k}(p)/\Phi(\mathcal{G}_\mathbf{k}(p))$-module. The main result of the chapter is this: we will consider a free product $\mathcal{G} = \mathcal{G}_1 * \mathcal{G}_2$ where $\mathcal{G}_1$ is free and $\mathcal{G}_2$ is a Demuškin group, so that (for certain values of the parameters at least) each of them is of the form $\mathcal{G}_\mathbf{k}(p)$ for some local field $\mathbf{k}$, but we shall establish that $\Phi(\mathcal{G})/\Phi^{(2)}(\mathcal{G})$ is not of constant Jordan type, when viewed as a $\mathcal{G}/\Phi(\mathcal{G})$-module. It is a well-known result that $\mathcal{G}$ must be itself of the form $\mathcal{G}_\mathbf{k}(p)$ for some field $\mathbf{k}$, so that there are fields not enjoying the properties of local fields discussed in this thesis.

There are good reasons to consider free products, and this is why we open, in §5.1, by recalling what groups of elementary type are, for motivation (this explains the title of the present chapter). Second, in §5.2, we will introduce some tools to study free products, in somewhat more generality than is needed for the counterexample, which appears in §5.3.

5.1 Groups of elementary type

In this section we give background information about the beautiful *elementary type conjecture*, for motivation. Strictly speaking, this is not used in the sequel.

Here, we follow closely [QW21]. It was conjectured by I. Efrat that if $\mathbf{k}$ is a field such that $\mathcal{G}_\mathbf{k}(p)$ is finitely generated, then the latter can be built from two families of pro-p-groups, the Demuškin groups and the free pro-p-groups, by applying to them two operations: the free product and the oriented semi-direct product. In order to introduce the second operation, we have to consider *oriented pairs* rather than mere groups. Throughout this section, we assume that the prime p is odd, unless we explicitly assume the converse.

Definition 5.1.1. An oriented pair $(\mathcal{G}, \chi)$ consists in a pro-p-group $\mathcal{G}$ and a continuous homomorphism $\chi\colon \mathcal{G} \longrightarrow \mathbf{Z}_p^\times$.

Remark. The vocabulary of group theory extends to the oriented pairs' one: an oriented pair $(\mathcal{G}, \chi)$ is said to verify "a group theoretic property" if $\mathcal{G}$ verifies it.

Example 5.1.2. Oriented pairs arise in a very natural way in Galois theory: consider a field $\mathbf{k}$, whose characteristic is different from p and such that $\xi_p \in \mathbf{k}$. The group $\mathcal{G}_\mathbf{k}(p)$ acts on

$\mu_\infty = \varinjlim_k \mu_k$, where $\mu_k = \{\xi \in \overline{\mathbf{k}} \mid \xi^{p^k} = 1\}$. Since $\mu_\infty \simeq \mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$, the action of $\mathcal{G}_\mathbf{k}(p)$ on it induces a continuous monomorphism χ from $\mathcal{G}_k(p)$ into $\mathrm{Aut}(\mathbf{Z}[\frac{1}{p}]/\mathbf{Z})$.

Furthermore, under the action of $\mathcal{G}_\mathbf{k}(p)$ a primitive p^k-th root of unity is sent into another primitive p^k-th root of unity, hence we have that for every $g \in \mathcal{G}_\mathbf{k}(p)$:

$$\chi(g)(\frac{1}{p^k}) = a_k \frac{1}{p^k}\,,$$

where a_k is prime to p and $1 \leq a_k \leq p^k - 1$. Thus the sequence $(a_k)_{k\geq 1}$ clearly defines an element of $\varprojlim_k (\mathbf{Z}/p^k\mathbf{Z})^\times \simeq \mathbf{Z}_p^\times$, and by a slight abuse of notation, we set $\chi(g) = (a_k)_{k\geq 1} \in \mathbf{Z}_p^\times$.

Such a morphism $\chi\colon \mathcal{G}_\mathbf{k}(p) \longrightarrow \mathbf{Z}_p^\times$ is called a *cyclotomic character*, since it describes the action of $\mathcal{G}_\mathbf{k}(p)$ on μ_∞. The oriented pair $(\mathcal{G}_\mathbf{k}(p), \chi)$ is then called a *cyclotomic pair*.

For Demuškin groups, we mention the following result by Labute (given here without details):

Theorem 5.1.3 (Labute [Lab67])**.** *If $\mathcal{D}_{k,n}$ is a Demuškin group, there exists a unique cyclotomic character $\chi\colon \mathcal{D}_{k,n} \longrightarrow \mathbf{Z}_p^\times$ satisfying a certain (mild and natural) cohomological condition. If p is odd it is defined by*

$$\chi(x_2) = (1-p^k)^{-1}\,, \quad \chi(x_i) = 1\,.$$

We shall now define the oriented semi-direct product. This operation arises in a natural way by studying the *p-Henselian fields*, however we shall remain silent about them. Yet, their study leads to the following lemma (see [EH94]):

Lemma 5.1.4. *Let $\mathbf{k}$ be a field whose characteristic is different from p, such that $\mathbf{k}$ contains ξ_p and such that $Gal(\overline{\mathbf{k}}/\mathbf{k})$ is a pro-p-group. Let m be a cardinal number. There exists a field $\mathbf{K}/\mathbf{k}$ such that the degree of transcendence of $\mathbf{K}/\mathbf{k}$ is m, and for which there is a short exact sequence*

$$1 \longrightarrow \mathbf{Z}_p^m \longrightarrow Gal(\bar{\mathbf{K}}/\mathbf{K}) \longrightarrow Gal(\bar{\mathbf{k}}/\mathbf{k}) \longrightarrow 1$$

This way of building up an absolute Galois group which is pro-p from $\mathbf{Z}_p^m$ and another absolute Galois group leads us to consider in fact the following operation on groups.

Definition 5.1.5. The oriented semidirect product of an oriented pair $(\mathcal{G}, \chi)$ with $\mathbf{Z}_p^m$, where $m \in \mathbf{N}\backslash\{0\}$, is the oriented pair $(\mathbf{Z}_p^m \rtimes \mathcal{G}, \chi\circ\pi)$, where π is the canonical projection from $\mathbf{Z}_p^m \rtimes \mathcal{G}$ onto $\mathcal{G}$ and the conjugation action of $\mathcal{G}$ on $\mathbf{Z}_p^m$ is defined by

$$(x_1, \ldots, x_m)^g = (\chi(g)x_1, \ldots, \chi(g)x_m)\,.$$

Now, since it is known that the free product of two absolute Galois groups remains an absolute Galois group, it makes sense to consider the following class of groups.

Definition 5.1.6. The class $\mathfrak{E}_p$ of elementary type pro-p-groups is the smallest class of oriented pairs verifying the following conditions:

1. Every oriented pair $(\mathcal{F}_n, \chi)$ where $\mathcal{F}_n$ is a free pro-p-group and χ is an arbitrary morphism from $\mathcal{F}_n \longrightarrow \mathbf{Z}_p^\times$ is in $\mathfrak{E}_p$.
2. Every oriented pair $(\mathcal{D}, \chi_\mathcal{D})$ where $\mathcal{D}$ is a Demuškin group and $\chi_\mathcal{D}$ is Labute's cyclotomic character (as in Theorem 5.1.3) is in $\mathfrak{E}_p$.
3. If $(\mathcal{G}_1, \chi_1)$ and $(\mathcal{G}_2, \chi_2)$ are two oriented pairs in $\mathfrak{E}_p$ then $(\mathcal{G}_1 * \mathcal{G}_2, \chi_1 * \chi_2)$ is also in $\mathfrak{E}_p$.
4. If $(\mathcal{G}, \chi)$ is in $\mathfrak{E}_p$, then for every $m \in \mathbf{N}$, the oriented semi-direct product $(\mathbf{Z}_p^m \rtimes \mathcal{G}, \chi\circ\pi)$ is also in $\mathfrak{E}_p$.

Conjecture (Efrat)**.** *Let* $\mathbf{k}$ *a field and* $\mathcal{G}_{\mathbf{k}}(p)$ *be the Galois group of a maximal pro-*p*-extension. Suppose* $\mathcal{G}_{\mathbf{k}}(p)$ *is finitely generated, then* $(\mathcal{G}, \chi\colon \mathcal{G} \longrightarrow \mathrm{Aut}(\mu_\infty) \simeq \mathbf{Z}_p^\times)$ *is an element of* $\mathfrak{E}_p$*.*

The converse of this conjecture (stating that every group which is an object of $\mathfrak{E}_p$ is the absolute pro-p-Galois group of some field) is even more mysterious: indeed it is not known if every Demuškin group is the Galois group of a maximal pro-p-closure.

Efrat's conjecture remains open, which means that to this day every finitely-generated group of the form $\mathcal{G}_{\mathbf{k}}(p)$ ever discovered is in fact of elementary type. This certainly means that the class of elementary type groups is a natural one to test a conjecture against. This is why we have investigated whether modules of constant Jordan type could always be obtained from elementary type groups; however, in this chapter we provide a counterexample, showing that the situation may be specific to local fields after all.

5.2 Free products

The goal of this section is to provide tools to better understand the following question: suppose you form the free product $\mathcal{G} = \mathcal{G}_1 * \mathcal{G}_2$ of two pro-p-groups, how does $\Phi(\mathcal{G})/\Phi^{(2)}(\mathcal{G})$, as a $\mathcal{G}/\Phi(\mathcal{G})$-module, relate to the two modules $\Phi(\mathcal{G}_i)/\Phi^{(2)}(\mathcal{G}_i)$ for $i = 1, 2$? Our main result, Proposition 5.2.7 below, produces an exact sequence which involves induced modules. A fair amount of notation is necessary, however, before we can state it.

5.2.1 Notation & Setup

Definition 5.2.1. For r a positive integer, we consider the category of weak presentations of pro-p-groups of rank r denoted $\mathfrak{pres}_r$. Its objects are pairs $(\mathcal{G}, \varphi)$ where $\mathcal{G}$ is a pro-p-group of rank r and $\varphi\colon E_r \longrightarrow \mathcal{G}/\Phi(\mathcal{G})$ is an isomorphism, whereas a morphism $\psi\colon (\mathcal{G}, \varphi_1) \longrightarrow (\mathcal{H}, \varphi_2)$ is but a (continuous) morphism $\psi\colon \mathcal{G} \longrightarrow \mathcal{H}$ of pro-p-groups such that the induced map $\tilde{\psi}\colon \mathcal{G}/\Phi(\mathcal{G}) \longrightarrow \mathcal{H}/\Phi(\mathcal{H})$ makes the following diagram commutative:

$$\begin{array}{ccc} & E_r & \\ {\scriptstyle\varphi_1}\swarrow & & \searrow{\scriptstyle\varphi_2} \\ \mathcal{G}/\Phi(\mathcal{G}) & \xrightarrow{\quad\tilde{\psi}\quad} & \mathcal{H}/\Phi(\mathcal{H}) \end{array} \tag{5.1}$$

Note that this requirement implies that ψ is an epimorphism.

Now, of course $E_r = C_p^r$ has a canonical basis: we will denote it $(e_i)_{1\leq i\leq r}$, in this chapter.

Examples 5.2.2. By a slight abuse of notation previously mentioned in §3.2, if x is an element of a pro-p-group $\mathcal{G}$, we also write x for the class of x in $\mathcal{G}/\Phi(\mathcal{G})$.

Take the free group $\mathcal{F}_r$ generated by r elements $x_1, \ldots, x_r$; we may set

$$\varphi_r(e_i) = x_i\,, \quad \forall i \in \{1, \ldots, r\}\,.$$

It is quite obvious that $(\mathcal{F}_r, \varphi_r)$ is an object of $\mathfrak{pres}_r$ (this simplified notation obviously suppresses the fact that we need to choose the generators $x_1, \ldots, x_r$).

If $\mathcal{D}_{k,r}$ is a Demuškin group, according to our own definition (see §1.5), there exists a minimal set of r generators denoted x_i verifying a particular relation, hence we may consider

$$\varphi_{k,r}(e_i) = x_i\,, \quad \forall i \in \{1, \ldots, r\}\,.$$

Again $(\mathcal{D}_{k,r}, \varphi_{k,r})$ is an object of $\mathfrak{pres}_r$, and the map which we used to write $\pi\colon \mathcal{F}_r \longrightarrow \mathcal{D}_{k,r}$, and which is the canonical presentation of $\mathcal{D}_{k,r}$, is obviously a morphism between $(\mathcal{F}_r, \varphi_r)$ and $(\mathcal{D}_{k,r}, \varphi_{k,r})$.

Remarks.

1. As we have just seen in the case of Demuškin groups and free groups, as soon as we have a presentation by generators and relations of a group $\mathcal{G}$, there is an obvious isomorphism φ between E_r and $\mathcal{G}/\Phi(\mathcal{G})$. Therefore, in those cases, we may not bother to make the distinction between $e_i \in E_r$ and $\varphi(e_i) = x_i$, which leads us to make again an abuse of notation.

2. Instead of studying weak presentations, we could have considered the category of pro-p-groups of rank r with generators, whose objects are pairs $(\mathcal{G}, S)$ where $\mathcal{G}$ is a pro-p-group of rank r and S is a set of r generators, however this category contains more information than required.

Now, let us build the family of functors $\mathfrak{J}_r \colon \mathfrak{pres}_r \longrightarrow \mathfrak{mod}(E_r)$: as expected it is simply defined on the objects by

$$\mathfrak{J}_r(\mathcal{G}, \varphi) = \Phi(\mathcal{G})/\Phi^{(2)}(\mathcal{G})\,.$$

The action of E_r is given by the action by conjugation of $\mathcal{G}/\Phi(\mathcal{G})$ through φ, which means, for $y \in \Phi(\mathcal{G})$, we put

$$\begin{array}{rcl} [y] \cdot e_i & = & [y^{\varphi(e_i)}] \\ & = & [\varphi(e_i)^{-1} y \varphi(e_i)] \end{array}$$

where $[y]$ is but the class of y modulo $\Phi^{(2)}(\mathcal{G})$. It is quite obvious that this defines an action of E_r.

For every morphism $f \colon (\mathcal{G}, \varphi_{\mathcal{G}}) \longrightarrow (\mathcal{H}, \varphi_{\mathcal{H}})$ of pro-p-groups, we have $f(\Phi^{(i)}(\mathcal{G})) \subset \Phi^{(i)}(\mathcal{H})$ for every $i \in \mathbf{N}$, so that f induces a map of abelian groups

$$\mathfrak{J}_r(f) \colon \mathfrak{J}_r(\mathcal{G}, \varphi_{\mathcal{G}}) \longrightarrow \mathfrak{J}_r(\mathcal{H}, \varphi_{\mathcal{H}})\,.$$

Furthermore the map $\mathfrak{J}_r(f)$ is E_r-equivariant: indeed for every $x \in E_r$ and $[g] \in \mathfrak{J}_r(\mathcal{G}, \varphi_{\mathcal{G}})$, we have the following equalities:

$$\begin{array}{rcll} \mathfrak{J}_r(f)([g] \cdot x) & = & [f(g^{\varphi_{\mathcal{G}}(x)})] & \text{(definitions)} \\ & = & [f(g)^{\tilde{f}(\varphi_{\mathcal{G}}(x))}] & (f \text{ is a group homomorphism}) \\ & = & [f(g)^{\varphi_{\mathcal{H}}(x)}] & \text{(commutativity of (5.1))} \\ & = & [f(g)] \cdot x = \mathfrak{J}_r(f)([g]) \cdot x\,. & \end{array}$$

Example 5.2.3. The module $\mathfrak{J}_n(\mathcal{F}_n, \varphi_n)$ is none other than M_n, as in §3.2.

Definition 5.2.4. For every morphism ρ of weak presentations, we set:

$$\kappa(\rho) = \ker(\mathfrak{J}_r(\rho))\,.$$

This is naturally an E_r-module.

Examples 5.2.5. We certainly have $\kappa(\mathrm{Id}_{\mathcal{F}_r}) = \{0\}$, while we have discovered with Proposition 2.1.4 that

$$\kappa\Big(\pi \colon (\mathcal{F}_r, \varphi_r) \longrightarrow (\mathcal{D}_{k,r}, \varphi_{k,r})\Big) = \Omega^{-1}(\mathbf{F}_p)\,.$$

Let $\mathfrak{pf\mathfrak{Grp}}_r$ denote the category of pro-p-groups of rank r. It is well known that the free products of pro-p-groups induces a bi-functor from $\mathfrak{pf\mathfrak{Grp}}_r \times \mathfrak{pf\mathfrak{Grp}}_{r'}$ to $\mathfrak{pf\mathfrak{Grp}}_{r+r'}$: we would like to extend it to the weak presentations.

Definition 5.2.6. Let $(\mathcal{G}, \varphi_{\mathcal{G}})$ and $(\mathcal{H}, \varphi_{\mathcal{H}})$ be objects respectively of $\mathfrak{pres}_r$ and $\mathfrak{pres}_{r'}$. We set $\varphi_{\mathcal{G}} * \varphi_{\mathcal{H}}$ to be

$$\begin{array}{rccl} \varphi_{\mathcal{G}} * \varphi_{\mathcal{H}} \colon & E_{r+r'} & \longrightarrow & \mathcal{G} * \mathcal{H}/\Phi(\mathcal{G} * \mathcal{H}) \\ & e_i & \longmapsto & \varphi_{\mathcal{G}} * \varphi_{\mathcal{H}}(e_i) = \left\{ \begin{array}{rl} \varphi_{\mathcal{G}}(e_i) & \text{for} \quad 1 \leq i \leq r \\ \varphi_{\mathcal{H}}(e_{i-r}) & \text{for} \quad r+1 \leq i \leq r+r' \end{array} \right. \end{array}$$

The object $(\mathcal{G} * \mathcal{H}, \varphi_{\mathcal{G}} * \varphi_{\mathcal{H}})$ is called the free product of $(\mathcal{G}, \varphi_{\mathcal{G}})$ with $(\mathcal{H}, \varphi_{\mathcal{H}})$.

5.2.2 Main result

The next proposition is the main technical result of the chapter. The statement uses the following notation: the morphisms ${}^n_r\psi : E_r \longrightarrow E_n$ and $\psi^n_{r'} : E_{r'} \longrightarrow E_n$, when $n = r + r'$, were defined in Notation 3.3.4; and whenever $\psi : H \longrightarrow G$ is a monomorphism between finite groups, and for an $\mathbf{F}_pH$-module M, the notation $M \uparrow_\psi$ refers to the usual induced module $M \otimes_\psi \mathbf{F}_pG$.

Proposition 5.2.7. *Let $\rho : (\mathcal{F}_r, \varphi_r) \longrightarrow (\mathcal{G}, \varphi_\mathcal{G})$ and $\rho' : (\mathcal{F}_{r'}, \varphi_{r'}) \longrightarrow (\mathcal{H}, \varphi_\mathcal{H})$ be morphisms in $\mathfrak{pres}_r$. Assume that $\ker(\rho) \subset \Phi(\mathcal{F}_r)$ and $\ker(\rho') \subset \Phi(\mathcal{F}_{r'})$. Put $n = r + r'$. Then there exists a short exact sequence of E_n-modules*

$$0 \longrightarrow \kappa(\rho) \uparrow_{{}^n_r\psi} \oplus \kappa(\rho') \uparrow_{\psi^n_{r'}} \longrightarrow \mathfrak{J}_n(\mathcal{F}_n, \varphi_n) \xrightarrow{\mathfrak{J}_n(\rho * \rho')} \mathfrak{J}_n(\mathcal{G} * \mathcal{H}, \varphi_\mathcal{G} * \varphi_\mathcal{H}) \longrightarrow 0$$

In other words,

$$\kappa(\rho * \rho') \simeq \kappa(\rho) \uparrow_{{}^n_r\psi} \oplus \kappa(\rho') \uparrow_{\psi^n_{r'}} .$$

Here of course $\mathfrak{J}_n(\mathcal{F}_n, \varphi_n) = M_n \simeq \Omega^2(\mathbf{F}_p)$ as an E_n-module.

The rest of the subsection is dedicated to the proof. We shall rely on material and notation from §3.3. Note that we shall identify $\mathcal{F}_r * \mathcal{F}_{r'}$ with $\mathcal{F}_n$; in fact, in this proof, we are going to assume that the generators for the group $\mathcal{F}_{r'}$, which appears as the source of the morphism ρ', are called $x_{r+1}, x_{r+2}, \dots, x_n$.

We have already pointed out that $\rho : \mathcal{F}_r \longrightarrow \mathcal{G}$ is surjective, as is $\rho' : \mathcal{F}_{r'} \longrightarrow \mathcal{H}$, and it follows that $\rho * \rho' : \mathcal{F}_n \longrightarrow \mathcal{G} * \mathcal{H}$ is also surjective. It is a general fact that the induced map $\Phi(\mathcal{F}_n) \longrightarrow \Phi(\mathcal{G} * \mathcal{H})$ must be surjective as well, and so there is an exact sequence of the form

$$0 \longrightarrow K \longrightarrow \mathfrak{J}_n(\mathcal{F}_n, \varphi_n) \longrightarrow \mathfrak{J}_n(\mathcal{G} * \mathcal{H}, \varphi_\mathcal{G} * \varphi_\mathcal{H}) \longrightarrow 0 .$$

Our task is to identify the kernel K. We start with a general lemma.

Lemma 5.2.8. *1. Let $\rho_1 : \mathcal{G}' \longrightarrow \mathcal{G}$ and $\rho_2 : \mathcal{H}' \longrightarrow \mathcal{H}$ be surjective morphisms between pro-p-groups. Then the kernel of $\rho_1 * \rho_2 : \mathcal{G}' * \mathcal{H}' \longrightarrow \mathcal{G} * \mathcal{H}$ is the closed, normal subgroup generated by $\ker(\rho_1)$ and $\ker(\rho_2)$.*

2. Let $\rho : \mathcal{G}' \longrightarrow \mathcal{G}$ be a surjective homomorphism between pro-p-groups, and assume that $\ker(\rho) \subset \Phi(\mathcal{G}')$. Let K denote the kernel of the induced map

$$\Phi(\mathcal{G}')/\Phi^{(2)}(\mathcal{G}') \longrightarrow \Phi(\mathcal{G})/\Phi^{(2)}(\mathcal{G}) .$$

Then K is the image of $\ker(\rho)$.

Proof. (1) We identify $\mathcal{G}$ with $\mathcal{G}'/\ker(\rho_1)$, and similarly we identify $\mathcal{H}$ with $\mathcal{H}'/\ker(\rho_2)$. Let N be the closed, normal subgroup generated by $\ker(\rho_1)$ and $\ker(\rho_2)$. It is clear that $N \subset \ker(\rho_1 * \rho_2)$, so that there is an induced map

$$(\mathcal{G}' * \mathcal{H}')/N \longrightarrow \mathcal{G} * \mathcal{H} \qquad (*)$$

and we wish to show that it is an isomorphism (it is obviously surjective). Consider then the composition of canonical maps

$$\mathcal{G}' \longrightarrow \mathcal{G}' * \mathcal{H}' \longrightarrow (\mathcal{G}' * \mathcal{H}')/N;$$

it must factor through $\mathcal{G}'/\ker(\rho_1) = \mathcal{G}$. Likewise, there is a map $\mathcal{H} \longrightarrow (\mathcal{G}' * \mathcal{H}')/N$.

We can combine these into a map

$$\mathcal{G} * \mathcal{H} \longrightarrow (\mathcal{G}' * \mathcal{H}')/N . \qquad (**)$$

(This uses that N is closed, so $(\mathcal{G}' * \mathcal{H}')/N$ is a pro-p-group, and we may use the universal property of free products.) Now it follows from the definitions that (*) and (**) are inverses to each other.

(2) Let $[x] \in K$, with $x \in \Phi(\mathcal{G}')$, so that $\rho(x) \in \Phi^{(2)}(\mathcal{G})$. The induced map $\Phi^{(2)}(\mathcal{G}') \longrightarrow \Phi^{(2)}(\mathcal{G})$ is surjective, so there is $c \in \Phi^{(2)}(\mathcal{G}')$ such that $xc \in \ker(\rho)$, and $[x] = [xc]$. □

Back to the situation at hand, part (1) of the lemma tells us that $\ker(\rho * \rho')$ is generated, as a closed, normal subgroup of $\mathcal{F}_n$, by $\ker(\rho)$ and $\ker(\rho')$. Combined with part (2) of the same lemma, this implies that K is generated, as an E_n-module, by $\kappa(\rho)$ and $\kappa(\rho')$.

More notation from §3.3 will be borrowed, in order to clarify things. We shall write $\Omega^2_n(\mathbf{F}_p)$ for the module $\mathfrak{J}_n(\mathcal{F}_n, \varphi_n) = M_n$, with its generators written $\zeta_1, \dots, \zeta_n$ and $\eta_i \smile \eta_j$ for $1 \leq i < j \leq n$; the module $\Omega^2_r(\mathbf{F}_p)$ is the sub-E_r-module of $\Omega^2_n(\mathbf{F}_p)$ generated by $\zeta_1, \dots, \zeta_r$ and $\eta_i \smile \eta_j$ for $1 \leq i < j \leq r$ (it is of course isomorphic to the $\mathbf{F}_p E_r$-module written simply $\Omega^2(\mathbf{F}_p)$ elsewhere in this thesis, but it is important to see it inside $\Omega^2_n(\mathbf{F}_p)$) ; and finally $\Omega^2_{r'}(\mathbf{F}_p)$ is the sub-$E_{r'}$-module of $\Omega^2(\mathbf{F}_p)$ generated by $\zeta_{r+1}, \dots, \zeta_n$ and $\eta_i \smile \eta_j$ for $r+1 \leq i < j \leq n$ (with similar comments).

By definition there are exact sequences

$$0 \longrightarrow \kappa(\rho) \longrightarrow \Omega^2_r(\mathbf{F}_p) \longrightarrow \mathfrak{J}_r(\mathcal{G}, \varphi_{\mathcal{G}}) \longrightarrow 0$$

and

$$0 \longrightarrow \kappa(\rho') \longrightarrow \Omega^2_{r'}(\mathbf{F}_p) \longrightarrow \mathfrak{J}_{r'}(\mathcal{H}, \varphi_{\mathcal{H}}) \longrightarrow 0\,.$$

Thus we see $\kappa(\rho)$ as a sub-E_r-module of $\Omega^2_n(\mathbf{F}_p)$, and the $\mathbf{F}_p E_n$-module generated by $\kappa(\rho)$ is the image of a morphism

$$\lambda\colon \kappa(\rho) \uparrow^n_{r\,\psi} \longrightarrow \Omega^2_n(\mathbf{F}_p)\,.$$

(One way to define λ is by Frobenius reciprocity from the inclusion $\kappa(\rho) \longrightarrow \Omega^2_n(\mathbf{F}_p) \downarrow_{E_r}$.) Moreover, this applies to $\Omega^2_r(\mathbf{F}_p)$ as well, and so for the same reason there is a morphism

$$\Omega^2_r(\mathbf{F}_p) \uparrow^n_{r\,\psi} \longrightarrow \Omega^2_n(\mathbf{F}_p)$$

whose image was studied in §3.3 and called N_1 there. Thus we see that the image of λ is contained in N_1.

Symmetrically, there is a map

$$\lambda'\colon \kappa(\rho') \uparrow_{\psi^n_{r'}} \longrightarrow \Omega^2_n(\mathbf{F}_p)$$

whose image is contained in the module N_2 studied earlier, which is itself the image of a homomorphism

$$\Omega^2_{r'}(\mathbf{F}_p) \uparrow_{\psi^n_{r'}} \longrightarrow \Omega^2_n(\mathbf{F}_p)\,.$$

Together, λ and λ' can be combined into a map

$$\kappa(\rho) \uparrow^n_{r\,\psi} \oplus \kappa(\rho') \uparrow_{\psi^n_{r'}} \longrightarrow \Omega^2_n(\mathbf{F}_p)$$

whose image, we have argued, is just K. We need to show that it is injective, and the proof will be complete.

However, we have $N_1 \cap N_2 = \{0\}$, which was Proposition 3.3.8. As a result, it suffices to show that λ and λ' are injective. We do this for λ' (by symmetry, this give the result for λ, even though the technical, intermediate results of §3.3 do not put r and r' in symmetrical positions!).

In fact, we now show that the map $\Omega^2_{r'}(\mathbf{F}_p) \uparrow_{\psi^n_{r'}} \longrightarrow N_2$ is an isomorphism. It will follow that, for any sub-$E_{r'}$-module $M \subset \Omega^2_{r'}(\mathbf{F}_p)$, the corresponding homomorphism $M \uparrow_{\psi^n_{r'}} \longrightarrow N_2$ is also injective. Thus the proposition will be proved at the same time as the next lemma.

Lemma 5.2.9. *We have* $\dim N_2 = \dim \Omega^2_{r'}(\mathbf{F}_p) \uparrow_{\psi^n_{r'}}$. *As a result, the surjective homomorphism* $\Omega^2_{r'}(\mathbf{F}_p) \uparrow_{\psi^n_{r'}} \longrightarrow N_2$ *is an isomorphism.*

Proof. The dimension of $\Omega^2_{r'}(\mathbf{F}_p)$ is $1 + (r'-1)p^{r'}$ by Lemma 3.2.3, so the dimension of the induced module $\Omega^2_{r'}(\mathbf{F}_p) \uparrow_{\psi^n_{r'}}$ is $p^r(1 + (r'-1)p^{r'})$, as the index of $E_{r'}$ in E_n is p^r.

Now, consider the basis of N_2 given in Lemma 3.3.6 (notice that the vectors listed in this lemma are obviously linearly independent, and by counting them as we are about to do, one obtains an alternative proof that they form a basis). There are, first and foremost, r' vectors called ζ_i for $r+1 \leq i \leq n$.

Next, we have a vector $(\eta_i \smile \eta_j) \cdot X^\nu$ for $r+1 \leq i < j \leq n$ whenever it belongs to the basis described in Proposition 3.2.12. Reasoning according as $\nu_j = p-1$ or not, we count

$$\sum_{i=r+1}^{n-1} \sum_{j=i+1}^{n} (p-1)(p^{i-1} + p^{j-1})$$

of these vectors. Let us rewrite this. First we turn our attention to

$$A = \sum_{i=r+1}^{n-1} \sum_{j=i+1}^{n} (p-1)p^{i-1} = (p-1) \sum_{i=r+1}^{n-1} (n-i)p^{i-1} = (p-1)(A_1 - A_2)\,,$$

where we have put

$$A_1 = n \sum_{i=r+1}^{n-1} p^{i-1} = n\,\frac{p^{n-1} - p^r}{p-1}\,,$$

and

$$A_2 = \sum_{i=r+1}^{n-1} ip^{i-1} = f'(p)\,,$$

using the polynomial

$$f = \sum_{i=r+1}^{n-1} X^i = \frac{X^n - X^{r+1}}{X-1}\,.$$

Write $(X-1)f = X^n - X^{r+1}$, differentiate with respect to X, evaluate at $X = p$ and rearrange terms to get

$$A_2 = \frac{1}{p-1}\left[np^{n-1} - (r+1)p^r - \frac{p^n - p^{r+1}}{p-1}\right].$$

In the end, we obtain

$$A = -(r'-1)p^r + \frac{p^n - p^{r+1}}{p-1}\,.$$

Next we rewrite

$$\begin{aligned} B &= \sum_{i=r+1}^{n-1} \sum_{j=i+1}^{n} (p-1)p^{j-1} \\ &= \sum_{i=r+1}^{n-1} (p^n - p^i) \\ &= (n-r)p^r - \sum_{i=r+1}^{n} p^i \\ &= r'p^n - \frac{p^{n+1} - p^{r+1}}{p-1}\,. \end{aligned}$$

In the end, there are $A + B$ vectors of the "second type".

We move to vectors of the "third type", still according to Lemma 3.3.6. There is one such vector $(\eta_i \smile \eta_j) \cdot X^\nu X_j^{p-1}$ for each choice of $1 \leq i \leq r$, $r+1 \leq j \leq n$, and of a multiindex ν with $\nu_k = 0$ for $i < k < j$ and $j < k$, and with $\nu_i \neq p-1$. The number of these vectors is thus

$$\sum_{i=1}^{r} \sum_{j=r+1}^{n} (p-1)p^{i-1} = (n-r)(p-1)\sum_{i=1}^{r} p^i = r'(p^r - 1)\,.$$

The grand total number of vectors which we have counted so far is

$$\begin{aligned} r' + A + B + r'(p^r - 1) &= p^r\left[r' + \frac{p^{r'} - p}{p-1} - (r'-1) + r'p^{r'} - \frac{p^{r'+1} - p}{p-1}\right] \\ &= p^r(1 + (r'-1)p^{r'})\,. \end{aligned}$$

This is also the dimension of the induced module $\Omega^2_{r'}(\mathbf{F}_p)\uparrow_{\psi^n_{r'}}$, as noted above, so the proof is complete. □

Remark. The hypothesis $\ker(\rho) \subset \Phi(\mathcal{F}_r)$, in the above proposition, has a simple interpretation. If $x_1, \dots, x_r$ are free generators for $\mathcal{F}_r$, then (given that ρ is surjective) the condition $\ker(\rho) \subset \Phi(\mathcal{F}_r)$ is equivalent to requiring that $\rho(x_1), \dots, \rho(x_r)$ be a *minimal* system of topological generators for $\mathcal{G}$ (that is, not proper subset generates $\mathcal{G}$ topologically). This is a consequence of Proposition 1.2.2.

5.3 A counterexample

Now we are equipped to consider our counterexample.

Proposition 5.3.1. *Let $\mathcal{G} = \mathcal{F}_r * \mathcal{D}_{k,r'}$ equipped with the obvious isomorphism $\varphi_{\mathcal{G}} \colon E_{r+r'} \longrightarrow \mathcal{G}/\Phi(\mathcal{G})$, with $r \geq 1$ and $r' > 2$. Put $n = r + r'$. Then $\mathfrak{J}_n(\mathcal{G}, \varphi_{\mathcal{G}})$ is not an E_n-module of constant Jordan type.*

Proof. Let $\pi \colon \mathcal{F}_{r'} \longrightarrow \mathcal{D}_{k,r'}$ the usual presentation of a Demuškin group (see §1.5). The group $\mathcal{G}$ has an obvious presentation

$$\mathcal{G} = \langle y_1, \dots, y_r,\, x_1, \dots, x_{r'} \mid x_1^{p^k}(x_1, x_2)(x_3, x_4)\dots(x_{r'-1}, x_{r'}) = 1 \rangle\,.$$

Note that this presentation is just $\mathrm{Id}_{\mathcal{F}_r} * \pi \colon \mathcal{F}_n \longrightarrow \mathcal{F}_r * \mathcal{D}_{k,r'}$, identifying $\mathcal{F}_n$ with $\mathcal{F}_r * \mathcal{F}_{r'}$. This defines $\varphi_{\mathcal{G}}$ in an obvious way, as mentioned in the proposition, so that $(\mathcal{G}, \varphi_{\mathcal{G}})$ is an object of $\mathfrak{pres}_n$, but we shall suppress it from the notation and write $\mathfrak{J}_n(\mathcal{G})$ for $\mathfrak{J}_n(\mathcal{G}, \varphi_{\mathcal{G}})$.

We have an exact sequence of $\mathbf{F}_p E_{r'}$-modules

$$0 \longrightarrow \Omega^{-1}(\mathbf{F}_p) \longrightarrow \Omega^2(\mathbf{F}_p) \xrightarrow{\mathfrak{J}_n(\pi)} \mathfrak{J}_{r'}(\mathcal{D}_{k,r'}) \longrightarrow 0\,;$$

this is the usual exact sequence from Proposition 2.1.4, with the notation from the current chapter employed (see also the remarks at the beginning of Chapter 4). Let us write $\Omega^{-1}_{r'}(\mathbf{F}_p)$ and $\Omega^2_{r'}(\mathbf{F}_p)$ for the first two modules in this exact sequence, in order to make it clear that they are $\mathbf{F}_p E_{r'}$-modules.

This means that $\kappa(\pi) = \Omega^{-1}_{r'}(\mathbf{F}_p)$. From Proposition 5.2.7, there is an exact sequence

$$0 \longrightarrow M \longrightarrow \Omega^2(\mathbf{F}_p) \xrightarrow{\mathfrak{J}_n(\mathrm{Id}_{\mathcal{F}_r} * \pi)} \mathfrak{J}_n(\mathcal{G}) \longrightarrow 0 \qquad (*)$$

where $M = \Omega^{-1}_{r'}(\mathbf{F}_p)\uparrow_{\psi^n_{r'}}$. Let us write M_1, resp. M_2, for the restriction of M to the subgroup E_r, resp. to the subgroup $E_{r'}$. Then it is clear that M_1 is isomorphic to d copies of $\mathbf{F}_p E_r$, where d is the dimension of $\Omega^{-1}_{r'}(\mathbf{F}_p)$, and in particular M_1 is free ; whereas the module M_2, as is equally clear, is isomorphic to p^r copies of $\Omega^{-1}_{r'}(\mathbf{F}_p)$.

In order to prove that $\mathfrak{J}_n(\mathcal{G})$ is not of constant Jordan type, we will compute the stable block decomposition of its restriction to two different π-points and observe that they are different. We will denote t a generator of E_1 and of course $T = t - 1 \in \mathbf{F}_p E_1$. The two π-points we have chosen are

$$\begin{array}{rccc} \beta_1 \colon & \mathbf{F}_p E_1 & \longrightarrow & \mathbf{F}_p E_n \\ & T & \longmapsto & Y_1 = y_1 - 1 \end{array}\,,$$

and

$$\begin{array}{rccc} \beta_2 \colon & \mathbf{F}_p E_1 & \longrightarrow & \mathbf{F}_p E_n \\ & T & \longmapsto & X_{r+1} = x_1 - 1 \end{array}\,.$$

We start with the stable block decomposition of $\beta_i^*(M)$, which is easy. Indeed, the descriptions we have given of M_1 and M_2 make it clear that the stable Jordan type of $\beta_1^*(M)$ is empty, since M_1 is free, and that of $\beta_2^*(M)$ is $[p-1]^{p^r}$, since the (constant) stable Jordan type of $\Omega^{-1}_{r'}(\mathbf{F}_p)$ is $[p-1]$ (see Example 1.1.9).

Now, since $\beta_1^*(M)$ is a projective module, the module $\beta_1^*(\mathfrak{J}_n(\mathcal{G}))$ is stably isomorphic to $\Omega^2(\mathbf{F}_p)$, hence its stable block decomposition is [1] ([Ben16, Proposition 5.4.3]). Now, if $\mathfrak{J}_n(\mathcal{G})$ were of constant Jordan type, then $\beta_2^*(\mathfrak{J}_n(\mathcal{G}))$ would also have this block decomposition. Let us assume so and find a contradiction.

Let us take a look at the following portion of the long exact sequence in cohomology associated with the restriction of (*) along β_2 :

$$\cdots \longrightarrow H^3(E_1, \beta_2^*(\mathfrak{J}_n(\mathcal{G}))) \longrightarrow H^4(E_1, \beta_2^*(M) \longrightarrow H^4(E_1, \beta_2^*(\Omega^2(\mathbf{F}_p))) \longrightarrow \cdots$$

Since the cohomology of a cyclic group is periodic [Bro94, Theorem 9.1] and according to Proposition 1.1.3 which links the block decomposition to the cohomology groups, we have that $H^4(E_1, \beta_2^*(\Omega^2(\mathbf{F}_p))) = \mathbf{F}_p$ and that $H^4(E_1, \beta_2^*(M)) = \mathbf{F}_p^{p^r}$. Furthermore, our assumption on the Jordan type of $\beta_2^*(\mathfrak{J}_n(\mathcal{G}))$ leads to $H^3(E_1, \beta_2^*(\mathfrak{J}_n(\mathcal{G}))) = \mathbf{F}_p$. Thus the exact sequence tells us that

$$\dim H^4(E_1, \beta_2^*(M)) = p^r \leq 2\,,$$

which is absurd given that $p \geq 3$ and $r \geq 1$. □

Chapter 6

Current investigations around κ

The criterion that we have established on the map κ (Proposition 2.2.10) is not so easy to check in the context of Galois extensions; furthermore it does not link the structure of the Galois module structure to the arithmetic of the field. Finally, we have not showed that the two cases, that we had to distinguish after Proposition 2.1.4, actually occur. We shall give here two concrete examples addressing the latter issue and which motivate the development of new results concerning elementary abelian p-extensions, which are currently under investigation.

Remember that p is an odd prime, $\mathbf{k}$ is a local field such that $\xi_p \in \mathbf{k}$, where ξ_p is a primitive p-th root of unity.

6.1 Some examples through computation

6.1.1 Setting

Here we shall exhibit two concrete extensions $\mathbf{K}_1/\mathbf{k}$ and $\mathbf{K}_2/\mathbf{k}$, such that

$$Gal(\mathbf{K}_1/\mathbf{k}) \simeq Gal(\mathbf{K}_2/\mathbf{k}) \simeq E_2\,,$$

and such that $J(\mathbf{K}_1)$ is stably isomorphic to $\Omega^2(\mathbf{F}_p) \oplus \Omega^{-2}(\mathbf{F}_p)$, whereas $J(\mathbf{K}_2)$ is not. For the sake of clarity, we set $p = 3$, but, for every (odd or even) prime p, other examples may be found without any difficulty, by mimicking the given ones.

Consider $\mathbf{k} = \mathbf{Q}_3(\xi_3)$: since the extension $\mathbf{Q}_3(\xi_3)/\mathbf{Q}_3$ is of degree 2, we have

$$\mathbf{k}^\times/\mathbf{k}^{\times 3} = \mathbf{F}_3^4\,,$$

according to [Gui18, Theorem 4.10]. Moreover, $\mathbf{Q}_3(\xi_3)$ does not contain any primitive 9-th root of unity – in fact $[\mathbf{Q}_p(\xi_{p^m}) : \mathbf{Q}_p] = p^{m-1}(p-1)$ by [Gui18, Proposition 2.48], so $\mathbf{Q}_3(\xi_3) \neq \mathbf{Q}_3(\xi_9)$. Hence the following isomorphism holds according to [Lab67, Theorem 7]:

$$\mathcal{G}_\mathbf{k}(3) \simeq Gal(\mathbf{k}(3)/\mathbf{k}) \simeq \mathcal{D}_{1,4} \simeq \langle x_1, x_2, x_3, x_4 | x_1^3(x_1, x_2)(x_3, x_4) = 1\rangle\,.$$

Notation 6.1.1. Now, set

$$\begin{cases} \mathcal{H}_1 &= \mathrm{Gr}(\Phi(\mathcal{D}_{1,4}), x_1, x_3) \\ \mathcal{H}_2 &= \mathrm{Gr}(\Phi(\mathcal{D}_{1,4}), x_1, x_2) \end{cases},$$

where $\mathrm{Gr}(\mathcal{S})$ denotes the closed normal subgroup generated by $\mathcal{S}$.

Let us then write $\mathbf{K}_i = \mathbf{k}(3)^{\mathcal{H}_i}$ for $i \in \{1, 2\}$.

As promised the Galois groups $Gal(\mathbf{K}_1/\mathbf{k})$ and $Gal(\mathbf{K}_2/\mathbf{k})$ are isomorphic. Indeed we have the following lemma:

Lemma 6.1.2. *For $i \in \{1, 2\}$, the following isomorphism holds*

$$Gal(\mathbf{K}_i/\mathbf{k}) \simeq \mathcal{G}_\mathbf{k}(3)/\mathcal{H}_i \simeq E_2\,.$$

Proof. Certainly $\mathcal{D}_{1,4}/\Phi(\mathcal{D}_{1,4})$ is elementary abelian, with a basis consisting of the classes of x_1, x_2, x_3, x_4. For $Gal(\mathbf{K}_1/\mathbf{k})$, we further kill the classes of x_1 and x_3, so this group is generated by the classes of x_2 and x_4. Similarly the group $Gal(\mathbf{K}_2/\mathbf{k})$ is generated by the classes of x_3 and x_4. □

According to Proposition 2.1.4, for $i \in \{1, 2\}$, there exists a short exact sequence

$$0 \longrightarrow \Omega^{-1}(\mathbf{F}_p) \xrightarrow{\kappa_i} \omega_2(\mathbf{F}_p) \longrightarrow J(\mathbf{K}_i) \longrightarrow 0 \ .$$

In order to establish the behaviour of κ_i, we shall in fact take a closer look at the module structure of $\omega_2(\mathbf{F}_p)$.

6.1.2 The module structure of $\omega_2(\mathbf{F}_p)$

Remember that, thanks to the presentation we use for a Demuškin group, there exists a canonical epimorphism

$$\pi \colon \mathcal{F}_4 = \langle \tilde{x}_1, \tilde{x}_2, \tilde{x}_3, \tilde{x}_4 \rangle \longrightarrow \mathcal{D}_{1,4}$$

sending $\tilde{x}_i$ to x_i.

Notation 6.1.3. We set $\tilde{\mathcal{H}}_i = \pi^{-1}(\mathcal{H}_i)$, for $i \in \{1, 2\}$.

Lemma 6.1.4. *The E_2-module $\tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1)$ (resp. $\tilde{\mathcal{H}}_2/\Phi(\tilde{\mathcal{H}}_2)$) is generated by the equivalence classes of the following elements:*

$$\tilde{x}_1, \tilde{x}_3, \tilde{x}_2^3, \tilde{x}_4^3, (\tilde{x}_2, \tilde{x}_4) \, ,$$

(resp. $\tilde{x}_1, \tilde{x}_2, \tilde{x}_3^3, \tilde{x}_4^3, (\tilde{x}_3, \tilde{x}_4)$).

Proof. Since, in $\mathcal{F}_4$, the elements $\tilde{x}_1, \tilde{x}_2, \tilde{x}_3$ and $\tilde{x}_4$ play a symmetric role, we shall only write an extensive proof for $\tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1)$.

Note that $\tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1)$ is generated, as a module, by a family of generators of $\tilde{\mathcal{H}}_1$ as a closed, normal subgroup. The latter, by definition, is generated by $\Phi(\mathcal{F}_4)$ together with $\tilde{x}_1$ and $\tilde{x}_3$. As a result, $\tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1)$ is generated by $\tilde{x}_1, \tilde{x}_3$ and the image of the natural map

$$M_4 = \Phi(\mathcal{F}_4)/\Phi^{(2)}(\mathcal{F}_4) \longrightarrow \tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1) \, .$$

Keep in mind that this is a map of $\mathcal{F}_4/\Phi(\mathcal{F}_4)$-modules, with $\mathcal{F}_4/\Phi(\mathcal{F}_4) \simeq E_4$, where the action on the target module factors through $\mathcal{F}_4/\tilde{\mathcal{H}}_1 \simeq E_2$.

Now in M_4, we have the generators $(\tilde{x}_i, \tilde{x}_j)$ (where $1 \leq i < j \leq 4$) and $\tilde{x}_i^3$ (with $1 \leq i \leq 4$), and we use the same names for their images in $\tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1)$. It is clear that $\tilde{x}_1^3$ and $\tilde{x}_3^3$ are redundant, as they now belong to $\Phi(\tilde{\mathcal{H}}_1)$.

Because $Gal(\mathbf{K}_1, \mathbf{k}) \simeq \langle \tilde{x}_3, \tilde{x}_4 \rangle$ acts on $\tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1)$, we have for instance

$$(\tilde{x}_1, \tilde{x}_4) = \tilde{x}_1^{-1}\tilde{x}_4^{-1}\tilde{x}_1\tilde{x}_4 = \tilde{x}_1^{-1}\tilde{x}_1^{\tilde{x}_4} \, .$$

This translates to

$$(\tilde{x}_1, \tilde{x}_4) \equiv -\tilde{x}_1 \cdot X_4 \mod \Phi(\tilde{\mathcal{H}}_1) \, .$$

Therefore we can get rid of $(\tilde{x}_1, \tilde{x}_4)$, and in a similar fashion any commutator implying $\tilde{x}_1$ or $\tilde{x}_3$. Note in fact that in $\tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1)$ the commutator $(\tilde{x}_1, \tilde{x}_3)$ is simply zero. We are left with the generators proposed in the lemma. □

As things become a little technical, we specialize the notation to $J(\mathbf{K}_1)$, even though the results may be, and will be, applied to $J(\mathbf{K}_2)$ after obvious changes in the indices (specifically, Corollary 6.1.8 below will be applied to $\tilde{\mathcal{H}}_2/\Phi(\tilde{\mathcal{H}}_2)$). The differences between the two will only appear in the next subsection.

Notation 6.1.5. Let $1 \leq i < j \leq 4$: the class of $(\tilde{x}_i, \tilde{x}_j)$ modulo $\Phi(\tilde{\mathcal{H}}_1)$ will be denoted (χ_i, χ_j), whereas χ_l^p denotes that of $\tilde{x}_l^p$ (for $1 \leq l \leq 4$). In the same fashion, we write χ_l for the class of $\tilde{x}_l$, for $l = 1, 3$.

Since the module $\tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1)$ contains a homomorphic image of M_4, the relations proven in Chapter 3 can be used. Which means that the following relations hold:

$$\left\{ \begin{array}{rcll} \chi_i^3 \cdot X_i & = & 0 & (i \in \{2,4\}) \\ \chi_2^3 \cdot X_4 + (\chi_2, \chi_4) \cdot X_2^2 & = & 0 & \\ \chi_4^3 \cdot X_2 - (\chi_2, \chi_4) \cdot X_4^2 & = & 0 & \end{array} \right. \tag{6.1}$$

Furthermore, according to (2.1),

$$\dim_{\mathbf{F}_p} \tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1) = 3^2 \cdot (4-1) + 1\,,$$

whereas $\dim \Omega^2(\mathbf{F}_p) = 3^2 + 1$, so that

$$\tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1) = \Omega^2(\mathbf{F}_3) \oplus (\mathbf{F}_3 E_2)^2\,. \tag{6.2}$$

We now aim to find some explicit generators of a free module of rank 2 in $\tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1)$: we claim that the generators χ_1 and χ_3 generate a free module of rank 2 over $\mathbf{F}_3 E_2$. In order to do so, we will need this lemma, which we may as well state for every prime p and every p group G:

Lemma 6.1.6. *Let M a finitely generated $\mathbf{F}_p G$-module, where G is a finite p-group. Remember that we have put*

$$\mathrm{N} = \sum_{g \in G} g\,.$$

Suppose that there exist some elements of M, called $\chi_1, \ldots, \chi_r$ such that the family $(\chi_i \cdot \mathrm{N})_{1 \leq i \leq r}$ is linearly independent. Then the $\mathbf{F}_p G$-module generated by the family $(\chi_i)_{1 \leq i \leq r}$ is free of rank r.

Proof. Let us prove this lemma by induction. When $r = 1$, the reader can refer to [Gui18, Lemma 1.31].

Now, suppose that the lemma holds for an $r \geq 1$ et let us prove it for $r+1$. We set

$$\left\{ \begin{array}{rcl} L_1 & = & \mathrm{Span}_{\mathbf{F}_p G}(\chi_1, \ldots, \chi_r) \\ L_2 & = & \mathrm{Span}_{\mathbf{F}_p G}(\chi_{r+1}) \end{array} \right. .$$

According to our hypothesis L_1 and L_2 are both free with respective rank r and 1. It remains to prove that

$$L_1 \cap L_2 = \{0\}\,.$$

Assume the converse. Therefore, there exists $x \in (L_1 \cap L_2)^G - \{0\}$, for G is a p-group and $\mathbf{F}_p$ is of characteristic p. Hence $x \in L_2^G$ and $x \in L_1^G$. Because L_1 and L_2 are free modules, we deduce that

$$\left\{ \begin{array}{rcll} x & = & \displaystyle\sum_{i=1}^{r} \chi_i a_i \cdot \mathrm{N} & (a_i \in \mathbf{F}_p) \\ x & = & \chi_{r+1} a_{r+1} \cdot \mathrm{N} & (a_{r+1} \in \mathbf{F}_p) \end{array} \right.$$

Hence we get

$$\sum_{i=1}^{r} \chi_i a_i \cdot \mathrm{N} - \chi_{r+1} a_{r+1} \cdot \mathrm{N} = 0\,,$$

which is absurd, since, by hypothesis, the family $(\chi_i \cdot \mathrm{N})_{1 \leq i \leq r+1}$ is linearly independent. □

Lemma 6.1.7. *The elements χ_1 and χ_3 generate a free module of rank 2 in $\tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1)$.*

Proof. As pointed out in (6.2), we have that

$$\tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1) = \Omega^2(\mathbf{F}_3) \oplus (\mathbf{F}_3 E_2)^2 \,.$$

Since there is no projective summand in $\Omega^2(\mathbf{F}_3)$ according to the first remark after 3.1.2, the last lemma for $r = 1$ shows that $\Omega^2(\mathbf{F}_3) \cdot \mathrm{N} = 0$, and thus

$$\dim_{\mathbf{F}_3} \tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1) \cdot \mathrm{N} = 2 \,.$$

It follows that

$$\dim_{\mathbf{F}_3} \mathrm{Span}_{\mathbf{F}_3}((\chi_2, \chi_4) \cdot \mathrm{N},\, \chi_2^3 \cdot \mathrm{N},\, \chi_4^3 \cdot \mathrm{N},\, \chi_1 \cdot \mathrm{N},\, \chi_3 \cdot \mathrm{N}) = 2 \,.$$

Since $\mathrm{N} = X_2^2 X_4^2$, according to the relations recalled in (6.1) we have

$$(\chi_2, \chi_4) \cdot \mathrm{N} = \chi_4^3 \cdot X_2 X_2^2 = 0 \,,$$

as well as:

$$\chi_2^3 \cdot \mathrm{N} = 0 = \chi_4^3 \cdot \mathrm{N} \,.$$

Hence, we have the following equality

$$\mathrm{Span}_{\mathbf{F}_3}((\chi_2, \chi_4) \cdot \mathrm{N},\, \chi_2^3 \cdot \mathrm{N},\, \chi_4^3 \cdot \mathrm{N},\, \chi_1 \cdot \mathrm{N},\, \chi_3\, \mathrm{N}) = \mathrm{Span}_{\mathbf{F}_3}(\chi_1 \cdot \mathrm{N}, \chi_3 \cdot \mathrm{N}) \,,$$

hence the vectors $\chi_1 \cdot \mathrm{N}$ and $\chi_3 \cdot \mathrm{N}$ are linearly independent. Therefore, according to Lemma 6.1.6, we may conclude. □

Corollary 6.1.8. *Let W denote the quotient of $\tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1)$ obtained by factoring out the submodule generated by χ_1 and χ_3. Then the quotient map $\tilde{\mathcal{H}}_1/\Phi(\tilde{\mathcal{H}}_1) \longrightarrow W$ is a stable isomorphism, and W is isomorphic to the minimal model $\Omega^2(\mathbf{F}_p)$. More precisely, there is an isomorphism from M_2 to W mapping χ_1^3, χ_2^3 and (χ_1, χ_2) to the classes of χ_2^3, χ_4^3 and (χ_2, χ_4) respectively.*

Proof. The first two statements are direct consequences of the lemma. Now let V denote the submodule of $\Phi(\mathcal{F}_4)/\Phi^{(2)}(\mathcal{F}_4)$ generated by $\tilde{x}_2^3, \tilde{x}_4^3$, and $(\tilde{x}_2, \tilde{x}_4)$. Then V and W are both isomorphic to $\Omega^2(\mathbf{F}_p)$, and for V, there is a specific isomorphism $M_2 \longrightarrow V$ taking χ_1^3, χ_2^3 and (χ_1, χ_2) to $\tilde{x}_2^3, \tilde{x}_4^3$, and $(\tilde{x}_2, \tilde{x}_4)$ respectively. Moreover, the induced map $V \longrightarrow W$ is obviously surjective, so it is an isomorphism. □

This is all we are going to need to elucidate the structure of $J(\mathbf{K}_1)$. As for $J(\mathbf{K}_2)$, we will require the following lemma, which we establish for every prime p and every n.

Lemma 6.1.9. *Let $n \in \mathbf{N} - \{0\}$. The homomorphisms of $\mathbf{F}_p E_n$-modules given by*

$$\begin{array}{rccc} \zeta_i^\wedge : & \Omega^{-1}(\mathbf{F}_p) = \langle \alpha | \alpha \cdot \mathrm{N} = 0 \rangle & \longrightarrow & M_n \simeq \Omega^2(\mathbf{F}_p) \\ & \alpha & \longmapsto & \zeta_i \end{array} \,,$$

for $i \in \{1, \ldots, n\}$, together with

$$\begin{array}{rccc} (\eta_i \smile \eta_j)^\wedge : & \Omega^{-1}(\mathbf{F}_p) = \langle \alpha | \alpha \cdot \mathrm{N} = 0 \rangle & \longrightarrow & M_n \simeq \Omega^2(\mathbf{F}_p) \\ & \alpha & \longmapsto & \eta_i \smile \eta_j \end{array} \,,$$

for $1 \leq i < j \leq n$, form a basis of $\underline{\hom}(\Omega^{-1}(\mathbf{F}_p), \Omega^2(\mathbf{F}_p))$.

Recall that $\underline{\hom}$ refers to the group of stable maps between the given $\mathbf{F}_p E_n$-modules, and that

$$\underline{\hom}(\Omega^{-1}(\mathbf{F}_p), \Omega^2(\mathbf{F}_p)) \cong \underline{\hom}(\Omega^{-3}(\mathbf{F}_p), \mathbf{F}_p) \cong H_2(E_n, \mathbf{F}_p) \cong H^2(E_n, \mathbf{F}_p) \,.$$

Proof. First, note that those maps are well-defined, since $\zeta_i^\wedge(\alpha)\cdot \mathrm{N} = 0$, because $\zeta_i^p \cdot X_i = 0$ according to Equation (3.12) and $(\eta_i \smile \eta_j)^\wedge(\alpha)\cdot \mathrm{N} = 0$, because $\eta_i \smile \eta_j \cdot X_i^{p-1}X_j^{p-1} = 0$ according to Equation (3.18).

Furthermore, those maps are linearly independent in $\underline{\hom}_{\mathbf{F}_p E_n}(\Omega^{-1}(\mathbf{F}_p), \Omega^2(\mathbf{F}_p))$. Indeed suppose that there exists a linear combination of the form

$$\psi = \sum_{i=1}^{n} \mu_i \zeta_i^\wedge + \sum_{1\leq i<j\leq n} \mu_{i,j}(\eta_i \smile \eta_j)^\wedge \tag{6.3}$$

which factors through a projective module, which means there exist morphisms f and g and a projective module P such that the following diagram is commutative

$$\begin{array}{ccc} \Omega^{-1}(\mathbf{F}_p) & \xrightarrow{\quad\psi\quad} & M_n \\ & {\scriptstyle f}\searrow \quad \nearrow{\scriptstyle g} & \\ & P & \end{array}$$

Since $\alpha\cdot\mathrm{N} = 0$, we know that $\mathrm{Im}(f) \subset \mathrm{Rad}(P)$, therefore $\mathrm{Im}(g\circ f) \subset \mathrm{Rad}(\Omega^2(\mathbf{F}_p))$. However,

$$\psi(\alpha) = \sum_{i=1}^{n} \mu_i \zeta_i + \sum_{1\leq i<j\leq n} \mu_{i,j}(\eta_i \smile \eta_j)\,,$$

and the right-hand-side is a linear combination of elements form our favourite basis for $M_n = \Omega^2(\mathbf{F}_p)$. Moreover, this linear combination can only lie in the radical when it is zero, as follows from the observations in the proof of Proposition 4.2.3. We conclude that the coefficients μ_i and $\mu_{i,j}$ are all zero.

Hence the maps $\zeta_i^\wedge$ and $(\eta_i \smile \eta_j)^\wedge$ are indeed linearly independent in $\underline{\hom}_{\mathbf{F}_p E_n}(\Omega^{-1}(\mathbf{F}_p), M_n)$; since we have the equalities

$$\dim_{\mathbf{F}_p} \underline{\hom}_{\mathbf{F}_p E_n}(\Omega^{-1}(\mathbf{F}_p), M_n) = \dim_{\mathbf{F}_p} H^2(E_n, \mathbf{F}_p) = n + \binom{n}{2}\,,$$

this family is a basis of $\underline{\hom}_{\mathbf{F}_p E_n}(\Omega^{-1}(\mathbf{F}_p), M_n)$. □

6.1.3 The image of κ

Now we are ready to draw the conclusion that we have announced:

Proposition 6.1.10. *The map κ_1 is stably zero, whereas the map κ_2 is not.*

Proof. The map κ_i sends the generator α of $\Omega^{-1}(\mathbf{F}_3)$ to the class of

$$\delta = \tilde{x}_1^3(\tilde{x}_1, \tilde{x}_2)(\tilde{x}_3, \tilde{x}_4) \in \mathcal{F}_4$$

in $\tilde{\mathcal{H}}_i/\Phi(\tilde{\mathcal{H}}_i)$. Let $[\delta]_i$ denote the class of δ modulo $\Phi(\tilde{\mathcal{H}}_i)$ for $i \in \{1,2\}$. On the one hand we have

$$\begin{array}{rcl} [\delta]_1 & = & [\tilde{x}_1^3(\tilde{x}_1, \tilde{x}_2)(\tilde{x}_3, \tilde{x}_4)] \\ & = & -\chi_1 \cdot X_2 - \chi_3 \cdot X_4 \end{array}\,,$$

whereas on the other hand, we have

$$[\delta]_2 = [(\tilde{x}_3, \tilde{x}_4)]\,.$$

Therefore according to Lemma 6.1.7, the image of κ_1 lies in a projective submodule, hence it is stably zero.

We turn to κ_2. Here we will require Corollary 6.1.8, applied to $\tilde{\mathcal{H}}_2/\Phi(\tilde{\mathcal{H}}_2)$. Accordingly, we have a stable isomorphism $\theta\colon \tilde{\mathcal{H}}_2/\Phi(\tilde{\mathcal{H}}_2) \longrightarrow W$, and an isomorphism $M_2 \longrightarrow W$ mapping χ_1^3, χ_2^3 and (χ_1, χ_2) to $\theta(\tilde{x}_3^3), \theta(\tilde{x}_4^3)$ and $\theta((\tilde{x}_3, \tilde{x}_4))$ respectively. It is enough to show that $\theta \circ \kappa_2$ is non-zero ; however, under the identification between W and M_2, the map $\theta \circ \kappa_2$ is none other than $(\eta_1 \smile \eta_2)^\wedge$. According to Lemma 6.1.9, the latter is non-zero. □

Corollary 6.1.11. *The E_2-module $J(\mathbf{K}_1)$ is stably isomorphic to $\Omega^2(\mathbf{F}_3) \oplus \Omega^{-2}(\mathbf{F}_3)$, whereas $J(\mathbf{K}_2)$ is not.*

6.2 Current studies

As examplified in the previous computations, our goal is mainly to know how to write $\kappa(\alpha)$ in $\omega_2(\mathbf{F}_p)$. We have succeeded because we have chosen some very particular extensions which behave nicely with the choices of generators given by Labute (in fact, we have started from Labute's presentation, and chosen the extensions afterwards!). But in a more generic situation, we shall need the help of the following theorem, which can be proved by using the same techniques as the ones in [Lab67]. This is work under progress, so we do not provide a proof.

Theorem 6.2.1. *Let $\tau_1, \dots, \tau_n$ be a symplectic basis of $(H^1(\mathcal{D}_{k,n}, \mathbf{F}_p), \smile)$. Then there exist $t_1, \dots, t_n$, which are lifts in $\mathcal{D}_{k,n}$ of the predual basis of $\tau_1, \dots, \tau_n$, and integers $a_1, \dots, a_n$ in $\{0, \dots, k-1\}$ such that*

$$\mathcal{D}_{k,n} = \langle t_1, \dots, t_n \mid (t_1^{a_1} \dots t_n^{a_n})^{p^k} (t_1, t_2)(t_3, t_4) \dots (t_{n-1}, t_n) = 1 \rangle . \qquad \square$$

This helps us work with more general generators than merely those provided by the initial presentation.

Now a recollection, as cup-products seem to be of some importance: remember that we have $H^1(\mathcal{D}_{k,n}, \mathbf{F}_p) \simeq \mathbf{k}^\times / \mathbf{k}^{\times p}$ and that the cup-product has a nice interpretation in Galois theory thanks to Hilbert's symbol:

Proposition 6.2.2. *Let $\mathbf{k}$ be a field such that $\xi_p \in \mathbf{k}^\times$. Let $a, b \in \mathbf{k}^\times$. Let $\sqrt[p]{a}$ and $\sqrt[p]{b}$ denote the classes of a and b in $\mathbf{k}^\times / \mathbf{k}^{\times p}$. Then the cup product $\sqrt[p]{a} \smile \sqrt[p]{b}$ is zero if and only if b is a norm from $\mathbf{k}(\sqrt[p]{a})/\mathbf{k}$.*

As the reader might have guessed, the term $(t_1^{a_1} \dots t_n^{a_n})^{p^k}$ above might cause some issues, as soon as $k = 1$; that is why, in order to avoid this difficulty, we shall suppose that $k \geq 2$, which translates into $\xi_{p^2} \in \mathbf{k}$, in order to express our next result in a clean-cut way:

Theorem 6.2.3. *Let $\mathbf{K} = \mathbf{k}(\sqrt[p]{a_1}, \dots, \sqrt[p]{a_r})$ be an elementary abelian extension of a local field $\mathbf{k}$ such that $\xi_{p^2} \in \mathbf{k}^\times$. Then $J(\mathbf{K})$ is stably isomorphic to $\Omega^2(\mathbf{F}_p) \oplus \Omega^{-2}(\mathbf{F}_p)$ if and only if for every i, j such that $1 \leq i < j \leq r$ the elements a_j is a norm from $\mathbf{k}(\sqrt[p]{a_i})/\mathbf{k}$.* $\square$

Again, this is work in progress.

Notation

In the text we have put:

- p for a prime number.
- C_p for the cyclic group of order p.
- $E_r = C_p^r$ for the elementary abelian p-group of rank r.
- $\mathbf{F}$ for a field of characteristic p.
- $\mathbf{F}_p$ for the finite field with p-elements.
- $n_j(M)$ for the number of block of length j in the decomposition in irreducible modules of M, if M is an $\bar{F}E_1$-module.
- $\mathfrak{mod}(R)$ for the category of finitely generated R-modules.
- $\underline{\mathfrak{mod}}(\mathbf{F}G)$ the category of stable $\mathbf{F}G$-modules, endowed with the Heller shift functor Ω.
- $\omega(M)$ for a module stably isomorphic to the Heller shift $\Omega(M)$.
- N for the norm, which means $\mathrm{N} = \sum_{g \in G} g$.
- ξ_s for a primitive s-root unity.
- $\mathbf{k}$ for a field. From Chapter 2, it is a local field.
- $\mathbf{k}(p)$ for a maximal pro-p-extension of $\mathbf{k}$.
- $\mathcal{G}_{\mathbf{k}}(p) = Gal(\mathbf{k}(p)/\mathbf{k})$.
- $\mathcal{F}_r$ for the free pro-p-group on r-integers.
- $\mathcal{D}_{k,2s}$ for the Demuškin group, which means, when $p \neq 2$

$$\mathcal{D}_{k,2s} = \langle x_1, \ldots, x_{2s} | x_1^{p^k}(x_1, x_2)(x_3, x_4) \ldots (x_{2s-1}, x_{2s}) = 1 \rangle .$$

- δ for the Demuškin relation

$$x_1^{p^k}(x_1, x_2)(x_3, x_4) \ldots (x_{2s-1}, x_{2s})$$

- $\Phi(\mathcal{G})$ for the Frattini subgroup of $\mathcal{G}$ a pro-p-group, and $\Phi^{(i)}(\mathcal{G}) = \Phi(\Phi^{(i-1)}(\mathcal{G}))$
- n and k for two integers, such that in Chapters 2, 4, $\mathcal{G}_{\mathbf{k}}(p) = \mathcal{D}_{k,n}$.
- G for a finite p-group.
- δ_i for the following function:

$$\begin{array}{rccc} \delta_i : & \mathbf{Z}^n & \longrightarrow & \mathbf{Z}^n \\ & (\nu_1, \ldots, \nu_n) & \longmapsto & (\nu_1, \ldots, \nu_i - 1, \ldots, \nu_n) \end{array} .$$

- γ_i for the following function:

$$\begin{array}{rccc} \gamma_i : & \mathbf{Z}^n & \longrightarrow & \mathbf{Z}^n \\ & (\nu_1, \ldots, \nu_n) & \longmapsto & (\nu_1, \ldots, \nu_i + 1, \ldots, \nu_n) \end{array} .$$

- $l(M)$ for the length of the module M.
- cd_p for the p-cohomological dimension.

Bibliography

[AGKM01] Alejandro Adem, Wenfeng Gao, Dikran B. Karagueuzian, and Ján Mináč. Field theory and the cohomology of some Galois groups. *J. Algebra*, 235(2):608–635, 2001.

[BC92] D. J. Benson and Jon F. Carlson. Products in negative cohomology. *J. Pure Appl. Algebra*, 82(2):107–129, 1992.

[Ben91] D. J. Benson. *Representations and cohomology. I*, volume 30 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1991. Basic representation theory of finite groups and associative algebras.

[Ben16] David J. Benson. *Representations of Elementary Abelian p-Groups and Vector Bundles*. Cambridge Tracts in Mathematics. Cambridge University Press, 2016.

[Bla69] Norman Blackburn. Note on a theorem of Magnus. *J. Austral. Math. Soc.*, 10:469–474, 1969.

[Bor65a] Z. I. Borevič. The multiplicative group of cyclic p-extensions of a local field. *Trudy Mat. Inst. Steklov*, 80:16–29, 1965.

[Bor65b] Z. I. Borevič. On the group of principal units of a normal p-extension of a regular local field. *Trudy Mat. Inst. Steklov*, 80:30–44, 1965.

[Bro94] Kenneth S. Brown. *Cohomology of groups*, volume 87 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. Corrected reprint of the 1982 original.

[Car83] Jon F. Carlson. The varieties and the cohomology ring of a module. *J. Algebra*, 85(1):104–143, 1983.

[Car96] Jon F. Carlson. *Modules and group algebras*. Lectures in Mathematics ETH Zürich. Birkhäuser Verlag, Basel, 1996. Notes by Ruedi Suter.

[CFP08] Jon F. Carlson, Eric M. Friedlander, and Julia Pevtsova. Modules of constant Jordan type. *J. Reine Angew. Math.*, 614:191–234, 2008.

[Con] Keith Conrad. History of class field theory.

[CTVEZ03] Jon F. Carlson, Lisa Townsley, Luis Valero-Elizondo, and Mucheng Zhang. *Cohomology rings of finite groups*, volume 3 of *Algebra and Applications*. Kluwer Academic Publishers, Dordrecht, 2003. With an appendix: Calculations of cohomology rings of groups of order dividing 64 by Carlson, Valero-Elizondo and Zhang.

[DDSMS99] J. D. Dixon, M. P. F. Du Sautoy, A. Mann, and D. Segal. *Analytic Pro-P Groups*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2 edition, 1999.

[Duf81] J. Duflot. Depth and equivariant cohomology. *Comment. Math. Helv.*, 56(4):627–637, 1981.

[EH94] Ido Efrat and Dan Haran. On Galois groups over Pythagorean and semi-real closed fields. *Israel J. Math.*, 85(1-3):57–78, 1994.

[EH01] David Eisenbud and Joe Harris. *The Geometry of Schemes*. Springer Verlag, 2001.

[Fad60] D. K. Faddeev. On the structure of the reduced multiplicative group of a cyclic extension of a local field. *Izv. Akad. Nauk SSSR Ser. Mat.*, 24:145–152, 1960.

[Fox53] Ralph H. Fox. Free differential calculus. I. Derivation in the free group ring. *Ann. of Math. (2)*, 57:547–560, 1953.

[FP11] Eric M. Friedlander and Julia Pevtsova. Constructions for infinitesimal group schemes. *Trans. Amer. Math. Soc.*, 363(11):6007–6061, 2011.

[Fri95] Michael D. Fried. Introduction to modular towers: generalizing dihedral group–modular curve connections, 1995.

[Gas54] W. Gasschütz. Über modulare darstellungen endlicher gruppen, die von freien gruppen induziert werden. *Mathematische Zeitschrift*, 60:274–286, 1954.

[Gui18] Pierre Guillot. *A Gentle Course in Local Class Field Theory: Local Number Fields, Brauer Groups, Galois Cohomology*. Cambridge University Press, 2018.

[Has67] Helmut Hasse. History of class field theory. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 266–279. Thompson, Washington, D.C., 1967.

[HJ10] Thorsten Holm and Peter Jørgensen. *Triangulated categories: definitions, properties, and examples*, page 1–51. London Mathematical Society Lecture Note Series. Cambridge University Press, 2010.

[Koc02] Helmut Koch. *Galois theory of p-extensions*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002. With a foreword by I. R. Shafarevich, Translated from the 1970 German original by Franz Lemmermeyer, With a postscript by the author and Lemmermeyer.

[Lab67] John P. Labute. Classification of Demushkin groups. *Canadian Journal of Mathematics*, 19:106–132, 1967.

[Laz54] Michel Lazard. Sur les groupes nilpotents et les anneaux de lie. *Annales scientifiques de l'École Normale Supérieure*, 3e série, 71(2):101–190, 1954.

[LMSS10] N. Lemire, J. Mináč, A. Schultz, and J. Swallow. Galois module structure of Galois cohomology for embeddable cyclic extensions of degree p^n. *J. Lond. Math. Soc. (2)*, 81(3):525–543, 2010.

[Mag39] Wilhelm Magnus. On a Theorem for Marshall Hall. *Annals of Mathematics*, 40(4):764–768, 1939.

[MS03] Ján Mináč and John Swallow. Galois module structure of pth-power classes of extensions of degree p. *Israel J. Math.*, 138:29–42, 2003.

[MST14] Ján Mináč, John Swallow, and Adam Topaz. Galois module structure of (ℓ^n)th classes of fields. *Bull. Lond. Math. Soc.*, 46(1):143–154, 2014.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. Grundlehren der mathematischen Wissenschaften. Springer-Verlag Berlin Heidelberg, 2008.

[QW21] Claudio Quadrelli and Thomas S. Weigel. Oriented pro-ℓ groups with the Bogomolov property, 2021.

[Ser94] Jean-Pierre Serre. *Cohomologie galoisienne*, volume 5 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, fifth edition, 1994.

[Web16] Peter Webb. *A Course in Finite Group Representation Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2016.

[Wym72] B. F. Wyman. What is a reciprocity law? *Amer. Math. Monthly*, 79:571–586; correction, ibid. 80 (1973), 281, 1972.

Soient p un nombre premier et $\mathbf{k}$ un corps local contenant une racine primitive p-ième de l'unité notée ξ_p. Donnons-nous alors $\mathbf{K}/\mathbf{k}$ une p-extension galoisienne finie de groupe de Galois G. Notre objectif premier est d'étudier la structure de G-module de $J(\mathbf{K}) = \mathbf{K}^\times/\mathbf{K}^{\times p}$. Pour ce faire, nous utilisons les outils donnés par la théorie des modules de type de Jordan constant mais nous calculons aussi les groupes de cohomologie avec des coefficients dans $J(\mathbf{K})$, sous certaines hypothèses.

De surcroît, lorsque $\mathbf{K}/\mathbf{k}$ est l'extension p-élémentaire abélienne maximale, nous tirons profit de notre étude pour calculer quelques invariants pertinents précédemment introduits pour $p = 2$.

Let p be a prime number and $\mathbf{k}$ a local field such that $\mathbf{k}$ contains a primitive p-th root of unity denoted ξ_p. Set $\mathbf{K}/\mathbf{k}$ a finite Galois p-extension. Let G denote its Galois group. Our main goal is to study the G-module structure of $J(\mathbf{K}) = \mathbf{K}^\times/\mathbf{K}^{\times p}$. To do so, we use the theory of modules of constant Jordan type and we also compute the cohomology groups of G with coefficients in $J(\mathbf{K})$ under some hypothesis.

Furthermore, when $\mathbf{K}/\mathbf{k}$ is the maximal p-elementary abelian extension, we take profit of our study in order to compute some invariants which were previously introduced for $p = 2$.

INSTITUT DE RECHERCHE MATHÉMATIQUE AVANCÉE
UMR 7501
Université de Strasbourg
CNRS
IRMA, UMR 7501
7 rue René Descartes
F-67000 STRASBOURG

Tél. 03 68 85 01 29

irma.math.unistra.fr
irma@math.unistra.fr

IRMA 2021/008
http://tel.archives-ouvertes.fr/tel-03418647