Le problème de Noether pour les groupes abéliens

Diego IZQUIERDO & Yichao HUANG
Sous la direction d'Olivier WITTENBERG

2011

Table des matières

1 Introduction: le problème de Noether et la preuve de Fischer

Soit k_0 un corps et soit $K_0 = k_0(X_1, ..., X_n)$ le corps des fractions rationnelles à n indéterminées. Soit G un sous-groupe du groupe symétrique $\mathcal{S}_n$. Faisons agir G sur K_0 par permutation des variables. L'extension $K_0^G|k_0$ est-elle transcendante pure?

Ce problème, dit "de Noether" même si Emmy Noether n'avait jamais conjecturé que la réponse serait affirmative, est apparu vers la fin du XIXème siècle. Il a attiré l'attention de nombreux mathématiciens, et est toujours un sujet de recherche. Le cas où $G = \mathcal{S}_n$ est un résultat classique: dans ce cas, K_0^G est engendré par les polynômes symétriques à n variables sur k_0, famille qui est bien algébriquement indépendante.

Le premier résultat général a été démontré par Fischer, en 1915, dans [Fis15]: il montre que le problème de Noether admet une réponse affirmative lorsque G est abélien, k_0 contient toutes les racines e-ièmes de l'unité où e est l'exposant de G et $car(k_0)$ ne divise pas e. À partir de là, tout le long de la deuxième moitié du XXème siècle, des articles sont parus donnant des réponses affirmatives au problème dans des cas particuliers. Ainsi, en 1955, Kuniyoshi prouve dans [Kun56] que si k_0 est de caractéristique $p > 0$ et si G est un p-groupe, alors K_0^G est bien une extension transcendante pure de k_0. En 1964, dans [Mat64], Matsuda améliore le résultat de Fisher dans le cas où G est cyclique. Parallèlement à ces études générales, Masuda a étudié le problème pour de petites valeurs de n. C'est ainsi qu'il montre en 1955 dans [Mas55] que lorsque $n \leq 7$, $car(k_0)$ ne divise pas n et G est cyclique d'ordre n, $K_0^G|k_0$ est transcendante pure. Il arrive ensuite à la même conclusion lorsque $n = 11$, $car(k_0) \neq 11$ et G est cyclique d'ordre n: la preuve se trouve dans [Mas68].

Cependant, dans certains cas, l'extension $K_0^G|k_0$ n'est pas transcendante pure. Jusqu'à la fin des années 1960, les mathématiciens conjecturent que le problème de Noether admet toujours une réponse affirmative. Si cette conjecture était vraie, elle permettrait de montrer à l'aide du théorème d'irréductibilité de Hilbert que lorsque k est un corps de nombres, tout groupe fini est le groupe de Galois d'une extension galoisienne de k. Mais en 1969, Swan publie l'article [Swa69] dans lequel il prouve que lorsque G est cyclique d'ordre n, $k_0 = \mathbb{Q}$ et n vaut 47, 113 ou 233, alors l'extension $K_0^G|k_0$ n'est pas transcendante pure. Un peu plus tard, en 1973, Endo et Miyata améliorent ces résultats dans [EM73] en arrivant à la même conclusion que Swan dans le cas où G est cyclique d'ordre 8, 121, 169...

Finalement, en 1974, Lenstra publie l'article [Len74] dans lequel il donne une condition nécessaire et suffisante pour que l'extension $K_0^G|k_0$ soit transcendante pure dans le cas où G est abélien fini et agit transitivement sur les n variables. Ce

résultat constitue un avancement majeur dans l'étude du problème de Noether. Cependant, encore de nos jours, le problème reste ouvert: dans le cas où le groupe G ne serait pas abélien, très peu de résultats sont connus, mais même dans des cas qui peuvent paraître simples, comme le cas où $G = \mathbb{Z}/53\mathbb{Z}$ et $k_0 = \mathbb{Q}$, le problème n'est pas résolu.
L'objet de ce mémoire est d'étudier le problème de Noether dans le cas d'un groupe abélien. Nous allons d'abord rappeler les résultats classiques d'algèbre et de théorie des nombres dont nous aurons besoin (partie 2). Nous supposons cependant connues la théorie de Galois, les représentations linéaires des groupes finis, ainsi que des notions d'algèbre commutative et d'algèbre multilinéaire. Dans la partie 4.5, nous ferons aussi appel à quelques notions rudimentaires de géométrie algébrique. Ensuite, nous détaillerons le raisonnement de Swan pour prouver que dans le cas où $G = \mathbb{Z}/47\mathbb{Z}$, le problème a une réponse négative (partie 3). Puis nous montrerons le théorème de Lenstra (partie 4) dont nous donnerons un certain nombre de conséquences (partie 5).
Avant de commencer notre étude, nous voudrions remercier chaleureusement Olivier Wittenberg pour son soutien constant, sa disponibilité, l'aide précieuse qu'il a apportée au cours du travail et pour nous avoir fait découvrir ce problème passionnant.

Commençons par le théorème de Fischer qui donne une réponse affirmative au problème de Noether dans un cas très particulier.

Théorème 1.0.1. ***Théorème de Fischer***
Soient G un groupe abélien fini d'exposant e et V une représentation de dimension finie sur un corps k_0. Si le corps k_0 contient toutes les racines e-ièmes de l'unité et si la caractéristique de k_0 ne divise pas e, alors $k_0(V)^G/k_0$ est une extension transcendante pure, où $k_0(V)^G$ désigne le sous-corps fixe du corps des fractions de l'algèbre symétrique de V sur k_0.

Preuve. Comme G est abélien fini et le corps contient les racines e-ièmes de l'unité, la représentation V s'écrit comme somme directe de représentations de dimension 1. Prenons $(y_1, \dots, y_n)$ une base adaptée à cette décomposition.
Comme V est engendré par la famille des $(y_i)_i$ en tant qu'espace vectoriel, un quotient dans le corps des fractions de l'algèbre symétrique de V s'écrit comme un élément dans $k_0(y_1, \dots, y_n)$. La famille $(y_i)_i$ est algébriquement indépendante, donc le sous-groupe multiplicatif Y engendré par $(y_1, \dots, y_n)$ du groupe $k_0(V)^*$ est abélien libre de base $(y_1, \dots, y_n)$.
Considérons maintenant le morphisme de groupes Φ de Y dans $X = Hom(G, k_0^*)$ qui à chaque y_i associe le caractère de la représentation restreinte à la droite y_i. On affirme que si $I = Ker\Phi$, alors $k_0(V)^G$ s'identifie à $k_0(I)$. En effet, $k_0[I] = k_0[Y]^G$, et $k_0(I)^G$ est le corps des fractions de $k_0[I]^G$. Le groupe I étant un sous-groupe

de Y, qui est libre de type fini sur $\mathbb{Z}$, il est abélien libre de type fini, et donc $k_0(I) = k_0(V)^G$ est une extension transcendante pure de k_0. □

Si dans le théorème précédent on choisit comme représentation V l'espace vectoriel de base X_i, G agissant par permutation, on obtient exactement que le problème de Noether tel qu'il a été énoncé au début de cette partie admet une réponse affirmative lorsque G est abélien fini d'exposant e, $car(k_0)$ ne divise pas e et k_0 contient toutes les racines e-ièmes de l'unité.
La démonstration de Fischer met en évidence une méthode naturelle et directe de montrer qu'une extension est transcendante pure. Il est beaucoup plus difficile de montrer qu'une extension ne l'est pas. Le contre-exemple de Swan, qui montre que le problème de Noether n'admet pas toujours une réponse affirmative, consiste à attacher un invariant aux extensions de corps, s'annulant lorsque l'extension est transcendante pure. Mais avant d'établir ce contre-exemple, nous avons besoin de quelques prérequis.

2 Quelques prérequis d'algèbre et de théorie des nombres

2.1 Modules sur les anneaux de Dedekind

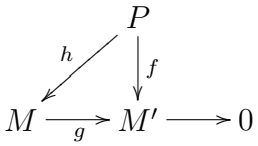
Dans cette partie, nous allons nous intéresser à des anneaux dits de Dedekind. Nous allons en particulier étudier la structure des idéaux dans un tel anneau, puis celle des modules. Nous verrons que, comme dans les anneaux principaux, tout idéal non nul s'écrit de manière unique comme produit d'idéaux premiers, puis nous remarquerons qu'il est possible d'établir une classification des modules sur un anneau de Dedekind qui rappelle énormément celle des modules sur un anneau principal.
On supposera dans cette section que les anneaux considérés sont commutatifs.

2.1.1 Modules projectifs

Soit A un anneau.

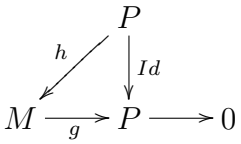
Définition 2.1.1. ***Modules projectifs***
On dit qu'un module P sur un anneau A est ***projectif*** *s'il vérifie l'une des trois propriétés équivalentes ci-dessous:*
1) Étant donnés M, M' deux A-modules quelconques, un morphisme surjectif g de M sur M' et un morphisme f de P dans M', il existe un morphisme h de P dans

M tel que le diagramme commute:



2) Quels que soient M et M′ deux A-modules, dès que $0 \to M' \to M \to P \to 0$ *est exacte, elle est scindée.*
3) Il existe un A-module S tel que $P \oplus S$ *soit libre.*

Preuve. Montrons que ces trois propriétés sont bien équivalentes.
1) $\Rightarrow$ 2) On se donne une suite exacte $0 \to M' \to M \to P \to 0$, on note $g : M \to P$ la surjection de la suite exacte, et on considère



Le morphisme h fournit une section de la suite exacte.
2) $\Rightarrow$ 3) Il est aisé de trouver une suite exacte courte $F \to P \to 0$ où F est libre (par exemple, on choisit F dont une base est construite sur une famille génératrice de P). Alors la section donnée par 2) nous permet de d'écrire $F = P \oplus S$ pour un certain S.
3) $\Rightarrow$ 1) Comme $Hom_A(X \oplus Y, M) = Hom_A(X, M) \oplus Hom_A(Y, M)$, et comme $M \mapsto Hom_A(F, M)$ est un foncteur exact si F est libre, 3) impose que $M \mapsto Hom_A(P, M)$ est un foncteur exact. Il suffit de voir ensuite que si $M \mapsto Hom_A(P, M)$ est exacte, alors P vérifie 1). Par conséquent, si on se donne M, M', f et g comme en 1), on déduit de la suite exacte $0 \to Ker(g) \to M \to M' \to 0$ que la suite $0 \to Hom_A(P, Ker(g)) \to Hom_A(P, M) \to Hom_A(P, M') \to 0$ est exacte, et alors la partie droite de cette suite exacte montre 1). □

2.1.2 Anneaux de Dedekind

Nous allons à présent définir les anneaux de Dedekind, puis nous allons étudier les idéaux dans un tel anneau.

Définition 2.1.2. ***Anneaux de Dedekind***
On dit qu'un anneau commutatif unitaire intègre A est ***de Dedekind*** *s'il vérifie les trois conditions suivantes:*
a) A est noethérien;
b) A est intégralement clos;
c) Tout idéal premier non nul de A est maximal.

L'étude des idéaux dans un anneau de Dedekind s'avère particulièrement intéressante, puisque, comme nous allons le voir, les idéaux fractionnaires forment un groupe (pour la multiplication d'idéaux).

Définition 2.1.3. ***Idéaux fractionnaires***
Soit A un anneau et soit K son corps des fractions. On appelle ***idéal fractionnaire*** *de A un sous-A-module non nul I de K tel qu'il existe un élément non nul d de A vérifiant $dI \subset A$. On appellera* ***idéal entier*** *un idéal au sens usuel, par opposition aux idéaux fractionnaires.*
De manière analogue à la multiplication usuelle des idéaux, on peut définir IJ comme l'ensemble des combinaisons linéaires finies de I et de J. On vérifie aussi que IJ est un idéal fractionnaire.
On définit enfin la ***divisibilité*** *des idéaux fractionnaires: $I|J$ s'il existe L idéal entier de A tel que $J = IL$.*

Dans la suite, A sera un anneau de Dedekind, et K son corps des fractions.

Lemme 2.1.4. ***Loi de simplification***
Soit I un idéal fractionnaire de A. Alors il existe un idéal fractionnaire J tel que IJ soit un idéal principal non nul de A.
Corollaire: Soient I, J, L trois idéaux fractionnaires de A. Si $IJ = IL$ alors $J = L$.

Preuve. Commençons par remarquer que tout idéal entier I non nul de A contient un produit fini d'idéaux premiers non nuls.
En effet, procédons par l'absurde. Supposons que l'ensemble $\mathbb{I}$ des idéaux ne contenant aucun produit fini d'idéaux premiers non nuls est non vide. Comme A est noethérien, toute suite croissante d'idéaux est stationnaire, donc l'inclusion sur $\mathbb{I}$ est un ordre inductif. D'après le lemme de Zorn, on peut trouver un idéal m maximal dans $\mathbb{I}$ qui ne contient pas de produit fini d'idéaux premiers non nuls. L'idéal m n'est pas premier et $m \neq A$, donc il existe r, s dans $A - m$ tels que $rs \in m$. Mais on remarque que $(m + (s))(m + (r))$ est dans m, et par maximalité de m, $m + (s)$ et $m + (r)$ contiennent chacun un produit fini d'idéaux premiers non nul, donc m aussi, ce qui est contradictoire.
Montrons un deuxième résultat préliminaire: si I est un idéal entier propre de A, alors il existe $d \in K - A$ tel que $dI \subset A$.
Soit $x \in I$ non inversible, et on choisit $p_1 \dots p_r \subset (x)$ avec r minimal ($r \neq 0$). I est inclus dans un idéal maximal p qui est premier. Alors $p_1 \dots p_r \subset p$, et par primalité de p, il existe p_i tel que $p_i \subset p$, disons $i = 1$. Cette inclusion est en fait une égalité par maximalité de p_i. Puis par minimalité de r, il existe un élément y dans $p_2 \dots p_r - (x)$, et alors $d = y/x$ convient.
Montrons maintenant le lemme.

Soit I un idéal fractionnaire, et soit $i \in I$ non nul. Considérons l'idéal $J = \{x \in A, xI \subset (i)\}$. Remarquons d'une part que J est non nul, d'autre part que $IJ \subset (i)$. S'il y a égalité dans la dernière inclusion, on a fini. Sinon, IJ/i est un idéal entier propre de A et on peut lui appliquer le résultat préliminaire: il existe $d \in K - A$ tel que $dIJ/i \subset A$. Montrons qu'on a forcément dans ce cas $d \in A$, ce qui fournira une contradiction.
Comme $i \in I$, on a $J \subset IJ/i$, donc $dJ \subset dIJ/i \subset A$. Par définition de J, on déduit que $dJ \subset J$. Maintenant on peut interpréter cette inclusion sous forme matricielle: soit $j_1, \ldots, j_m$ une famille de générateurs de J, alors on peut écrire chaque dj_k comme une combinaison linéaire d'éléments de cette famille, ce qui fournit une matrice M de taille $m \times m$ à coefficients dans A telle que $(d - M)(j_k) = 0$, (j_k) étant le vecteur colonne des j_k. En inversant le système à l'aide de la comatrice, on obtient que $det(d - M) = 0$. Or $det(d - M)$ est un polynôme unitaire en d, à coefficients dans A. Comme A est intégralement clos, $d \in A$, absurde.
Le corollaire de ce lemme en découle facilement: il suffit de multiplier I par un autre idéal bien choisi pour que le produit soit un idéal principal, puis d'effectuer une division par le générateur de cet idéal principal. □

Lemme 2.1.5. ***Les idéaux fractionnaires d'un anneau de Dedekind forment un groupe***
Dans un anneau de Dedekind, les idéaux fractionnaires forment un groupe.

Preuve. Le seul point qui manque est l'existence d'un inverse, ce qui est garanti par la première partie de la loi de simplification. □

Ce lemme nous permet de définir la notion de groupe des classes:

Définition 2.1.6. ***Groupe des classes***
On appelle ***groupe des classes*** *le groupe des idéaux fractionnaires quotienté par le sous-groupe des idéaux fractionnaires principaux.*

On remarque au passage que grâce au lemme précédent, la relation de division coïncide avec la relation d'inclusion pour les anneaux de Dedekind.

Théorème 2.1.7. ***Décomposition en produit d'idéaux premiers***
Si l'anneau de Dedekind A n'est pas un corps, alors chaque idéal non trivial I de A s'écrit de manière unique comme produit d'idéaux premiers.

Preuve. Commençons par montrer l'unicité de la même façon que pour la factorisation des nombres premiers.
Unicité: supposons que $I = P_1 \ldots P_r = Q_1 \ldots Q_s$, avec les P_i et les Q_i idéaux premiers non nuls pas forcément deux à deux distincts. Alors $P_1 \supset Q_1 \ldots Q_s$ donc $P_1 \supset Q_i$ pour un certain i par primalité. Cette inclusion est en fait une égalité par

maximalité puisque A est un anneau de Dedekind. Finalement, en vertu de la loi de simplification, par une récurrence simple, on peut identifier terme à terme les P_i et Q_i, d'où l'unicité.
Existence: Par l'absurde. Comme A est noethérien, en procédant comme pour la démonstration du lemme 2.1.4, avec le lemme de Zorn, on peut trouver un idéal m qui soit maximal dans l'ensemble des idéaux qui ne s'écrivent pas sous la forme d'un produit d'idéaux premiers et distincts de (0) et de (1). Alors m est inclus dans un idéal maximal p. D'après le lemme précédent, on peut trouver un idéal propre I tel que $m = pI$, et alors $m \subset I$. Mais si $m = I$ alors $pm = m$ donc $p = A$, absurde. Donc I est produit d'idéaux premiers par maximalité de m, et par conséquent m l'est aussi car $m = pI$, absurde. □

On peut aussi montrer que la décomposition en produit d'idéaux premiers est une condition nécessaire et suffisante pour qu'un anneau soit de Dedekind, mais on n'aura pas besoin dans la suite de cette caractérisation.

Remarque 2.1.8. ***Analogie et intérêt***
L'énoncé de cette dernière propriété est l'analogue du théorème de décomposition en facteurs premiers dans le cas d'un anneau factoriel. Dans les anneaux non factoriels (exemple classique: $\mathbb{Z}[\sqrt{-3}]$: on a $2 \times 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$), on ne peut pas espérer une factorialité en produit d'éléments premiers, mais on peut espérer qu'un tel anneau est de Dedekind, d'où une factorisation des idéaux.

La remarque suivante sera utile dans la suite:

Remarque 2.1.9. *Soit I un idéal de A. Alors I est engendré par deux éléments.*

Preuve. L'idéal I est de type fini: disons $I = (a_1, ..., a_n)$. Soit $J = (a_1)$. Montrons d'abord que tout idéal de A/J est principal. D'après le théorème des restes chinois, il suffit de le faire lorsque $J = P^s$, où P est un idéal premier. Les idéaux propres de A/J sont alors P/P^s, P^2/P^s,...,P^{s-1}/P^s. Pour chaque j, on choisit $x_j \in P^j - P^{j+1}$. Alors le pgcd de (x_j) et de P^s est P^j et donc $P^j = (x_j) + P^s$. Ainsi P^j/P^s est engendré par la classe de x_j et est principal. Par conséquent, tout idéal de A/J est bien principal.
On en déduit que I/J est un idéal principal de A/J. Soit $a \in I$ tel que la classe de a dans A/J est un générateur de I/J. Il est clair que $(a_1, a) \subseteq I$. Réciproquement, soit $b \in I$. Alors la classe de b modulo J est dans I/J et donc $b \in (a_1, a)$. Donc $I = (a_1, a)$ □

2.1.3 Modules de type fini sur un anneau de Dedekind

Afin de construire une classification des modules de type fini sur un anneau de Dedekind, nous aurons besoin de la proposition suivante:

Lemme 2.1.10. ***Somme directe des idéaux fractionnaires***
Soit I, J deux idéaux fractionnaires d'un anneau de Dedekind A. Alors $I \oplus J \cong A \oplus IJ$. On a donc aussi $\bigoplus_{i=1,\dots,n} I_i \cong A^{n-1} \oplus \prod_{i=1,\dots,n} I_i$, où les I_i sont des idéaux fractionnaires de A.

Preuve. On peut supposer que I et J sont premiers entre eux dans A quitte à multiplier par des éléments de K (rappelons que K désigne le corps des fractions de A). En effet, on peut déjà supposer que I et J sont dans A, quitte à multiplier par un élément de A. On peut alors les décomposer en produits d'idéaux premiers, disons $I = \prod P_i^{r_i}$ et $J = \prod P_i^{r'_i}$, avec des puissances positives. Puis on choisit un élément a tel que les ordres des P_i dans la décomposition de (a) soient exactement les r_i. Pour ce faire, on choisit pour chaque i un élément $x_i \in P_i^{r_i} - P_i^{r_i+1}$ et on prend a tel que $a \equiv x_i \pmod{P_i^{r_i+1}}$ pour tout i (grâce au théorème des restes chinois). Soit α idéal propre de A tel que $I\alpha = (a)$. De la même façon on choisit β idéal propre et un élément b tels que $\alpha\beta = (b)$, et tels que les P_i et les facteurs premiers de α ne soient pas facteurs premiers de β. Alors $bI/a = (\alpha\beta)I(\alpha^{-1}I^{-1}) = \beta$, qui est premier avec J par construction.
On définit alors l'application $\pi : I \oplus J \to A$ par $\pi(i,j) = i+j$, de noyau $I \cap J = IJ$ et d'image A car I et J sont premiers entre eux. Alors la suite

$$0 \longrightarrow IJ \longrightarrow I \oplus J \longrightarrow A \longrightarrow 0$$

est exacte et scindée car A est libre. D'où la conclusion. □

Étudions à présent la structure des modules projectifs:

Lemme 2.1.11. ***Stucture des modules projectifs de type fini sur un anneau de Dedekind***
Soient A un anneau de Dedekind et K son corps des fractions. Un module M de type fini sur A est projectif si, et seulement si, il est sans torsion.
De plus, si $M \neq 0$ est projectif, alors $M \cong A^{n-1} \oplus I$ où $n = rang(M) = dim_K(M \otimes_A K) > 0$ et I un idéal de A.

Preuve. Montrons qu'un module de type fini M sur A est projectif si et seulement s'il est sans torsion. Si M est projectif, alors il existe un module S tel que $S \oplus M$ libre en tant que A-module, donc M est sans torsion. Réciproquement, supposons que M est sans torsion, et procédons par récurrence sur $n = rang(M)$. Si $n = 1$, alors M est un sous A-module de type fini de $M \otimes_A K \cong K$, et donc il est isomorphe à un idéal fractionnaire, projectif d'après 2.1.10.
Maintenant si on choisit $n-1$ éléments de M tels que le sous-espace vectoriel V qu'ils engendrent dans $M \otimes_A K$ est de dimension $n-1$, on peut construire le sous-A-module $N = \{m \in M, m \otimes_A 1 \in V\}$ de M de rang $n-1$. La suite exacte

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

reste exacte après avoir tensorisé avec K, donc M/N est de rang 1. Donc M/N étant sans torsion, il est projectif et la suite est scindée. La récurrence est établie, et le résultat en découle par le lemme précédent. □

Le lemme précédent nous donne l'existence d'un certain idéal I. Le lemme suivant nous donne l'unicité de cet idéal à isomorphisme près:

Lemme 2.1.12. *Soit A un anneau de Dedekind et K son corps des fractions. Soient n et m des entiers naturels et I et J des idéaux non nuls tels que $A^n \oplus I \cong A^m \oplus J$. Alors $n = m$ et $I \cong J$.*

Preuve. On a $I \otimes_A K \cong K$ et $J \otimes_A K \cong K$. En tensorisant l'isomorphisme donné, on a alors $K^{n+1} \cong K^{m+1}$, d'où $n = m$.
D'autre part, on a $\bigwedge^{n+1}(A^n \oplus I) \cong \bigwedge^{n+1}(A^n \oplus J)$, donc

$$\bigoplus_{p+q=n+1} (\bigwedge^p (A^n) \otimes \bigwedge^q (I)) \cong \bigoplus_{p+q=n+1} (\bigwedge^p (A^n) \otimes \bigwedge^q (J))$$

Comme I et J sont engendrés par au plus deux éléments, on obtient un isomorphisme $I \oplus \Lambda^2(I)^n \cong J \oplus \Lambda^2(J)^n$. Les deux éléments qui engendrent un idéal de A ne pouvant pas être libres, $\Lambda^2(I)$ et $\Lambda^2(J)$ sont de torsion, alors que I et J ne le sont pas. Donc $I \cong J$. □

Nous pouvons finalement établir une classification des modules de type fini sur un anneau de Dedekind:

Théorème 2.1.13. ***Structure des modules de type fini sur un anneau de Dedekind***
Soit M un module de type fini sur un anneau de Dedekind A. Alors $M \cong M_0 \oplus M_1$, où M_0 est sans torsion et M_1 est de torsion. Si $M_0 \neq 0$, il existe un unique idéal non nul I à isomorphisme près et un unique entier naturel n tels que $M_0 \cong A^n \oplus I$. Il existe des idéaux premiers uniques $P_1, ..., P_q$ et des uniques entiers strictement positifs $r_1, ..., r_q$ tels que $M_1 \cong \bigoplus A/P_i^{r_i}$.

Preuve. Soit $Tor(M)$ le sous-module de torsion de M. La suite exacte $0 \to Tor(M) \to M \to M/Tor(M) \to 0$ est scindée puisque $M/Tor(M)$ est sans torsion et donc projectif (2.1.11). On peut donc écrire $M \cong M/Tor(M) \oplus Tor(M)$. $M/Tor(M)$ a déjà été étudié. Intéressons-nous à $Tor(M)$.
Notons J l'annulateur de $TorM$, i.e. $J = \{a | aTor(M) = 0\}$. Comme M est de type fini, $Tor(M)$ l'est aussi, donc J est non nul. Par le théorème de décomposition des idéaux premiers, $J = \prod P_i^{r_i}$, où P_i sont des idéaux premiers de A.
Le théorème des restes chinois permet d'écrire l'isomorphisme de A/J-modules: $Tor(M) \cong \bigoplus Tor(M)/P_i^{r_i} Tor(M)$. Afin d'étudier $Tor(M)/P^r Tor(M)$ pour un

idéal premier P et un entier strictement positif r, montrons le lemme suivant:
Lemme: Soit N un module de type fini sur A/P^r où A est un anneau de Dedekind, P un idéal premier non nul, et r un entier strictement positif. Alors N est isomorphe à une somme directe de modules de la forme A/P^s pour $1 \leq s \leq r$.
Preuve du lemme: Procédons par récurrence sur r. Pour $r = 1$, l'énoncé est évident par la théorie des espaces vectoriels, puisque A/P est un corps. Soit maintenant $r > 1$. Soit $x_1, ..., x_n$ une base du A/P-espace vectoriel $P^{r-1}N$. Soient $\alpha \in P^{r-1}/P^r$ et $y_1, ..., y_n \in N$ tels que $x_i = \alpha y_i$. Soit $N' = N/(y_1A/P^r \oplus ... \oplus y_nA/P^r)$. Le module N' est alors un A/P^{r-1}-module, donc, par hypothèse de récurrence, on peut écrire: $N' = \bigoplus_{0<i<r}(A/P^i)^{a_i}$. On a alors la suite exacte:

$$0 \to y_1A/P^r \oplus ... \oplus y_nA/P^r \to N \to \bigoplus_{i<r}(A/P^i)^{a_i} \to 0$$

Montrons qu'elle est scindée. Considérons $N'' = A/P^i$ un des facteurs directs de N'. Soit $x \in N$ dont la projection dans N' vaut $1 \in N''$. Soit $\beta \in P^i/P^r - P^{i+1}/P^r$. Alors $\beta x \in y_1A/P^r \oplus ... \oplus y_nA/P^r$, d'où $P^{r-i}\beta x = 0$. Donc $\beta x \in y_1P^i/P^r \oplus ... \oplus y_nP^i/P^r$. Il existe donc $y \in y_1A/P^r \oplus ... \oplus y_nA/P^r$ tel que $\beta(x - y) = 0$. Soit $z = x - y$. On vérifie alors facilement qu'il existe un morphisme de A/P^r-modules $g : N'' \to N$ tel que $g(1) = z$. En sommant sur tous les facteurs N'' de N', on arrive à scinder la suite exacte précédente. On a donc

$$N \cong (A/P^r)^n \oplus \bigoplus_{0<i<r} (A/P^i)^{a_i}$$

Reste à voir l'unicité des P_i. Écrivons donc $N \cong \bigoplus_{P,i}(A/P^i)^{a_{P,i}} \cong \bigoplus_{P,i}(A/P^i)^{b_{P,i}}$, où P décrit les idéaux premiers et i les entiers naturels, avec $a_{P,0} = 0$. Étant donné un idéal premier P_0 et un entier j, la dimension du A/P_0-espace vectoriel $P_0^jN/P_0^{j+1}N$ est $\sum_{i=j+1}^{\infty} a_{P_0,i} = \sum_{i=j+1}^{\infty} b_{P_0,i}$. L'unicité en découle immédiatement. □

Exemple 2.1.14. $\mathbb{Z}[\zeta]$ ***est un anneau de Dedekind***
Si ζ est une racine de l'unité, $\mathbb{Z}[\zeta]$ est l'anneau de entiers de $\mathbb{Q}(\zeta)$ et est un anneau de Dedekind.

Preuve. La preuve fera l'objet de la section qui suit. □

2.2 Entiers algébriques

L'objectif central de cette partie va être de déterminer l'anneau des entiers algébriques de $\mathbb{Q}(\zeta)$, où ζ est une racine primitive de l'unité. Rappelons donc brièvement les notions d'entier et de fermeture intégrale.

Soient A un anneau intègre et K son corps des fractions. Soit $L|K$ une extension finie. On dit qu'un élément $b \in L$ est un **entier sur** A s'il est racine d'un polynôme unitaire à coefficients dans A. On parlera d'**entier algébrique** lorsque $A = \mathbb{Z}$. On appelle **fermeture intégrale** de A dans L l'ensemble des entiers sur A dans L. On parlera d'**anneau des entiers** lorsque $A = \mathbb{Z}$. On dit qu'un anneau est **intégralement clos** s'il est intègre et s'il est sa propre fermeture intégrale dans son corps des fractions. La fermeture intégrale de A dans L est alors intégralement close. Nous voulons donc déterminer la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}(\zeta)$.

2.2.1 Norme, trace et discriminant

Commençons en définissant quelques notions liées aux extensions de corps qui vont être essentielles pour la suite. Considérons $L|K$ une extension finie de degré n. Nous allons définir la norme et la trace d'un élément de L:

Définition 2.2.1. ***Norme et trace d'un élément***
Soit $x \in L$. Soit $f_a : x \mapsto ax$. Il s'agit d'un endomorphisme du K-espace vectoriel L. On définit alors la ***norme*** *et la* ***trace*** *de x par: $N_{L/K}(a) = det(f_a)$ et $Tr_{L/K}(a) = Tr(f_a)$.*

On supposera dans le reste de cette section que l'extension est séparable. Dans ce cas, on peut alors calculer la norme et la trace d'un élément facilement grâce à la proposition suivante:

Proposition 2.2.2. ***Calcul explicite de la norme et la trace***
Soit Ω une clôture algébrique de K. Alors le polynôme caractéristique de f_a est donné par: $\chi(f_a) = \prod_\sigma (X - \sigma(a))$, où σ décrit les K-morphismes $L \to \Omega$.

Preuve. Soient d le degré de a et $d' = \dfrac{n}{d}$. On considère $a_1, ..., a_{d'}$ une base de $L|K(a)$. Soit $P = \sum c_k X^k$ le polynôme minimal de a. Alors, dans la base $(a^{i-1}a_j)_{1 \le i \le d, 1 \le j \le d'}$ de $L|K$, la matrice de f_a est diagonale par blocs, chaque bloc étant une matrice compagnon

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & 0 & \dots & 0 & -c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -c_{d-1} \end{pmatrix}$$

Donc $\chi(f_a) = P^{d'} = \prod_\sigma (X - \sigma(a))$, puisque, $L|K$ étant séparable, chaque racine de P apparaît exactement d' fois parmi les $\sigma(a)$. □

On en déduit immédiatement les relations:

$$N_{L/K}(a) = \prod_{\sigma} \sigma(a)$$

et

$$Tr_{L/K}(a) = \sum_{\sigma} \sigma(a)$$

Définissons à présent le discriminant d'une base du K-espace vectoriel L:

Définition 2.2.3. ***Discriminant***
Si $b_1, \ldots, b_n$ est une base de L et Ω une clôture algébrique de K, on définit le ***discriminant*** *de $b_1, \ldots, b_n$ par: $d(b_1, \ldots, b_n) = det(\sigma_i(b_j))^2$, où les σ_i décrivent les K-morphismes $L \to \Omega$. Remarquons que, l'extension étant séparable, son degré et son degré séparable coïncident, et donc le discriminant est bien défini.*

De plus, en tenant compte de la proposition précédente, on remarque que la matrice $(Tr_{L/K}(b_i b_j))_{i,j}$ est égale au produit de la matrice $(\sigma_i(b_j))_{i,j}$ par sa transposée, donc $d(b_1, ..., b_n) = det(Tr_{L/K}(b_i b_j))$. Il semble donc naturel d'étudier le discriminant en s'intéressant à la forme bilinéaire symétrique du K-espace vectoriel L donnée par $\beta : (x, y) \to Tr_{L/K}(xy)$, d'où la proposition suivante:

Proposition 2.2.4. ***Le discriminant est non nul***
β est non dégénérée et $d(b_1, \ldots, b_n) \neq 0$.

Preuve. D'après le théorème de l'élément primitif, il existe $z \in L$ tel que $L = K(z)$. Alors, dans la base $(1, z, \ldots, z^{n-1})$, la matrice de β est $(Tr_{L/K}(z^{i-1} z^{j-1}))_{i,j}$, dont le déterminant est $d(1, z, ..., z^{n-1}) \neq 0$ puisque la matrice $(\sigma_i(z^j))$ est la matrice de Vandermonde associée aux conjugués de z. Donc β est non dégénérée, et sa matrice dans la base $(b_1, \ldots, b_n)$ étant $(Tr_{L/K}(b_i b_j))_{i,j}$, $d(b_1, \ldots, b_n) \neq 0$. □

Mais... pourquoi avons-nous défini le discriminant? Quel est le lien avec les entiers algébriques? Considérons A un anneau intègre et son corps des fractions K. Supposons que A est intégralement clos. Soient alors $L|K$ une extension finie séparable et B la fermeture intégrale de A dans L. Remarquons alors que, étant algébrique sur K, tout élément de L s'écrit $\frac{b}{a}$, avec $b \in B$ et $a \in A$. L'anneau A étant intégralement clos, $A = B \cap K$, et donc, si $b \in B$, les conjugués de b dans Ω étant aussi des entiers sur A, en vertu de $N_{L/K}(b) = \prod_\sigma \sigma(b)$ et $Tr_{L/K}(b) = \sum_\sigma \sigma(b)$, on a $N_{L/K}(b) \in A$ et $Tr_{L/K}(b) \in A$. Une fois ces remarques faites, l'utilité du discriminant découle de la proposition suivante:

Proposition 2.2.5. ***Propriété fondamentale du discriminant***
Soit $(b_1, \ldots, b_n)$ une base de L contenue dans B. Soit $d = d(b_1, \ldots, b_n)$. Alors $dB \subseteq b_1 A + ... + b_n A$.

Preuve. Soit $b = a_1b_1 + ... + a_nb_n \in B$, avec $a_i \in K$. Montrons que, pour tout i, $da_i \in A$. On remarque que, pour tout i, on a: $Tr_{L/K}(bb_i) = a_1Tr_{L/K}(b_1b_i) + \cdots + a_nTr_{L/K}(b_nb_i)$. On reconnaît ici un système linéaire dont les a_i sont solutions. La matrice de ce système est $T = (Tr_{L/K}(b_ib_j))_{i,j}$, dont le déterminant est d. Comme $d \neq 0$, T est inversible, d'inverse $\dfrac{{}^tCom(T)}{d}$, où ${}^tCom(T)$ est la transposée de la comatrice de T. Comme les coefficients de ${}^tCom(T)$ et les $Tr_{L/K}(bb_i)$ pour $1 \leq i \leq n$ sont dans A d'après les remarques précédentes, en inversant le système, on obtient bien que $da_i \in A$ pour tout i. □

2.2.2 Indice de ramification et degré résiduel

Gardons les notations et hypothèses de la partie précédente. Supposons de plus que A est de Dedekind. Commençons par montrer que B est aussi un anneau de Dedekind:

Proposition 2.2.6. ***La fermeture intégrale est un anneau de Dedekind*** *B est un anneau de Dedekind.*

Preuve. B est intégralement clos par définition.
Montrons qu'il est noethérien. Considérons une base $(b_1, \ldots, b_n)$ de L contenue dans B (elle existe puisque tout élément de L est quotient d'un élément de B par un élément de A). Alors, d'après les propositions 2.2.4 et 2.2.5, si l'on pose $d = d(b_1, \ldots, b_n)$, alors $d \neq 0$ et $B \subseteq \dfrac{b_1}{d}A + \cdots + \dfrac{b_n}{d}A$. L'anneau A étant noethérien et $\dfrac{b_1}{d}A + \cdots + \dfrac{b_n}{d}A$ étant un A-module de type fini, B l'est aussi, ainsi que tout idéal de B. Par conséquent, tout idéal de B est un B-module de type fini, et B est bien noethérien.
Reste à prouver que tout idéal premier non nul de B est maximal. Soit Π un idéal premier non nul de B. Alors $A \cap \Pi$ est un idéal premier non nul de A. Donc, comme les idéaux premiers non nuls de A sont maximaux, $A/(A \cap \Pi)$ est un corps, et B/Π est alors une algèbre intègre sur $A/(A \cap \Pi)$, de dimension finie. En écrivant alors le polynôme minimal d'un élément x non nul de B/Π, on s'aperçoit que x est inversible dans B/Π. Donc B/Π est un corps et Π est maximal. Nous avons ainsi montré que B est de Dedekind. □

Remarquons que nous avons prouvé que B est un A-module de type fini.
Soit π un idéal premier non nul de A. On note alors $\Pi = \pi B$: c'est un idéal de B, et il est distinct de B. En vertu de 2.1.7, B étant de Dedekind, on peut donc écrire $\Pi = \Pi_1^{e_1} \ldots \Pi_r^{e_r}$, où les Π_i sont des idéaux premiers de B. Remarquons que $\pi = \Pi_i \cap A$. On dit que les e_i sont les **indices de ramification** et les

$f_i = [B/\Pi_i : A/\pi]$ sont les **degrés résiduels**. Alors les indices de ramification et les degrés résiduels satisfont une équation remarquable:

Proposition 2.2.7. ***Lien entre les indices de ramification et les degrés résiduels***
$n = e_1 f_1 + \cdots + e_r f_r$.

Preuve. D'après le théorème des restes chinois, on a l'isomorphisme de A/π-espaces vectoriels: $B/\Pi \cong \bigoplus_{i=1}^{r} B/\Pi_i^{e_i}$. Montrons que $dim(B/\Pi) = n$ et que $dim(B/\Pi_i^{e_i}) = e_i f_i$.
B/Π est de dimension finie car B est un A-module de type fini. Soient $b_1, \ldots, b_k \in B$ tels que $\overline{b_1}, \ldots, \overline{b_k}$ est une base de B/Π.
Montrons d'abord que $b_1, \ldots, b_k$ est libre sur K. Supposons qu'elle ne l'est pas. Alors elle n'est pas libre sur A. Considérons donc une relation de liaison non triviale $\sum_{i=1}^{k} a_i b_i = 0$, $a_i \in A$. Soit l'idéal $I = (a_1, ..., a_k)$ dans A. Soit $a \in I^{-1} - I^{-1}\pi$. Alors, après passage modulo π, la relation $\sum_{i=1}^{k} a a_i b_i = 0$ fournit une relation de liaison non triviale entre les $\overline{b_i}$: absurde! Donc $b_1, \ldots, b_k$ est libre sur K.
Montrons à présent que $b_1, \ldots, b_k$ engendre L. Soient les A-modules $M = Ab_1 + \cdots + Ab_k$ et $N = B/M$. L'anneau B étant un A-module de type fini, M et N sont aussi des A-modules de type fini. Soient donc $\lambda_1, \ldots, \lambda_s$ des générateurs de N. Par définition de $b_1, \ldots, b_k$, $B = M + \Pi$, donc $N = \pi N$. On peut donc écrire $\lambda_i = \sum_{j=1}^{s} a_{ij}\lambda_j$, $a_{ij} \in \pi$. Notons T la matrice $(a_{ij}) - Id$, et $\Lambda = {}^t(\lambda_1, \ldots, \lambda_s)$. Alors $T\Lambda = 0$. Donc, en inversant avec la comatrice, $(detT)\Lambda = 0$, et alors $(detT)N = 0$, d'où $(detT)B \subseteq M$. Comme de plus $detT$ est non nul puisqu'il n'est pas congru à 0 modulo π, $L = (detT)L$ est bien engendré par $b_1, \ldots, b_k$. Donc $dim(B/\Pi) = n$.
Montrons finalement que $dim(B/\Pi_i^{e_i}) = e_i f_i$. Remarquons que, si $a \in \Pi_i^v - \Pi_i^{v+1}$, alors $B \to \Pi_i^v/\Pi_i^{v+1}$, $x \mapsto ax$ est une application linéaire surjective de noyau Π_i, puisque le pgcd de (a) et de Π_i^{v+1} est Π_i^v et alors $(a) + \Pi_i^{v+1} = \Pi_i^v$. On déduit que $\Pi_i^v/\Pi_i^{v+1} \cong B/\Pi_i$. Donc dans la suite d'espaces vectoriels emboîtés $(0) \subseteq \Pi_i^{e_i-1}/\Pi_i^{e_i} \subseteq \cdots \subseteq \Pi_i/\Pi_i^{e_i} \subseteq B/\Pi_i^{e_i}$, chaque quotient est isomorphe à B/Π_i, et $dim(B/\Pi_i^{e_i}) = e_i f_i$. □

2.2.3 Anneau des entiers de $\mathbb{Q}(\zeta)$

Soit ζ une racine primitive m-ième de l'unité. On se place ici dans le cas où $A = \mathbb{Z}$, $K = \mathbb{Q}$ et $L = \mathbb{Q}(\zeta)$. On note toujours n le degré de $L|K$. Remarquons que l'extension $L|K$ est bien finie séparable et que A est bien intégralement clos. Pour déterminer l'anneau des entiers de $\mathbb{Q}(\zeta)$, nous allons procéder par récurrence. Le lemme suivant établit la propriété d'hérédité:

Lemme 2.2.8. ***Propriété d'hérédité***
Soient ζ_1 et ζ_2 des racines primitives m_1-ième et m_2-ième de l'unité, avec $m_1 \wedge$

$m_2 = 1$. *Soient* $m = m_1 m_2$ *et* ζ *une racine primitive* m*-ième de l'unité. Soient* $n_1 = [\mathbb{Q}(\zeta_1) : \mathbb{Q}]$ *et* $n_2 = [\mathbb{Q}(\zeta_2) : \mathbb{Q}]$. *On suppose que les anneaux des entiers dans* $\mathbb{Q}(\zeta_1)$ *et* $\mathbb{Q}(\zeta_2)$ *sont respectivement* $\mathbb{Z}[\zeta_1]$ *et* $\mathbb{Z}[\zeta_2]$. *On suppose de plus que les discriminants respectifs* $d_1 = d(1, \zeta_1, \ldots, \zeta_1^{n_1-1})$ *et* $d_2 = d(1, \zeta_2, \ldots, \zeta_2^{n_2-1})$ *sont des entiers premiers entre eux. Alors l'anneau des entiers* B *de* $\mathbb{Q}(\zeta)$ *est* $\mathbb{Z}[\zeta]$ *et* $d = d(1, \zeta, \ldots, \zeta^{\varphi(m)-1}) = d_1^{n_2} d_2^{n_1}$.

Preuve. On remarque aisément que $(\zeta_1^i \zeta_2^j)_{0 \leq i < n_1, 0 \leq j < n_2}$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\zeta)$ (la famille est génératrice et a la bonne dimension). Montrons que c'est une base du $\mathbb{Z}$-module B. Soit $b = \sum_{i,j} a_{ij} \zeta_1^i \zeta_2^j \in B$, $a_{ij} \in \mathbb{Q}$. Montrons que $a_{ij} \in \mathbb{Z}$. Notons $\alpha_j = \sum_i a_{ij} \zeta_1^i$. Alors $b = \sum_j \alpha_j \zeta_2^j$. Notons $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta_1)) = \{\sigma_1^{(2)}, \ldots, \sigma_{n_2}^{(2)}\}$ et $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta_2)) = \{\sigma_1^{(1)}, \ldots, \sigma_{n_1}^{(1)}\}$. Les équations $\sigma_i^{(2)}(b) = \sum_j \alpha_j \sigma_i^{(2)}(\zeta_2^j)$ constituent un système linéaire dont les α_j sont solutions. La matrice de ce système est $T = (\sigma_i^{(2)}(\zeta_2^j))$. Or $(detT)^2 = d_2$. Comme de plus les coordonnées de T sont des entiers algébriques ainsi que les $\sigma_i^{(2)}(b)$, en inversant le système à l'aide de la comatrice de T, les $d_2 \alpha_j$ sont aussi des entiers algébriques. Ils sont de plus dans $\mathbb{Q}(\zeta_1)$. Donc, par hypothèse, les $d_2 a_{ij}$ sont entiers. Il en est de même des $d_1 a_{ij}$. Donc, par le théorème de Bezout, d_1 et d_2 étant premiers entre eux, les a_{ij} sont entiers. Donc l'anneau des entiers de $\mathbb{Q}(\zeta)$ est $\bigoplus_{i,j} \zeta_1^i \zeta_2^j \mathbb{Z} = \mathbb{Z}[\zeta]$.
Calculons $d = [det(\sigma_k^{(1)}(\zeta_1^i)\sigma_l^{(2)}(\zeta_2^j))]^2$. La matrice $(\sigma_k^{(1)}(\zeta_1^i)\sigma_l^{(2)}(\zeta_2^j))$ s'écrit comme le produit d'une matrice diagonale par blocs ayant n' blocs égaux à $(\sigma_k^{(1)}(\zeta_1^i))$ par une matrice qui, quitte à réordonner les colonnes, est aussi diagonale par blocs ayant n blocs égaux à $(\sigma_l^{(2)}(\zeta_2^j))$. On en déduit que $d = d_1^{n_2} d_2^{n_1}$. □

Nous sommes actuellement en mesure de prouver le théorème suivant:

Théorème 2.2.9. ***Anneau des entiers pour une extension cyclotomique finie***
L'anneau des entiers de $\mathbb{Q}(\zeta)$ *est* $\mathbb{Z}[\zeta]$.

Preuve. Notons B l'anneau des entiers de $\mathbb{Q}(\zeta)$. Supposons dans un premier temps que $m = p^v$ où p est premier. Soit ϕ_m le m-ième polynôme cyclotomique. On a alors $\phi_m = \prod_{1 \leq i \leq m, i \wedge m = 1} (X - \zeta^i) = \sum_{i=0}^{p-1} X^{ip^{v-1}}$. On en déduit que $p = \prod_{1 \leq i \leq m, i \wedge m = 1} (1 - \zeta^i)$. Or, si $1 \leq i \leq m$ et $i \wedge m = 1$, en choisissant i' tel que $m | ii' - 1$, on a $\dfrac{\zeta^i - 1}{\zeta - 1} = 1 + \zeta + \cdots + \zeta^{i-1} \in O$ et $\dfrac{\zeta - 1}{\zeta^i - 1} = \dfrac{\zeta^{ii'} - 1}{\zeta^i - 1} = 1 + \zeta^i + \cdots + \zeta^{i(i'-1)} \in O$. Par conséquent, $\dfrac{\zeta^i - 1}{\zeta - 1}$ est une unité dans B, et donc p et $(\zeta - 1)^{\varphi(m)}$ sont associés, où φ est la fonction indicatrice d'Euler. Donc les idéaux pB et $(\zeta - 1)^{\varphi(m)}$ sont égaux. Appliquons la relation de la proposition 2.2.7

à $\pi = p\mathbb{Z}$. On a alors $\Pi = pB = (\zeta - 1)^{\varphi(m)}$. Si on note e_i et f_i les indices de ramification et les degrés résiduels respectivement, pour i allant de 1 à r, alors chaque e_i est multiple de $\varphi(m)$. Or $n = \varphi(m) = e_1 f_1 + \cdots + e_r f_r$. Par des inégalités évidentes, on a donc $r = 1$, $e_1 = \varphi(m)$ et $f_1 = 1$.
On en déduit que $(\zeta - 1)$ est premier et que $B/(\zeta - 1) \cong \mathbb{Z}/p\mathbb{Z}$. Par conséquent $B = \mathbb{Z} + (\zeta - 1)B$, d'où $B = \mathbb{Z}[\zeta] + (\zeta - 1)B$. En multipliant par $\zeta - 1$, $(\zeta - 1)B = (\zeta - 1)\mathbb{Z}[\zeta] + (\zeta - 1)^2 B$, puis en réinjectant, $B = \mathbb{Z}[\zeta] + (\zeta - 1)^2 B$. En itérant ce processus, par une récurrence simple, on obtient $B = \mathbb{Z}[\zeta] + (\zeta - 1)^k B$ pour tout entier naturel k. Reste à choisir k. On voudrait $(\zeta - 1)^k B \subseteq \mathbb{Z}[\zeta]$. En tenant compte de $pB = (\zeta - 1)^{\varphi(m)}$, il suffit de trouver l tel que $p^l B \subseteq \mathbb{Z}[\zeta]$ puis de choisir $k = l\varphi(m)$. C'est ici que la proposition 2.2.5 entre en jeu: si $d = d(1, \zeta, ..., \zeta^{\varphi(m)-1})$, on a $dB \subseteq \mathbb{Z}[\zeta]$. Il suffit donc de montrer que, au signe près, d est une puissance de p. Calculons d.
Notons $\zeta_1, ..., \zeta_{\varphi(m)}$ les conjugués de ζ. Alors, en remarquant que $(\sigma_i(\zeta^j))$ est la matrice de Van der Monde associée à $\zeta_1, ..., \zeta_{\varphi(m)}$, où les σ_i sont les $\mathbb{Q}$-morphismes de $\mathbb{Q}(\zeta)$ dans $\mathbb{C}$, on a $d = \pm \prod_{i \neq j}(\zeta_i - \zeta_j) = \pm \prod_i \phi'_m(\zeta_i)$. Donc, avec la proposition 2.2.2, $d = \pm N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\phi'_m(\zeta))$. En dérivant la relation $(X^{p^{v-1}} - 1)\phi_m = (X^{p^v} - 1)$ puis en évaluant en ζ, on obtient: $\zeta(\epsilon - 1)\phi'_m(\zeta) = p^v$, où $\epsilon = \zeta^{p^{v-1}}$ est une racine primitive p-ième de l'unité. Or $N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\zeta) = \pm 1$, $N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\epsilon - 1) = \pm \phi_p(1)^{p^{v-1}} = \pm p^{p^{v-1}}$ et $N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(p^v) = p^{v\varphi(m)}$. Donc d est bien une puissance de p (au signe près) et nous avons montré le théorème lorsque m est la puissance d'un nombre premier.
Le cas général découle alors immédiatement du lemme 2.2.8. □

Nous avons ainsi déterminé l'anneau des entiers dans $\mathbb{Q}(\zeta)$. Nous aurons cependant aussi besoin dans la suite de connaître l'anneau des entiers dans un corps quadratique. C'est l'objet de la section suivante.

2.2.4 Anneau des entiers d'un corps quadratique

Soit d un entier relatif sans facteur carré. Nous nous intéressons ici au cas où $A = \mathbb{Z}$, $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt{d})$. La proposition suivante permet de caractériser les entiers algébriques à l'aide de leur norme et de leur trace:

Proposition 2.2.10. ***Entiers algébriques dans un corps quadratique*** *Soit $a \in \mathbb{Q}(\sqrt{d})$. Alors a est un entier algébrique si, et seulement si, $N_{L/K}(a) \in \mathbb{Z}$ et $Tr_{L/K}(a) \in \mathbb{Z}$.*

Preuve. Notons $a = x + y\sqrt{d}$, avec $x, y \in \mathbb{Q}$. Un calcul élémentaire donne $N_{L/K}(a) = x^2 - dy^2$ et $Tr_{L/K}(a) = 2x$. Nous avons déjà montré que, si a est un entier algébrique, alors $N_{L/K}(a) \in \mathbb{Z}$ et $Tr_{L/K}(a) \in \mathbb{Z}$. Réciproquement, si $N_{L/K}(a) \in \mathbb{Z}$ et $Tr_{L/K}(a) \in \mathbb{Z}$, alors a est racine de $(X - x - y\sqrt{d})(X - x + y\sqrt{d}) = X^2 - Tr_{L/K}(a)X + N_{L/K}(a) \in \mathbb{Z}[X]$. □

Il est alors facile de déterminer l'anneau des entiers:

Théorème 2.2.11. ***Anneau des entiers pour une extension quadratique*** *Soit B l'anneau des entiers dans $\mathbb{Q}(\sqrt{d})$.*

(i) Si $d \equiv 2, 3\ [4]$, alors $B = \mathbb{Z} + \mathbb{Z}\sqrt{d}$.

(ii) Si $d \equiv 1\ [4]$, alors $B = \mathbb{Z} + \mathbb{Z}\dfrac{-1+\sqrt{d}}{2}$.

La preuve reposant sur des arguments arithmétiques élémentaires d'une extrême simplicité à partir de la proposition précédente, elle est laissée au lecteur.

2.3 Norme d'un idéal

Dans cette section, nous allons définir la norme d'un idéal, notion dont nous aurons besoin dans la suite. Considérons une extension finie séparable $L|K$. Soit A un sous-anneau de K dont le corps des fractions est K. Soit finalement B la fermeture intégrale de A dans L. Supposons que A est de Dedekind. Alors, d'après la proposition 2.2.6, B est aussi de Dedekind.

Définition 2.3.1. ***Norme relative d'un idéal***
Soit I un idéal de B. Écrivons $I = \Pi_1^{e_1}...\Pi_r^{e_r}$, où les Π_i sont des idéaux premiers. Notons $\pi_i = \Pi_i \cap A$ et $f_1 = [B/\Pi_1 : A/\pi_1]$, ..., $f_r = [B/\Pi_r : A/\pi_r]$. On définit alors la ***norme*** *de I, notée $N_{L|K}(I)$, par $N_{L|K}(I) = \prod_{i=1}^{r} \pi_i^{e_i f_i}$. Par convention, si $I = B$, alors $N_{L|K}(I) = A$, et si $I = 0$, alors $N_{L|K}(I) = 0$.*

Nous aurons alors besoin de trois propriétés essentielles de la norme. Établissons d'abord la compatibilité de la norme avec les tours d'extensions:

Proposition 2.3.2. ***Tours de normes***
Considérons une deuxième extension finie séparable $M|L$, et soit C la fermeture intégrale de A dans M. Alors, pour I idéal de C, on a $N_{M|K}(I) = N_{L|K}\big(N_{M|L}(I)\big)$.

Preuve. Par multiplicativité, il suffit de prouver la propriété lorsque I est un idéal premier de C. Notons $\Pi = I \cap B$ et $\pi = I \cap A$. Notons aussi $f_1 = [C/I : B/\Pi]$, $f_2 = [B/\Pi : A/\pi]$ et $f = [C/I : A/\pi]$. Comme $f = f_1 f_2$, on a $N_{M|K}(I) = \pi^f = \pi^{f_1 f_2} = N_{L|K}\big(N_{M|L}(I)\big)$. □

Intéressons-nous maintenant à la norme d'un idéal principal. Pour ce faire, nous avons d'abord besoin d'étudier la norme lorsque $L|K$ est galoisienne:

Lemme 2.3.3. ***Norme dans le cas d'une extension galoisienne***
Supposons $L|K$ galoisienne. Soit Π un idéal premier de B. Soit $\pi = \Pi \cap A$. Alors

$$N_{L|K}(\Pi)B = \prod_{\sigma \in Gal(L|K)} \sigma\Pi$$

Preuve. Écrivons $\pi B = \Pi_1^{e_1}...\Pi_r^{e_r}$ et $f_i = [B/\Pi_i : A/\pi]$. Notons $G = Gal(L|K)$. Fixons i entre 1 et r. Supposons que, pour tout $\sigma \in G$, $\sigma(\Pi_1) \neq \Pi_i$. Alors le théorème des restes chinois garantit l'existence de $b \in B$ tel que

$$b \equiv 0 \pmod{\Pi_i}$$
$$b \equiv 1 \pmod{\sigma(\Pi_1)} \text{ pour tout } \sigma \in G$$

Alors $N_{L|K}(b) = \prod_{\sigma \in G} \sigma(b)$ est dans $\Pi_i \cap A = \pi$. Comme cette norme est aussi dans Π_1 et ce dernier est premier, il existe $\sigma \in G$ tel que $\sigma(b) \in \Pi_1$, ce qui contredit la définition de b. Donc tous les Π_i sont conjugués via des éléments de G.
On déduit alors immédiatement que tous les f_i sont égaux, disons égaux à f. Comme pour $\sigma \in G$ on a $\pi B = \sigma(\pi B) = \prod_{i=1}^r \sigma(\Pi_i)^{e_i}$, on déduit que tous les e_i sont égaux, disons à e. La proposition 2.2.7 impose donc que $efr = [L : K] = Card(G)$. Le lemme découle alors immédiatement. □

Remarquons que, par multiplicativité, la formule montrée dans le lemme précédent est encore vraie si Π n'est pas premier. Nous ne supposons plus $L|K$ galoisienne. Nous pouvons à présent étudier la norme d'un idéal principal:

Proposition 2.3.4. ***Norme d'un idéal principal***
Supposons que $I = (\alpha)$ est principal. Alors $N_{L|K}(I)$ l'est aussi.

Preuve. On considère M la clôture galoisienne de $L|K$. Soit C la fermeture intégrale de A dans M. Alors, avec 2.3.2 et 2.3.3, on a

$$N_{M/K}(IC) = N_{L/K}(N_{M/L}(IC)) = N_{L|K}(I)^{[M:L]}$$
$$N_{M/K}(IC) = \prod_{\sigma \in Gal(M|K)} \sigma(IC) = (N_{L|K}(\alpha))^{[M:L]}$$

La proposition découle immédiatement de ces deux relations. □

Pour terminer, étudions la norme dans le cas particulier où $K = \mathbb{Q}$:

Proposition 2.3.5. ***Norme absolue***
Soit I un idéal de B. Alors $N_{L|\mathbb{Q}}(I)$ est engendré par l'indice de I dans B.

Preuve. Décomposons $I = \Pi_1^{e_i}...\Pi_r^{e_r}$, où les Π_i sont des idéaux premiers. Notons $p_i\mathbb{Z} = \Pi_i \cap \mathbb{Z}$ et $f_i = [B/\Pi_i : \mathbb{Z}/p_i\mathbb{Z}]$. Alors $N_{L|\mathbb{Q}}(I) = \left(\prod_{i=1}^r p_i^{e_i f_i}\right)\mathbb{Z}$. D'après le théorème des restes chinois, $B/I \cong \prod_{i=1}^r B/\Pi_i^{e_i}$. Il suffit donc de montrer que, pour tout i, $[B : \Pi_i^{e_i}] = p_i^{e_i f_i}$. Cela découle immédiatement de la démonstration de la proposition 2.2.7, où l'on prouve qu'il y a une filtration $(0) \subseteq \Pi_i^{e_i-1}/\Pi_i^{e_i} \subseteq \cdots \subseteq \Pi_i/\Pi_i^{e_i} \subseteq B/\Pi_i^{e_i}$ dont les quotients successifs sont des $\mathbb{Z}/p_i\mathbb{Z}$-espaces vectoriels de dimension f_i. □

3 Le contre-exemple de Swan

Nous avons vu que le théorème de Fischer donne une réponse affirmative au problème de Noether dans certains cas. Cependant, le problème de Noether admet parfois une réponse négative. C'est ainsi que Richard Swan proposa en 1969 un contre-exemple, que nous allons développer ici.

3.1 Construction d'un premier invariant dans le groupe de Grothendieck

Considérons un corps L et H un groupe fini d'automorphismes de L. Soit k un sous-corps de L stable par H tel que L soit une extension de type fini de k. Attention, remarquons qu'on ne suppose pas que les éléments de k sont fixes par H. Si A est un sous-anneau de L, on note A^H l'ensemble des éléments fixes par H.

Définition 3.1.1. ***Module de permutation***
On dit qu'un $\mathbb{Z}[H]$-module P est un ***module de permutation*** *si P est libre sur $\mathbb{Z}$, et possède une base permutée par H.*

Remarque 3.1.2. *Un module de permutation est une somme directe de modules de la forme $\mathbb{Z}[H/H']$ où H' désigne un sous-groupe de H.*

Nous allons à présent construire un invariant pour la famille des anneaux vérifiant les cinq propriétés suivantes:
P1: Le corps des fractions de A est L.
P2: A est une k-algèbre de type fini.
P3: A est stable par H.
P4: A est factoriel.
P5: A^*/k^* est un groupe abélien de type fini. Ici, A^* (resp. k^*) désigne le groupe des unités de A (resp. k).
Dans la suite, nous noterons $\mathcal{F}$ la famille des anneaux vérifiant les propriétés $P1$ à $P5$.

Lemme 3.1.3. ***Passage entre anneaux***
Soient A, A' deux anneaux dans $\mathcal{F}$. Alors il existe $a \in A^H$, $a' \in A'^H$ avec $A[a^{-1}] = A'[a'^{-1}]$.

Preuve. A' étant une k-algèbre de type fini ($P2$), considérons $a'_1, \ldots, a'_s$ une famille de générateurs. D'après la propriété $P1$ appliquée à A, on peut écrire $a'_i = x_i/c_i$ avec x_i, c_i dans A. Considérons le produit $c = \prod_{i=1}^{s} c_i$, et soit $b = \prod_{\sigma \in H} \sigma(c)$. On vérifie sans peine que $b \in A^H$, $a'_i \in A[b^{-1}]$ et par conséquent $A' \subset A[b^{-1}]$.
Il suffit maintenant de montrer le lemme pour $A[b^{-1}]$ et A'. En effet, si on suppose

le lemme montré pour A' et $A[b^{-1}]$ avec $b \in A^H$, en choisissant $a \in A[b^{-1}]^H$, $a' \in A'^H$ tels que $A[b^{-1}][a^{-1}] = A'[a'^{-1}]$ et en écrivant a sous la forme d/b^n avec $d \in A^H$, on a $A[b^{-1}][a^{-1}] = A[(bd)^{-1}]$.
On peut donc supposer que $A' \subset A$. En inversant les rôles de A et A' dans le raisonnement précédent, on trouve un élément $a \in A'^H$ tel que $A \subset A'[a^{-1}]$. Notons que $a \in A^H$. En remarquant de plus que $A'[a^{-1}] \subset A[a^{-1}]$ (car $A' \subset A$) et que $A[a^{-1}] \subset A'[a^{-1}]$ (car $A \subset A'[a^{-1}]$), on déduit que $A[a^{-1}] = A'[a^{-1}]$. □

Le lemme précédent nous permet de passer de $A[a^{-1}]$ à $A'[a'^{-1}]$ pour a et a' bien choisis. Le lemme suivant nous permettra de passer de A à $A[a^{-1}]$ et de A' à $A'[a'^{-1}]$:

Lemme 3.1.4. ***Une suite exacte***
Soit A un anneau dans $\mathcal{F}$. Soit $a \in A^H$ non nul. Alors il existe une suite exacte

$$0 \longrightarrow A^* \longrightarrow A[a^{-1}]^* \longrightarrow P \longrightarrow 0$$

où P est un module de permutation de type fini sur $\mathbb{Z}[H]$.
De plus, $A[a^{-1}]$ est dans $\mathcal{F}$.
Corollaire immédiat: la suite

$$0 \longrightarrow A^*/k^* \longrightarrow A[a^{-1}]^*/k^* \longrightarrow P \longrightarrow 0$$

est exacte.

Preuve. Établissons d'abord la suite exacte. Pour cela, nous allons construire une application de $A[a^{-1}]^*$ dans P après avoir bien choisi P.
Notons $(p_i)_{1 \leq i \leq r}$ les diviseurs irréductibles de a dans A (non associés) et écrivons $a = up_1^{v_1} \dots p_r^{v_r}$ avec u une unité de A, v_i entiers strictement positifs. Comme $a \in A^H$, $\forall \sigma \in H$, $a = \sigma(a) = \sigma(u)\sigma(p_1)^{v_1} \dots \sigma(p_r)^{v_r}$. L'anneau A étant factoriel, par unicité de la factorisation de a, nous déduisons que les idéaux premiers (p_i) sont permutés par H.
Faisons correspondre à chaque idéal (p_i) un élément e_i et considérons le module de permutation P de base $e_1, \dots, e_r$, de telle sorte que H agit sur cette base de la même façon que sur les idéaux premiers $(p_i)_{1 \leq i \leq r}$. Définissons ensuite l'application de $A[a^{-1}]^*$ dans P, en envoyant p_i sur e_i, i.e. en envoyant $x \in A[a^{-1}]^*$ sur $\sum val_{p_i}(x)e_i$. C'est un morphisme de $\mathbb{Z}[H]$-modules. Un élément $a^{-n}p_1^{m_1} \dots p_r^{m_r}$ dans $A[a^{-1}]^*$ avec n, m_i entiers positifs a pour image $\sum(m_i - n.v_i)e_i$ dans P. Comme tous les v_i sont strictement positifs, cette application est surjective.
Cherchons son noyau. Un élément $y = a^{-n}x$ de $A[a^{-1}]^*$ avec n entier positif est dans le noyau si et seulement si $val_{p_i}(a^{-n}x) = 0$, $\forall i \in I$. Dans ce cas, $val_{p_i}(a^n) = val_{p_i}(x)$ pour tout $i \in I$, et il vient du caractère factoriel de l'anneau A que $a^n \mid x$, donc $y \in A$. Le même raisonnement marche pour y^{-1}, donc $y^{-1} \in A$

et y est inversible dans A.
On vient de démontrer que l'application surjective qu'on a construite a pour noyau A^*. D'où l'exactitude de la suite

$$0 \longrightarrow A^* \longrightarrow A[a^{-1}]^* \longrightarrow P \longrightarrow 0$$

On en déduit immédiatement l'exactitude de la suite

$$0 \longrightarrow A^*/k^* \longrightarrow A[a^{-1}]^*/k^* \longrightarrow P \longrightarrow 0$$

Montrons à présent que $A[a^{-1}]$ vérifie les propriétés $P1$ à $P5$.
$P1$, $P2$ et $P3$ sont trivialement satisfaites par $A[a^{-1}]$.
$P4$: Notons $(p_i)_{i\in I}$ les diviseurs irréductibles de a dans A, $(p_j)_{j\in J}$ les autres éléments irréductibles de A. Les $(p_j)_{j\in J}$ sont exactement les éléments irréductibles de $A[a^{-1}]$ (à unité près). Prenons un élément d/a^n dans $A[a^{-1}]$, avec $d \in A$. On obtient l'existence de la factorisation en factorisant d dans A, et l'unicité découlde de celle de A.
Donc $A[a^{-1}]$ est dans $\mathcal{F}$. □

Nous sommes à présent en mesure de définir le premier invariant. Cependant, nous avons préalablement besoin de définir le groupe de Grothendieck:

Définition 3.1.5. ***Groupe de Grothendieck***
On définit le ***groupe de Grothendieck*** *de la catégorie des $\mathbb{Z}[H]$-modules de type fini de la façon suivante:*
Soit S le groupe abélien libre dont une base est donnée par les symboles $[A]$, où A décrit les classes d'isomorphisme de $\mathbb{Z}[H]$-modules de type fini. Soit R le sous-groupe engendré par tous les élément de la forme $[A]+[C]-[B]$ dès que A, B, C s'inscrivent dans une suite exacte

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

Le groupe de Grothendieck est alors défini comme le quotient S/R.

Notons $K_0(H)$ le groupe de Grothendieck de la catégorie des $\mathbb{Z}[H]$-modules de type fini. La suite exacte dans le lemme précédent nous incite à nous intéresser à ce groupe. Afin de prendre en compte le fait que P est un module de permutation, nous considérons le quotient de $K_0(H)$ par le sous-groupe engendré par tous les modules de permutation P. Notons $Sw(H)$ le groupe ainsi construit. Alors de tout ce qui a été vu jusqu'ici découle un invariant:

Théorème 3.1.6. ***Invariant dans le groupe*** $Sw(H)$
L'image de A^*/k^* dans $Sw(H)$ ne dépend pas du choix de l'anneau A vérifiant les propriétés $P1$ à $P5$.

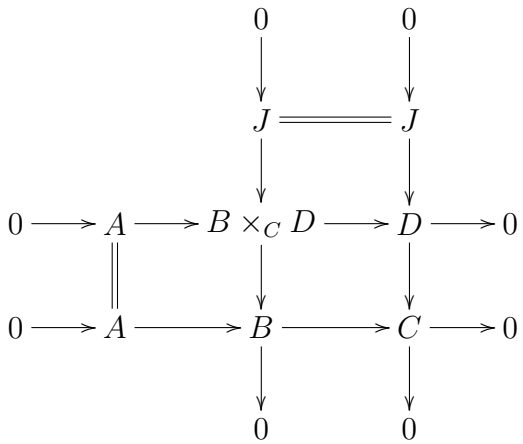
Preuve. Soient A et A' deux anneaux dans $\mathcal{F}$. Choisissons a et a' comme dans le lemme 3.1.3. La suite exacte du lemme 3.1.4 donne alors immédiatement les relations $[A^*/k^*] = [A[a^{-1}]^*/k^*]$ et $[A'^*/k^*] = [A'[a'^{-1}]^*/k^*]$ dans $Sw(H)$. Comme de plus $A[a^{-1}]^* = A'[a'^{-1}]^*$, on a $[A^*/k^*] = [A'^*/k^*]$ dans $Sw(H)$. □

3.2 Construction d'un deuxième invariant dans le groupe des classes

On suppose à présent que H est un groupe cyclique d'ordre n. Soit σ un générateur. Soit ϕ_n le n-ième polynôme cyclotomique. Considérons l'anneau $O = \mathbb{Z}[H]/(\phi_n(\sigma))$. Isomorphe à $\mathbb{Z}[\zeta]$ où ζ est une racine primitive n-ième de l'unité, d'après la proposition 2.2.6, c'est un anneau de Dedekind. Soit M un O-module de type fini. Alors, d'après l'étude des modules de type fini sur un anneau de Dedekind développée dans la section 2.1.3, on peut écrire $M \cong N \oplus I \oplus \bigoplus_{i=1}^{q} O/\Pi_i^{\alpha_i}$, où N est libre, I est un idéal de O et les Π_i sont des idéaux premiers non nuls de O. Notons $J = \Pi_1^{\alpha_1}...\Pi_q^{\alpha_q}$. On définit alors la **classe de M**, notée $c(M)$, par la classe de IJ^{-1} dans le groupe des classes défini en 2.1.2 si $I \neq 0$, celle de J^{-1} sinon. Il est immédiat que la classe est compatible avec la somme directe, au sens où $c(M \oplus M') = c(M)c(M')$: en effet, si $M \cong N \oplus I \oplus \bigoplus_{i=1}^{q} O/\Pi_i^{\alpha_i}$ et $M' \cong N' \oplus I' \oplus \bigoplus_{i=1}^{q'} O/\Pi_i'^{\alpha_i'}$ avec N et N' libres, alors $M \oplus M' \cong N \oplus N' \oplus O \oplus II' \oplus \bigoplus_{i=1}^{q} O/\Pi_i^{\alpha_i} \oplus \bigoplus_{i=1}^{q'} O/\Pi_i'^{\alpha_i'}$ en tenant compte du fait que $I \oplus I' \cong O \oplus II'$. Cependant, la compatibilité de la classe avec les suites exactes est beaucoup moins triviale et s'exprime ainsi:

Proposition 3.2.1. ***Compatibilité de la classe avec les suites exactes*** *Soit* $0 \to A \to B \to C \to 0$ *une suite exacte de* O*-modules. Alors* $c(B) = c(A)c(C)$.

Preuve. Écrivons $C = N \oplus I \oplus \bigoplus_{i=1}^{q} O/\Pi_i^{\alpha_i}$, où N est libre, et notons $J = \prod_{i=1}^{q} \Pi_i^{\alpha_i}$ et $D = N \oplus O \oplus I$ puis considérons le diagramme suivant:



où $B \times_C D$ est le produit fibré de B et D au-dessus de C. Il est facile de voir que le diagramme est exact en lignes et en colonnes. Par définition de la classe, on a toujours $c(D) = c(J)c(C)$. Comme la classe est compatible avec la somme directe, comme D est sans torsion (et donc projectif), $c(B \times_C D) = c(A)c(D)$. Si de plus B est sans torsion, on a $c(B \times_C D) = c(J)c(B)$, et les trois relations trouvées entre les classes imposent que $c(B) = c(A)c(C)$. Donc la proposition 3.2.1 est vraie dès que B est sans torsion. Maintenant, si l'on ne suppose rien pour B mais on suppose que A est sans torsion, alors $B \times_C D \cong A \oplus D$ est sans torsion, et donc $c(B \times_C D) = c(J)c(B)$. On conclut que la proposition 3.2.1 est vraie dès que A est sans torsion. Finalement, si l'on ne suppose rien, on déduit de ce qui précède que $c(B \times_C D) = c(J)c(B)$ puisque J est sans torsion. La proposition est donc prouvée en toute généralité. □

Pour un $\mathbb{Z}[H]$-module M, nous considérons le O-module $M^{\phi_n(\sigma)} = \{m \in M, \phi_n(\sigma)m = 0\}$. Nous pouvons alors énoncer le lemme suivant qui établit une compatibilité partielle avec les suites exactes de $\mathbb{Z}[H]$-modules:

Lemme 3.2.2. ***Compatibilité de la classe avec les suites exactes de*** $\mathbb{Z}[H]$***-modules***
Soit P un $\mathbb{Z}[H]$-module de permutation.

(i) $P^{\phi_n(\sigma)}$ est un O-module libre.

(ii) Si $0 \to M \to N \to P \to 0$ est une suite exacte de $\mathbb{Z}[H]$-modules, alors $0 \to M^{\phi_n(\sigma)} \to N^{\phi_n(\sigma)} \to P^{\phi_n(\sigma)} \to 0$ est une suite exacte de O-modules.

Preuve.

(i) P étant un module de permutation, on peut écrire $P \cong \mathbb{Z}[H]^r \oplus \bigoplus_i \mathbb{Z}[H/H_i]$, où les H_i sont des sous-groupes de H non triviaux. Pour chaque i, si $d = [H : H_i]$, alors $(\sigma^d - 1)\mathbb{Z}[H/H_i] = 0$. Or on a aussi $\phi_n(\sigma)\mathbb{Z}[H/H_i]^{\phi_n(\sigma)} = 0$. Donc, comme $(X^d - 1) \wedge \phi_n = 1$, grâce à l'identité de Bezout, $\mathbb{Z}[H/H_i]^{\phi_n(\sigma)} = 0$. D'autre part, soit $\psi_n \in \mathbb{Z}[X]$ tel que $X^n - 1 = \phi_n\psi_n$ et considérons $f : \mathbb{Z}[H] \to \mathbb{Z}[H]^{\phi_n(\sigma)}, x \mapsto \psi_n(\sigma)x$. L'application f est un morphisme de $\mathbb{Z}[H]$-modules, dont le noyau est $\phi_n(\sigma)\mathbb{Z}[H]$ et dont l'image est $\mathbb{Z}[H]^{\phi_n(\sigma)}$ tout entier. En effet, il existe des polynômes à coefficients entiers A et B et un entier non nul m tels que $A\phi_n + B\psi_n = m$, et $\mathbb{Z}[X]/(\phi_n)$ et $\mathbb{Z}[X]/(\psi_n)$ sont des groupes sans torsion, donc l'annulateur de $\phi_n(\sigma)$ est $(\psi_n(\sigma))$ et l'annulateur de $\psi_n(\sigma)$ est $(\phi_n(\sigma))$. Donc $\mathbb{Z}[H]^{\phi_n(\sigma)} \cong \mathbb{Z}[H]/\phi_n(\sigma)\mathbb{Z}[H]$. Par conséquent, $P^{\phi_n(\sigma)} \cong O^r$.

(ii) Notons $P_1 = \mathbb{Z}[H]^r$ et $P_2 = \bigoplus_i \mathbb{Z}[H/H_i]$. Soit N_2 l'image réciproque de P_2 dans N. On a alors les suites exactes de $\mathbb{Z}[H]$-modules:

$$0 \to N_2 \to N \to P_1 \to 0$$
$$0 \to M \to N_2 \to P_2 \to 0$$

P_1 étant libre, la première suite exacte donne $N \cong N_2 \oplus P_1$, donc $N^{\phi_n(\sigma)} = N_2^{\phi_n(\sigma)} \oplus P_1^{\phi_n(\sigma)}$. La deuxième suite exacte permet d'établir $0 \to M^{\phi_n(\sigma)} \to N_2^{\phi_n(\sigma)} \to P_2^{\phi_n(\sigma)} = 0$ d'après (i), donc $M^{\phi_n(\sigma)} \cong N_2^{\phi_n(\sigma)}$. On en déduit alors que $0 \to M^{\phi_n(\sigma)} \to N^{\phi_n(\sigma)} \to P^{\phi_n(\sigma)} \to 0$ est une suite exacte de O-modules.

□

Le lemme précédent montre alors que $N^{\phi_n(\sigma)} \cong M^{\phi_n(\sigma)} \oplus P^{\phi_n(\sigma)}$ et que $c(M^{\phi_n(\sigma)}) = c(N^{\phi_n(\sigma)})$. Nous sommes à présent en mesure de définir l'invariant de Swan, qui va jouer un rôle majeur dans la suite:

Théorème 3.2.3. ***Invariant dans le groupe des classes***
La classe $c((A^*/k^*)^{\phi_n(\sigma)})$ est indépendante du choix de l'anneau A vérifiant les conditions (P1) à (P5).

Preuve. Soient A et A' deux anneaux vérifiant les conditions (P1) à (P5). D'après le lemme 3.1.3, il existe a et a' dans A^H et A'^H tels que $A[a^{-1}] = A'[a'^{-1}]$. Notons $B = A[a^{-1}] = A'[a'^{-1}]$. Alors, d'après le lemme 3.1.4, on a les suites exactes de $\mathbb{Z}[H]$-modules suivantes:

$$0 \to A^*/k^* \to B^*/k^* \to P \to 0$$
$$0 \to A'^*/k^* \to B^*/k^* \to P' \to 0$$

où P et P' sont des modules de permutation. Donc le lemme 3.2.2 impose que $c((A^*/k^*)^{\phi_n(\sigma)}) = c((B^*/k^*)^{\phi_n(\sigma)}) = c((A'^*/k^*)^{\phi_n(\sigma)})$, d'où le théorème. □

Nous noterons à partir d'ici $\alpha(k, L, H) = c((A^*/k^*)^{\phi_n(\sigma)})$. Dans la suite, il s'agira de déterminer que cet invariant est toujours le même dès que le problème de Noether admet une réponse affirmative, puis de montrer qu'en choisissant judicieusement les paramètres du problème on obtient un invariant différent.

3.3 Le contre-exemple de Swan

Commençons par calculer l'invariant précédent dans le cas d'une extension transcendante pure.
Fixons p un entier premier de $\mathbb{Z}$: ultérieurement, on prendra $p = 47$. Soit k_0 un corps, qui sera pris égal à $\mathbb{Q}$ plus tard. Notons k le corps obtenu à partir de k_0 par adjonction des racines p-ièmes de l'unité. On suppose que $[k : k_0] = p - 1$, ce qui est évidemment vérifié lorsque $k_0 = \mathbb{Q}$. Soit $K_0 = k_0(x_1, \ldots, x_p)$ le corps des fractions rationnelles sur k_0.
Soit G le groupe cyclique d'ordre p qui opère sur K_0 en permutant circulairement

$x_1, \ldots, x_p$. On note $L_0 = K_0^G$ le corps fixe sous l'action de G. Notons K et L les corps obtenus à partir de K_0 et L_0 respectivement par adjonction des racines p-ièmes de l'unité. Il est alors clair que $[K : K_0] = [L : L_0] = p - 1$. On choisit ensuite pour H le groupe de Galois de K/K_0, qui est canoniquement isomorphe aux groupes de Galois de L/L_0 et de k/k_0 par restriction. H est alors le groupe cyclique à $n = p - 1$ éléments.

Théorème 3.3.1. ***Cas d'une extension transcendante pure***
Si L_0/k_0 est une extension transcendante pure, alors on a $\alpha(k, L, H) = 1$.

Preuve. Si $L_0 = k_0(y_1, \ldots, y_p)$, avec les y_i algébriquement indépendants sur k_0, alors en prenant $A = k[y_1, \ldots, y_p]$, A vérifie les conditions $P1$ à $P5$. Or A^*/k^* n'est autre que l'élément neutre, on a donc par définition $\alpha(k, L, H) = 1$. □

Par conséquent, pour montrer qu'une extension n'est pas transcendante pure, il suffit de calculer $\alpha(k, L, H)$ et de voir que l'on n'obtient pas 1, ce qui revient à voir qu'un certain idéal n'est pas principal. Pour cela, nous aurons besoin du lemme suivant:

Lemme 3.3.2. ***47 est un nombre magique***
Si ζ est une racine primitive 46-ième de l'unité, et $\mathfrak{p}$ un idéal premier de $\mathbb{Z}[\zeta]$ tel que $Card(\mathbb{Z}[\zeta]/\mathfrak{p}) = 47$, alors $\mathfrak{p}$ n'est pas principal.

Preuve. La preuve est basée sur l'étude de la norme relative de l'idéal $\mathfrak{p}$ (section 2.1.3).
Raisonnons par l'absurde.
Tout d'abord, d'après le théorème 2.2.9, on sait que $\mathbb{Z}[\zeta]$ est la clôture intégrale de $\mathbb{Z}$ dans le corps k. Ce corps contient le corps $\mathbb{Q}(\sqrt{-23})$. En effet, si ξ est une racine primitive 23-ème de l'unité, on remarque que

$$\phi_{23}(1) = 23 = \prod_{i=1}^{22}(1 - \xi^i) = \prod_{i=1}^{11}(1 - \xi^i)(1 - \xi^{23-i}) = -\xi^{-66}\left(\prod_{i=1}^{11}(\xi^i - 1)\right)^2$$

et on a donc bien que $\sqrt{-23} \in k$.
Comme $\mathbb{Q}(\sqrt{-23})$ est un corps quadratique avec $-23 \equiv 1$ [4], le théorème 2.2.11 impose que l'anneau des entiers de $\mathbb{Q}(\sqrt{-23})$ est engendré par 1 et $\frac{1+\sqrt{-23}}{2}$.
Si $\mathfrak{p}$ était principal, sa norme relativement à $\mathbb{Q}(\sqrt{-23})$ serait encore un idéal principal (α) d'après la proposition 2.3.4. Si $\alpha = \frac{x+y\sqrt{-23}}{2}$ ($x \equiv y$ [2]), on a $N_{\mathbb{Q}(\sqrt{-23})/\mathbb{Q}}(\alpha) = \frac{x^2+23y^2}{4}$. De plus, avec la proposition 2.3.5, on a $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\mathfrak{p}) = 47$. La proposition 2.3.2 impose alors $47 = \frac{x^2+23y^2}{4}$. En examinant les cas où $|y| = 0, 1, 2$, on remarque que l'équation précédente n'a pas de solutions, d'où la contradiction. □

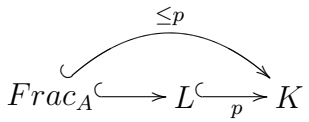
La définition suivante sera utile dans la suite:

Définition 3.3.3. ***Résolvantes de Lagrange***
Soit ω une racine p-ième de l'unité. On appelle ***résolvantes de Lagrange*** *les y_i définis par: $\forall i \in \{0, 1, \ldots, p-1\}$, $y_i = \sum_{j=1}^{p} \omega^{-ij} x_j$.*

Nous sommes à présent en mesure d'établir le contre-exemple de Swan:

Théorème 3.3.4. ***Contre-exemple de Swan***
On prend $p = 47$, $k_0 = \mathbb{Q}$, G le groupe $\mathbb{Z}/47\mathbb{Z}$ agissant sur les x_i par permutation cyclique, $K_0 = \mathbb{Q}(x_1, \ldots, x_{47})$. Alors L_0, le corps des fractions rationnelles invariantes par G, n'est pas une extension transcendante pure de $\mathbb{Q}$.

Preuve. Rappelons que nous avons choisi pour H le groupe de Galois de K/K_0 isomorphe aux groupes de Galois de L/L_0, k/k_0: il est cyclique d'ordre $n = p-1$. Notons y_i les résolvantes de Lagrange définies précédemment, pour i allant de 0 à $p-1$. On remarque que les actions de G et H sur K commutent. Le groupe H fixe y_0 et le sous-$\mathbb{Z}$-module M' de K^* de base $y_1, \ldots, y_{p-1}$ est libre sur $\mathbb{Z}[H]$. En effet, H permute (transitivement) les y_i et donc ce module est monogène (engendré par y_1) sur $\mathbb{Z}[H]$. On utilise bien sûr ici que la matrice de Van der Monde qui traduit le changement de variables donné par les résolvantes de Lagrange est inversible.
On considère ensuite le sous-module M de M' défini par $M = M' \cap L^*$. On va montrer que M est un sous-module d'indice p de M'. Par un calcul simple on voit que y_1^p et $y_1^{-i} y_i$ sont des éléments de M. Ils engendrent un sous-module d'indice p de M'. Si c'est M, il n'y a rien à montrer. Sinon, $M = M'$ donc $M' \subset L^*$ ce qui est absurde puisque y_1 n'est pas dans L. Donc M est un sous-module d'indice p de M'. On voit aussi que M est de rang $p-1$ en tant que $\mathbb{Z}$-module. Soit $m_1, \ldots, m_{p-1}$ une base de M.
Maintenant considérons A l'anneau $k[y_0, m_1, \ldots, m_{p-1}, m_1^{-1}, \ldots, m_{p-1}^{-1}]$, alors A vérifie les propriété $P1$ à $P5$. En effet, la seule difficulté est de montrer que le corps des fractions de A est L. Pour cela, on utilise que le degré de l'extension K/L est p (car l'extension est galoisienne), et on va le comparer au degré de K sur le corps des fractions de A (noté $Frac_A$). Mais $K = k(y_0, m_1, \ldots, m_{p-1}, m_1^{-1}, \ldots, m_{p-1}^{-1})(y_1)$, donc le degré d'extension de ce dernier sur $k(y_0, m_1, \ldots, m_{p-1}, m_1^{-1}, \ldots, m_{p-1}^{-1})$ est au plus p. Mais alors on a



ce qui montre que $L = k(y_0, m_1, \ldots, m_{p-1}, m_1^{-1}, \ldots, m_{p-1}^{-1})$, le corps des fractions de A. On remarque aussi que A^*/k^* est égal à M.

Par définition du second invariant, $\alpha(k, L, H) = c(M^{\phi_n(\sigma)})$. En regardant la suite exacte

$$0 \longrightarrow M^{\phi_n(\sigma)} \longrightarrow M'^{\phi_n(\sigma)} \longrightarrow M'^{\phi_n(\sigma)}/M^{\phi_n(\sigma)} \longrightarrow 0$$

on a $\alpha(k, L, H) = c(M'^{\phi_n(\sigma)}/M^{\phi_n(\sigma)})^{-1}$ par compatibilité de la classe avec les suites exactes (proposition 3.2.1 et proposition 3.2.2). Le module M étant un sous-module d'indice p de M', $M^{\phi_n(\sigma)}$ est un sous-O-module d'indice 1 ou p de $M'^{\phi_n(\sigma)}$. Montrons que $M^{\phi_n(\sigma)} \neq M'^{\phi_n(\sigma)}$. Pour ce faire, on va construire un élément annulé par $\phi_n(\sigma)$ dans M' mais qui n'est pas dans M. Regardons par exemple l'élément

$$T = \prod_{d|n, d\neq n} (\sigma^d - 1) \in \mathbb{Z}[H]$$

Alors $T.y_1$ est annulé par $\phi_n(\sigma)$. Montrons que son image dans M'/M est non nulle. On sait que M'/M est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, engendré par y_1, et l'action de σ sur M'/M est une multiplication par r où r est l'élément dans $\mathbb{Z}/p\mathbb{Z}$ tel que $\sigma(\omega) = \omega^r$. Donc T agit sur M'/M par multiplication par l'élément de $\mathbb{Z}/p\mathbb{Z}$

$$\prod_{d|n, d\neq n} (r^d - 1)$$

qui est non nul car l'ordre de r dans $(\mathbb{Z}/p\mathbb{Z})^*$ est n. Par conséquent T est injectif et donc $T.y_1$ est non nul.
Donc $M^{\phi_n(\sigma)}$ est un sous-O-module d'indice p de $M'^{\phi_n(\sigma)} \cong O$. Par conséquent, $M'^{\phi_n(\sigma)}/M^{\phi_n(\sigma)}$ est isomorphe à un quotient $\mathbb{Z}[\zeta]/\mathfrak{p}$, $\mathfrak{p}$ idéal premier, et donc $\alpha(k, L, H) = 1$ si, et seulement si, $\mathfrak{p}$ est principal. Or, avec $p = 47$, la propriété "47 est un nombre magique" (proposition 3.3.2) impose immédiatement que $\mathfrak{p}$ n'est pas principal. □

4 Résolution du problème de Noether pour un groupe abélien

4.1 Un peu de cohomologie des groupes finis

Dans la suite, nous aurons besoin de définir quelques notions de cohomologie des groupes. Soit G un groupe fini, et définissons:

Définition 4.1.1. *H^1 et $\widehat{H}^{-1}$*
Soit M un $\mathbb{Z}[G]$-module. Soit $N : M \to M, m \mapsto \sum_{g\in G} gm$. Soit I_G l'idéal de $\mathbb{Z}[G]$ engendré par les éléments de la forme $g-1$, pour $g \in G$. Alors on définit les groupes:

$$H^1(G, M) = \frac{\{f : G \to M | \forall g, g' \in G, f(gg') = gf(g') + f(g)\}}{\{G \to M, g \mapsto ga - a; a \in M\}}$$

$$\widehat{H}^{-1}(G,M) = KerN/I_GM$$

Considérons $0 \to A \to B \to C \to 0$ une suite exacte de $\mathbb{Z}[G]$-modules. Il est alors immédiat que la suite $0 \to A^G \to B^G \to C^G$ est exacte, mais la dernière flèche n'est pas nécessairement surjective. Le groupe H^1 permet alors de compléter cette suite, comme l'exprime la proposition suivante:

Proposition 4.1.2. ***Suite exacte de cohomologie***
Soit $0 \to A \to B \to C \to 0$ une suite exacte de $\mathbb{Z}[G]$-modules. Alors il existe une application canonique $C^G \to H^1(G,A)$ telle que la suite $0 \to A^G \to B^G \to C^G \to H^1(G,A) \to H^1(G,B)$ est une suite exacte de $\mathbb{Z}[G]$-modules.

Preuve. Soit $\pi : B \to C$ la projection. On considère $\psi : C^G \to H^1(G,A), c \mapsto (g \mapsto gb - b)$ où b est un élément de B tel que $\pi(b) = c$ et $i : H^1(G,A) \to H^1(G,B)$ l'application canonique. On vérifie immédiatement que l'image de c par ψ ne dépend pas du choix de b, puis que, comme $\pi(gb-b) = g\pi(b) - \pi(b) = gc - c = 0$, on a bien $gb - b \in A$. ψ est donc bien définie. L'exactitude de la suite proposée est alors facile à établir. □

On énonce maintenant un théorème classique connu sous le nom du "théorème de Hilbert 90" qui sera utile dans la suite:

Théorème 4.1.3. ***Théorème de Hilbert 90***
Soit L/K une extension galoisienne finie de groupe de Galois $G = Gal(L/K)$. Alors $H^1(G, L^*) = 0$.

Preuve. Les opérations sont notées multiplicativement dans cette preuve. Soit $f : G \to L^*$ une application non nulle telle que $f(gg') = gf(g') \cdot f(g)$. On veut trouver un élément c dans L^* tel que $f(g) = gc \cdot c^{-1}$. On considère pour cela un élément b de la forme $b = \sum_{g \in G} f(g) \cdot g(a)$ avec $a \in L^*$ que l'on déterminera ultérieurement. Un calcul montre que $\forall g \in G$, $gb = f(g)^{-1}b$. Si $b \neq 0$, alors, en posant $c = b^{-1}$, on a $\forall g \in G$, $f(g) = gc \cdot c^{-1}$.
Reste à montrer que l'on peut choisir $a \in L^*$ tel que $b \neq 0$. Autrement dit il suffit de voir que l'application $a \mapsto \sum_{g \in G} f(g) \cdot g(a)$ soit non nulle. Ceci résulte de l'indépendance linéaire des automorphismes de corps. □

Pour terminer, nous aurons besoin du lemme de Shapiro, que nous admettrons:

Lemme 4.1.4. ***Lemme de Shapiro***
Soient H un sous-groupe de G et M un $\mathbb{Z}[H]$-module. Nous pouvons munir $Hom_{\mathbb{Z}[H]}(\mathbb{Z}[G], M)$ d'une structure de $\mathbb{Z}[G]$-module par:

$$(gf)(a) = f(ag) \text{ pour } g \in G \text{ et } f \in Hom_{\mathbb{Z}[H]}(\mathbb{Z}[G], M) \text{ et } a \in \mathbb{Z}[G].$$

Alors on a l'isomorphisme

$$H^1(G, Hom_{\mathbb{Z}[H]}(\mathbb{Z}[G], M)) \cong H^1(H, M)$$

4.2 Notations, objectif et stratégie

Considérons un corps k et G un groupe abélien fini qui agit sur $k(\{x_g, g \in G\})$ par permutation des variables. Notons $k_G = k(\{x_g, g \in G\})^G$. On cherche à établir une condition nécessaire et suffisante pour que k_G soit une extension transcendante pure de k.
Étant donné un groupe cyclique ρ d'ordre m et de générateur τ, on définit $\mathbb{Z}(\rho) = \mathbb{Z}[\rho]/\Phi_m(\tau)\mathbb{Z}[\rho]$. C'est un anneau de Dedekind isomorphe à $\mathbb{Z}[\zeta_m]$, où ζ_m est une racine primitive m-ième de l'unité. Remarquons que cet anneau est indépendant du choix de τ.
Notons à présent k_c l'extension cyclotomique maximale de k dans une clôture algébrique. Donnons-nous un sous-corps K de k_c contenant k tel que $\rho_K = Gal(K/k)$ est cyclique, de générateur τ_K. Soient $\mathbb{P}$ l'ensemble des nombres premiers et $T = (\mathbb{P} - \{2, car(k)\}) \times \mathbb{N}^*$. Pour $(p, s) \in T$, on définit l'idéal $\mathfrak{a}_K(p^s)$ de $\mathbb{Z}(\rho_K)$ par:

$$\mathfrak{a}_K(p^s) = \mathbb{Z}(\rho_K) \text{ si } K \neq k(\zeta_{p^s})$$
$$\mathfrak{a}_K(p^s) = (\tau_K - t, p) \text{ si } K = k(\zeta_{p^s}) \text{ et } t \in \mathbb{Z} \text{ vérifie } \tau_K(\zeta_p) = \zeta_p^t$$

Remarquons que cette définition est indépendante du choix de τ_K.
On définit alors pour un groupe abélien fini H:

$$\mathfrak{a}_K(H) = \prod_{(p,s)\in T} \mathfrak{a}_K(p^s)^{m(H,p,s)}$$

où $m(H, p, s) = dim_{\mathbb{Z}/p\mathbb{Z}}(p^{s-1}H/p^sH)$.
Notons finalement $v(G)$ la plus grande puissance de 2 divisant l'exposant de G.
Nous sommes maintenant en mesure d'énoncer le théorème de Lenstra:

Théorème 4.2.1. ***Théorème de Lenstra***
Avec les définitions et notations précédentes, k_G est une extension transcendante pure de k si, et seulement si, les deux assertions suivantes sont vérifiées:

(i) quel que soit le sous-corps K de k_c contenant k tel que ρ_K est cyclique, $\mathfrak{a}_K(G)$ est principal.

(ii) Si $car(k) \neq 2$, alors $k(\zeta_{v(G)})$ est une extension cyclique de k.

La démonstration de ce théorème est délicate et longue. Décrivons la stratrégie suivie.
Dans un premier temps (parties 4.3 et 4.4), nous allons nous essayer d'établir des

liens entre les modules de permutation et les extemsions transcendantes pures, afin de montrer le théorème 4.4.6. Ensuite, dans un deuxième temps, afin de relier la nature de l'extension $k_G|k$ à l'idéal $\mathfrak{a}_K(G)$, nous allons construire un module F_ρ puis nous allons relier F_ρ à l'extension $k_G|k$ (partie 4.5 théorème 4.5.8) et aux idéaux de la forme $\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z})$ (partie 4.6 théorème 4.6.7). Pour ce faire, nous aurons besoin d'introduire dans la partie 4.6 deux modules que nous appellerons I_q et J_q et qui joueront aussi un rôle important dans les parties suivantes. Après cela, dans la partie 4.7, le théorème 4.7.4 nous permettra d'éviter tous les problèmes de caractéristique, en particulier la situation problématique où $car(k)$ divise $|G|$. Finalement, la partie 4.8 permettra de montrer le théorème de Lenstra en établissant d'abord quelques isomorphismes de corps puis en combinant tous les résultats vus jusque là.
L'énoncé du théorème de Lenstra n'est pas particulièrement simple ni joli. Il est assez difficile à appréhender et assez technique. Cependant, il est puissant et il permet d'obtenir de très belles conséquences, en particulier dans le cas où G est cyclique. Nous donnerons quelques-unes de ces conséquences dans la partie 5.

4.3 Facteurs directs de permutation

Soit π un groupe fini. En nous inspirant de la définition des modules projectifs, nous posons la définition suivante:

Définition 4.3.1. ***Facteurs directs de permutation***
On dit qu'un $\mathbb{Z}[\pi]$-module P est un ***facteurs directs de permutation*** *s'il existe un $\mathbb{Z}[\pi]$-module P' tel que $P \oplus P'$ est un module de permutation.*

Intéressons-nous d'abord à la cohomologie des facteurs directs de permutation:

Proposition 4.3.2. ***Cohomologie des facteurs directs de permutation***
Soit P un $\mathbb{Z}[\pi]$-module, facteur direct de permutation. Soit ρ un sous-groupe de π. Alors $H^1(\rho, P) = \widehat{H}^{-1}(\rho, P) = 0$.

Preuve. Comme P est un $\mathbb{Z}[\rho]$-module facteur direct de permutation, on peut supposer $\rho = \pi$. Il existe alors P' tel que $P \oplus P'$ est une somme directe de modules de la forme $\mathbb{Z}[\pi/\pi']$, pour π' sous groupe de π. On peut donc supposer que $P = \mathbb{Z}[\pi/\pi']$. En appliquant le lemme de Shapiro (4.1.4), on obtient que $H^1(\pi, P) = H^1(\pi, Hom_{\mathbb{Z}[\pi']}(\mathbb{Z}[\pi], \mathbb{Z})) = H^1(\pi', \mathbb{Z}) = 0$.
D'autre part, on vérifie facilement à la main que $KerN = I_\rho P$, où $N : P \to P, p \mapsto \sum_{g\in\rho} gp$ et I_ρ est l'idéal de $\mathbb{Z}[\rho]$ engendré par les éléments de la forme $g - 1$, pour $g \in \rho$. Donc $\widehat{H}^{-1}(\rho, P) = 0$. □

On peut alors énoncer les caractérisations suivantes des facteurs directs de permutation:

Proposition 4.3.3. ***Caractérisations des facteurs directs de permutation*** *Soit P un $\mathbb{Z}[\pi]$-module. Les propositions suivantes sont équivalentes:*

(i) *P est un facteur direct de permutation.*

(ii) *Pour tout morphisme de $\mathbb{Z}[\pi]$-modules $f : P_1 \to P_2$ induisant des surjections $P_1^\rho \to P_2^\rho$ quel que soit le sous-groupe ρ de π, l'application induite $Hom_{\mathbb{Z}[\pi]}(P, P_1) \to Hom_{\mathbb{Z}[\pi]}(P, P_2)$ est surjective.*

(iii) *Si L est un $\mathbb{Z}[\pi]$-module tel que $H^1(\rho, L) = 0$ quel que soit ρ sous-groupe de π, alors toute suite exacte de $\mathbb{Z}[\pi]$-modules $0 \to L \to M \to P \to 0$ est scindée.*

Preuve. Supposons (i). Écrivons $S = P \oplus P'$ de telle sorte que S soit un module de permutation. Soit $f : P_1 \to P_2$ un morphisme de $\mathbb{Z}[\pi]$-modules induisant des surjections $P_1^\rho \to P_2^\rho$ quel que soit le sous-groupe ρ de π. Soit $h \in Hom_{\mathbb{Z}[\pi]}(P, P_2)$. Alors on peut prolonger h par 0 sur P', obtenant ainsi $\widehat{h} : S \to P_2$. Le module S s'écrit comme somme directe de facteurs de la forme $\mathbb{Z}[\pi/\rho]$, pour ρ sous-groupe de π. Considérons $N = \mathbb{Z}[\pi/\rho]$ un de ces facteurs. L'élément $\widehat{h}|_N(1)$ appartient à P_2^ρ: on peut donc choisir $x_0 \in P_1^\rho$ tel que $\widehat{h}|_N(1) = f(x_0)$. Posons alors $k(1) = x_0$ et prolongeons k par $\mathbb{Z}[\pi]$ linéarité à N. On a alors $\widehat{h}|_N = f \circ k$. Il est donc possible de trouver k' dans $Hom_{\mathbb{Z}[\pi]}(S, P_1)$ tel que $\widehat{h} = f \circ k'$. Il suffit alors de restreindre k' à P pour montrer que h est bien dans l'image de $Hom_{\mathbb{Z}[\pi]}(P, P_1) \to Hom_{\mathbb{Z}[\pi]}(P, P_2)$, d'où (ii).
Supposons (ii). Soient L un $\mathbb{Z}[\pi]$-module tel que $H^1(\rho, L) = 0$ quel que soit ρ sous-groupe de π et une suite exacte de $\mathbb{Z}[\pi]$-modules $0 \to L \to M \to P \to 0$. En écrivant la suite exacte de cohomologie, on obtient alors, pour tout sous-groupe ρ de π, l'exactitude de la suite $0 \to L^\rho \to M^\rho \to P^\rho \to 0$, donc $M^\rho \to P^\rho$ est surjective. Donc, avec (ii), $Hom_{\mathbb{Z}[\pi]}(P, M) \to Hom_{\mathbb{Z}[\pi]}(P, P)$ est surjective, ce qui permet immédiatement de scinder la suite $0 \to L \to M \to P \to 0$, d'où (iii).
Supposons (iii). Soit M le $\mathbb{Z}[\pi]$-module qui, en tant que groupe, est le groupe abélien libre de base $(e_p)_{p \in P}$ indexée par P, et sur lequel la multiplication par les éléments de $\mathbb{Z}[\pi]$ est donnée par: $\forall \lambda \in \pi, \forall p \in P, \lambda e_p = e_{\lambda p}$. On a alors une surjection naturelle $M \to P$, qui envoie e_p sur p, et M est un $\mathbb{Z}[\pi]$-module de permutation. Soit L le noyau de la surjection $M \to P$. Alors la suite $0 \to L \to M \to P \to 0$ est exacte, et, pour tout sous-groupe ρ de π, on a la suite exacte de cohomologie: $0 \to L^\rho \to M^\rho \to P^\rho \to H^1(\rho, L) \to H^1(\rho, B) = 0$, en tenant compte de la proposition précédente. Or la flèche $M^\rho \to P^\rho$ est clairement surjective, donc $H^1(\rho, L) = 0$. En appliquant (iii), on obtient que $M = L \oplus P$, et donc P est un facteur direct de permutation. □

Cette caractérisation rappelle celle des modules projectifs.

4.4 Liens entre les modules de permutation et les extensions transcendantes pures

Soit l un corps sur lequel π agit fidèlement par automorphismes de corps. Lorsque M est un $\mathbb{Z}[\pi]$-module, libre et de rang fini sur $\mathbb{Z}$, on fait agir π sur $l[M]$, l'anneau de groupe de M, par $\sigma(\sum_{m\in M}\lambda_m m)=\sum_{m\in M}\sigma(\lambda)\sigma(m)$, pour $\sigma\in\pi$, et $(\lambda_m)_{m\in M}$ une famille presque nulle d'éléments de l. On étend cette action à $l(M)$, corps des fractions de $l[M]$, par $\sigma(ab^{-1})=\sigma(a)\sigma(b)^{-1}$.

Proposition 4.4.1. ***Une base formée d'éléments fixes***
Soit V un l-espace vectoriel sur lequel π agit semi-linéairement, au sens où V est un $\mathbb{Z}[\pi]$-module tel que:

$$\forall v\in V,\forall\sigma\in\pi,\forall\lambda\in l,\sigma(\lambda v)=\sigma(\lambda)\sigma(v)$$

Alors il existe une base de V contenue dans V^π.

Preuve. Il suffit de montrer que toute forme linéaire sur V s'annulant sur V^π est nulle. Soit donc f une telle forme linéaire. Soit $v\in V$. Pour tout $\lambda\in l$, $\sum_{\sigma\in\pi}\sigma(\lambda v)\in V^\pi$, donc $0=f(\sum_{\sigma\in\pi}\sigma(\lambda v))=\sum_{\sigma\in\pi}f(\sigma v)\sigma(\lambda)$. Étant donné que les automorphismes de corps sont linéairement indépendants et que l'action de π est fidèle, on a $f(v)=0$, d'où le résultat. □

Nous allons à présent montrer un certain nombre de propriétés exprimant les liens entre les extensions transcendantes pures et les facteurs directs de permutation. Le premier résultat concerne les modules de permutation.

Proposition 4.4.2. ***Extension transcendante pure associée à un module de permutation***
Soit P un $\mathbb{Z}[\pi]$-module de permutation de type fini. Alors $l(P)^\pi/l^\pi$ est une extension transcendante pure.

Preuve. Considérons $(e_1,...,e_r)$ une $\mathbb{Z}$-base de P permutée par π. Soit V le sous-l-espace vectoriel de $l(P)$ engendré par $e_1,...,e_r$. La proposition précédente impose alors qu'il existe $f_1,...,f_r$ une base de V contenue dans V^π. On a alors $l(P)=l(f_1,...,f_r)$, et $(f_1,...,f_r)$ est une famille algébriquement libre sur l. Par conséquent, $l(P)^\pi=l^\pi(f_1,...,f_r)$, d'où le résultat. □

Le résultat suivant permet d'établir un isomorphisme de corps lorsqu'une certaine suite est exacte. Nous aurons besoin ici du théorème de Hilbert 90, démontré en 4.1.3:

Proposition 4.4.3. ***Suite exacte et isomorphisme***
Considérons $0\to M_1\to M_2\to P\to 0$ une suite exacte de $\mathbb{Z}[\pi]$-modules de type fini, libres en tant que groupes abéliens. On suppose de plus que P est un facteur direct de permutation. Alors les corps $l(M_2)^\pi$ et $l(M_1\oplus P)^\pi$ sont l^π-isomorphes.

Preuve. Notons $p : M_2 \to P$ la projection. On a une inclusion naturelle de $l(M_1)$ dans $l(M_2)$. Soit H le sous-groupe de $l(M_2)^*$ engendré par $l(M_1)^*$ et M_2. C'est un $\mathbb{Z}[\pi]$-module. Soit $f : H \to P$ définie par:

$$\forall \lambda \in l(M_1)^*, \forall m \in M_2, f(\lambda m) = p(m)$$

La suite

$$0 \longrightarrow l(M_1)^* \longrightarrow H \xrightarrow{f} P \longrightarrow 0$$

est alors exacte. Pour ρ sous-groupe de π, d'après le théorème de Hilbert 90, on a $H^1(\rho, l(M_1)^*) = H^1(Gal(l(M_1)|l(M_1)^\rho), l(M_1)^*) = 0$. D'après la caractérisation des facteurs directs de permutation (4.3.3), la suite exacte précédente est scindée. La section $P \to H$ permet alors de construire un isomorphisme entre $l(M_2)$ et $l(M_1 \oplus P)$ qui commute à l'action de π, d'où le résultat. □

On en déduit le corollaire suivant:

Corollaire 4.4.4. ***Suite exacte et extension transcendante pure***
Considérons $0 \to M_1 \to M_2 \to P \to 0$ une suite exacte de $\mathbb{Z}[\pi]$-modules de type fini, libres en tant que groupes abéliens. On suppose de plus que P est de permutation. Alors $l(M_2)^\pi$ est une extension transcendante pure de $l(M_1)^\pi$.

Preuve. D'après la proposition précédente, les corps $l(M_2)^\pi$ et $l(M_1 \oplus P)^\pi$ sont l^π-isomorphes. En appliquant la proposition 4.4.2, en prenant $l(M_1)$ comme corps de base, on obtient que $l(M_1 \oplus P)^\pi \cong l(M_1)(P)^\pi$ est une extension transcendante pure de $l(M_1)^\pi$, d'où le résultat. □

Nous sommes à présent en mesure d'énoncer le théorème central de cette partie. Pour le montrer, nous ferons appel à des résultats montrés dans la partie 3, afin d'établir le contre-exemple de Swan:

Théorème 4.4.5. ***Modules de permutation et extensions transcendantes pures***
Soit M un $\mathbb{Z}[\pi]$-module de type fini, libre en tant que groupe abélien. Les affirmations suivantes sont équivalentes:

(i) Il existe une extension transcendante pure L de $l(M)^\pi$, de degré de transcendance fini, qui est aussi transcendante pure sur l^π.

(ii) Il existe des modules de permutation P_1 et P_2 de type fini rendant exacte la suite

$$0 \to M \to P_2 \to P_1 \to 0$$

Preuve. Supposons (i). Écrivons $L = l(M)^\pi(x_1, ..., x_r) = l^\pi(y_1, ..., y_{r+s})$, où $(x_1, .., x_r)$ et $(y_1, ..., y_{r+s})$ sont des familles algébriquement libres sur $l(M)^\pi$ et l^π respectivement. Faisons agir π sur $l(M)(x_1, ..., x_r) = l(M) \otimes_{l(M)^\pi} l(M)^\pi(x_1, .., x_r)$ à travers le premier facteur, c'est-à-dire, $\sigma(a \otimes b) = \sigma(a) \otimes b$. Posons finalement $A = l[M][x_1, ..., x_r]$ et $A' = l[y_1, ..., y_{r+s}]$. Vérifions que ces anneaux satisfont les propriétés $(P1) - (P5)$.
$(P1)$: Le corps des fractions de A est clairement $l(M)(x_1, ..., x_r)$. Le corps des fractions de A' est $l(y_1, ..., y_{r+s})$, et on a le diagramme:

$$\begin{array}{ccc} l(y_1, ..., y_{r+s}) & \hookrightarrow & l(M)(x_1, ..., x_r) \\ {\scriptstyle \text{degré}=|\pi|}\uparrow & & \uparrow{\scriptstyle \text{degré}=|\pi|} \\ l^\pi(y_1, ..., y_{r+s}) & = & l(M)^\pi(x_1, ..., x_r) \end{array}$$

Donc $l(M)(x_1, ..., x_r)$ est le corps des fractions de A'.
$(P2)$: A et A' sont clairement des l-algèbres de type fini.
$(P3)$: A est clairement stable par π. On a de plus $l^\pi(y_1, ...y_{r+s}) = l(M)^\pi(x_1, ..., x_r) \subseteq (l(M)(x_1, ..., x_r))^\pi$, donc les y_i sont fixés par π et A' est bien stable par π.
$(P4)$: A et A' sont bien factoriels.
$(P5)$: $A^*/l^* = M$ et $A'^*/l^* = 1$ sont bien des groupes abéliens de type fini.
D'après 3.1.3, il existe $a \in A^\pi$ et $a' \in A'^\pi$ tels que $A[a^{-1}] = A'[a'^{-1}]$. Notons B cet anneau. La propriété 3.1.4 permet alors d'établir l'existence de deux $\mathbb{Z}[\pi]$-modules de permutation de type fini P_1 et P_2 rendant exactes les deux suites:

$$0 \to A^*/l^* \to B^*/l^* \to P_1 \to 0$$

$$0 \to A'^*/l^* \to B^*/l^* \to P_2 \to 0$$

On déduit l'exactitude des suites:

$$0 \to M \to B^*/l^* \to P_1 \to 0$$

$$0 \to 0 \to B^*/l^* \to P_2 \to 0$$

et donc la propriété (ii) est démontrée.
Supposons (ii). La proposition précédente impose alors que $l(P_2)^\pi/l(M)^\pi$ est une extension transcendante pure. Son degré de transcendance est clairement fini. De plus, d'après 4.4.2, $l(P_2)^\pi/l^\pi$ est aussi transcendante pure. La propriété (i) est donc établie, avec $L = l(P_2)^\pi$. □

Nous en déduisons le corollaire suivant, qui nous sera très utile dans la suite:

Corollaire 4.4.6. ***Modules de permutation et extensions transcendantes pures 2***
Soit M un $\mathbb{Z}[\pi]$-module de type fini, libre en tant que groupe abélien. On suppose que , pour tout sous-groupe ρ de π, on a $H^1(\rho, M) = 0$. Les propositions suivantes sont alors équivalentes:

(i) Il existe une extension transcendante pure L de $l(M)^\pi$, de degré de transcendance fini, qui est aussi transcendante pure sur l^π.

(ii) Il existe des modules de permutation P_1 et P_2 de type fini tels que

$$M \oplus P_1 \cong P_2$$

Preuve. Supposons (i). Alors, d'après le théorème précédent, on peut trouver des modules de permutation P_1 et P_2 de type fini rendant exacte la suite $0 \to M \to P_2 \to P_1 \to 0$. D'après les caractérisations des facteurs directs de permutation (4.3.3), cette suite est scindée, d'où la propriété (ii).
L'implication $(ii) \Rightarrow (i)$ découle immédiatement du théorème précédent. □

4.5 Construction du module F_ρ et liens avec les extensions transcendantes pures

On suppose maintenant que π est abélien. Dans cette section, nous allons définir un foncteur de la catégorie des π-modules dans la catégorie des $\mathbb{Z}(\rho)$-modules sans torsion, et nous verrons comment l'étude de ce foncteur permet de dire si une certaine extension est transcendante pure ou pas.
On définit ce foncteur par $F_{\pi,\rho}(M) = (M \otimes_\pi \mathbb{Z}(\rho))/\{\text{éléments d'ordre additif fini}\}$, où M est un π-module et ρ est un groupe quotient cyclique de π. Ce foncteur est bien défini, car le morphisme d'anneaux surjectif $\mathbb{Z}[\pi] \to \mathbb{Z}(\rho)$ nous permet de considérer chaque $\mathbb{Z}(\rho)$-module comme un π-module.

Proposition 4.5.1. ***"Indépendance par rapport au choix de π"***
Soient $S(\pi)$ l'ensemble des quotients cycliques de π et π' un groupe quotient de π. Alors il y a une inclusion naturelle $S(\pi') \subset S(\pi)$. En plus, pour tout π'-module M on a:
i) Si $\rho \in S(\pi')$, alors $F_{\pi,\rho}(M) \cong F_{\pi',\rho}(M)$ en tant que $\mathbb{Z}(\rho)$-modules;
ii) Si $\rho \in S(\pi)$ mais $\rho \notin S(\pi')$, alors $F_{\pi,\rho}(M) = 0$.

Preuve. Déjà, l'inclusion est claire (elle est induite par le morphisme surjectif $\pi \to \pi'$).
Montrons l'assertion i). On a l'isomorphisme $M \otimes_\pi \mathbb{Z}[\pi'] \cong M$, donc $M \otimes_\pi \mathbb{Z}(\rho) = M \otimes_\pi \mathbb{Z}[\pi'] \otimes_{\pi'} \mathbb{Z}(\rho) = M \otimes_{\pi'} \mathbb{Z}(\rho)$.

Montrons l'assertion ii). L'hypothèse $\rho \notin S(\pi')$ montre l'existence d'un élément $\sigma \in \pi$ qui a pour l'image 1 dans π' et dont l'image σ^* dans ρ est différente de 1. L'action de σ sur M est alors triviale, donc $(\sigma^* - 1) \cdot (M \otimes_\pi \mathbb{Z}(\rho)) = 0$, où $\sigma^* - 1$ est un élément non nul de $\mathbb{Z}(\rho)$. Mais alors, si τ est un générateur de ρ et $\sigma^* = \tau^d$ avec $0 < d < |\rho|$, comme les polynômes $\phi_{|\rho|}(X)$ et $X^d - 1$ ($d < |\rho|$) sont premiers entre eux, il suit que $\sigma^* - 1$ divise un entier non nul dans $\mathbb{Z}(\rho)$ par Bézout. Mais alors $M \otimes_\pi \mathbb{Z}(\rho)$ est un groupe de torsion, et donc $F_{\pi,\rho}(M) = 0$. □

On écrit dorénavant F_ρ au lieu de $F_{\pi,\rho}$ par abus de langage.

Proposition 4.5.2. ***Une certaine compatibilité avec l'inclusion***
Soient N un π-module et $M \subset N$ un sous-π-module de N tel que N/M soit un groupe de torsion. Alors $F_\rho(M)$ est isomorphe à l'image de M par l'application naturelle $N \to F_\rho(N)$, pour tout groupe quotient cyclique ρ de π.

Preuve. Soit J le noyau du morphisme $\mathbb{Z}[\pi] \to \mathbb{Z}(\rho)$. Ceci induit, pour tout π-module P, une surjection $P \to F_\rho(P)$ de noyau $\{p \in P | \exists k \in \mathbb{Z}, k \neq 0, k \cdot p \in J \cdot P\}$. Il suffit alors de voir que $\{m \in M | \exists k \in \mathbb{Z}, k \neq 0, k \cdot m \in J \cdot M\} = M \cap \{n \in N | \exists k \in \mathbb{Z}, k \neq 0, k \cdot n \in J \cdot N\}$. Mais ceci est vrai car N/M est de torsion. □

Proposition 4.5.3. ***Cas d'un module de permutation***
Si N est un π-module de permutation, alors $F_\rho(N)$ est $\mathbb{Z}(\rho)$-libre pour tout ρ groupe quotient cyclique de π.

Preuve. Le module N est un π-module de permutation, donc il suffit de traiter le cas $N = \mathbb{Z}[\pi']$ avec π' un groupe quotient de π car le foncteur que nous avons défini est compatible avec la somme directe. Mais alors d'après la proposition 4.5.1, $F_\rho(N) \cong \mathbb{Z}(\rho)$ ou $F_\rho(N) = 0$. D'où la proposition. □

Théorème 4.5.4. F_ρ ***et isomorphismes 1***
Soit π un groupe cyclique. Soit M un π-module projectif de type fini. Alors $l(M)^\pi$ et $l(\bigoplus_\rho F_\rho(M))^\pi$ sont isomorphes sur l^π, où ρ parcourt l'ensemble des quotients cycliques de π.

Preuve. Cette preuve est assez longue et délicate. Fixons d'abord les notations pour cette preuve. Soit π un groupe cyclique d'ordre m et de générateur τ. On note $E(m)$ l'ensemble des diviseurs positifs de m. On note π_d l'unique groupe quotient de π d'ordre d pour $d \in E(m)$. On note aussi, pour $C \subset E(m)$, $\phi_C = \prod_{d \in C} \phi_d$.
Si M est un π-module, alors on note, pour tout $C \subset E(m)$, $M_C = M/\phi_C(\tau)M$.
On introduit aussi un graphe qui sera étudié dans lemme 3 et dont l'ensemble des sommets est l'ensemble des relations d'équivalence sur $E(m)$: si $G(m)$ est l'ensemble des relations d'équivalence sur $E(m)$ et u un élément de $G(m)$ dont

l'ensemble de ses classes d'équivalence (non vides) est noté $[u]$, alors deux sommets u et v sont les extrémités d'une arête si la condition suivante est vérifiée: il existe $d \in E(m)$ et $D \in [u]$ tels que $E(d) \subset D$, $E(d) \neq D$ et $[v] = \{E(d), D - E(d), C | C \in [u], C \neq D\}$. L'ensemble des arêtes sera noté $S(m)$, et on montrera dans le lemme 3 que ce graphe est connexe.
Lemme 1: Soit M un $\mathbb{Z}[\pi]$-module projectif, et soit $d \in E(m)$. Alors $M_{E(d)}$ est un $\mathbb{Z}[\pi]$-module, facteur direct de permutation.
Preuve du lemme 1: $M_{E(d)} \cong M/(\tau^d - 1)M \cong M \otimes_{\mathbb{Z}[\pi]} \mathbb{Z}[\pi]/(\tau^d - 1) \cong M \otimes_{\mathbb{Z}[\pi]} \mathbb{Z}[\pi_d]$. M étant projectif, cet isomorphisme impose que $M_{E(d)}$ est un $\mathbb{Z}[\pi_d]$-module projectif, et donc un $\mathbb{Z}[\pi]$-module, facteur direct de permutation.

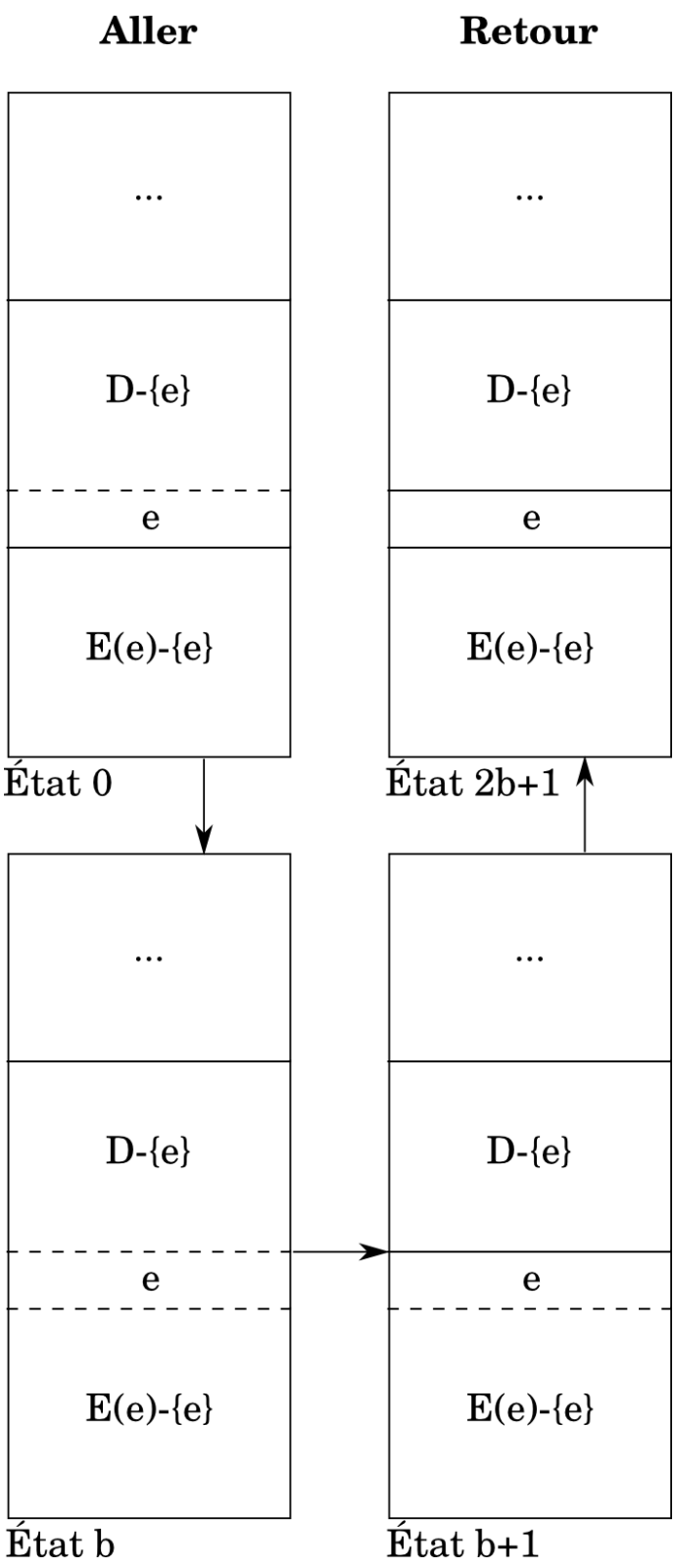
Lemme 2: Soient M un π-module projectif, et C, C' deux sous-ensembles disjoints de $E(m)$. Alors on a une suite exacte de π-modules:

$$0 \to M_C \to M_{C \cup C'} \to M_{C'} \to 0$$

Preuve du lemme 2: Comme tout passe à la somme directe, il suffit de traiter le cas où $M = \mathbb{Z}[\pi]$. On vérifie l'exactitude de la suite pour les applications suivantes: celle de $M_{C \cup C'}$ vers $M_{C'}$ est la projection naturelle, et celle de M_C vers $M_{C \cup C'}$ est induite par la multiplication par $\phi_{C'}(\tau)$.

Lemme 3: Le graphe $(G(m), S(m))$ est connexe.
Un mot avant de faire la preuve de ce lemme: on ne prend pas en compte l'orientation des chemins.
Preuve du lemme 3:
On note $i(m)$ (resp. $w(m)$) la relation d'équivalence sur $E(m)$ telle que $[i(m)] = \{\{d\} | d \in E(m)\}$ (resp. $[w(m)] = \{E(m)\}$). Il suffit de voir qu'il existe un chemin de u vers $i(m)$ pour tout $u \in G(m)$. On va faire une récurrence (forte) sur m. On note aussi $n(u) = |E(m)| - |[u]|$. Pour m fixé, on fait une récurrence sur $n(u)$.
Récurrence sur m: Si $m = 1$ il n'y a rien à démontrer. Le passage de $\leq m$ à $m+1$ se fait par une récurrence sur $n(u)$.
Récurrence sur $n(u)$: Si $n(u) = 0$, alors $u = i(m)$ et on a gagné. On suppose donc $n(u) > 0$, et soit e le plus petit élément de $E(m)$ tel qu'il existe $D \in [u]$ avec $|D| > 1$ (non trivial) et $e \in D$. Il suffit donc de montrer qu'on peut isoler e dans D. Comme $u \neq i(m)$, on a $e < m$. On peut donc appliquer l'hypothèse de récurrence sur m, qui donne un chemin de $i(e)$ à $w(e)$ dans le graphe $(G(e), S(e))$. On va noter ce chemin $(v_j)_{0 \leq j \leq b}$, et on va modifier ce chemin dans la suite. Pour $0 \leq j \leq b$, on note $D_j \in [v_j]$ la classe qui contient e, i.e. $e \in D_j$. On définit alors un chemin de longueur $2b+1$ qui permet de séparer e des autres éléments de D. Pour $0 \leq j \leq b$, on définit $u_j \in G(m)$ par $[u_j] = \{C \in [u] | C \cap E(e) = \emptyset\} \cup \{D \cup D_j\} \cup ([v_j] - \{D_j\})$. Pour $b+1 \leq j \leq 2b+1$,

on définit $u_j \in G(m)$ par $[u_j] = \{C \in [u] | C \cap E(e) = \emptyset\} \cup \{D - \{e\}\} \cup [v_{2b+1-j}]$. On vérifie bien qu'il s'agit d'un chemin sur le graphe, comme on peut s'en convaincre à partir d'une figure:


Aller
Retour
...
D-{e}
e
E(e)-{e}
État 0
État 2b+1
...
D-{e}
e
E(e)-{e}
État b
État b+1

On a par ailleurs $[u_{2b+1}] = \{D - \{e\}, \{e\}\} \cup \{[u] - \{D\}\}$. On a donc réussi à isoler e dans la classe D, il suit que $n(u_{2b+1}) = n(u) - 1$. L'hypothèse de récurrence fournit alors un chemin de u_{2b+1} à $i(m)$. On peut donc relier u à $i(m)$.
On a ainsi bien montré la connexité du graphe (dans le sens d'un graphe non-orienté).

Lemme 4: (Un invariant du graphe) Si $u, v \in G(m)$, alors $l(M(u))^\pi \cong l(M(v))^\pi$ sur l^π, où $M(s) = \underset{C\in[s]}{\oplus} M_C$ pour $s \in G(m)$.
Preuve du lemme 4: Déjà remarquons que le lemme précédent nous permet de simplifier la situation: il suffit de faire cette preuve dans le cas de deux extrémités d'une arête du graphe. On peut alors appliquer le lemme 2 pour avoir une suite exacte de π-modules:

$$0 \to M_{D-E(d)} \to M_D \to M_{E(d)} \to 0$$

Cette suite exacte donne lieu alors, en ajoutant un facteur $N = \underset{C\in[u],C\neq D}{\oplus} M_C$, la suite exacte suivante:

$$0 \to N \oplus M_{D-E(d)} \to N \oplus M_D \to M_{E(d)} \to 0$$

de modules $\mathbb{Z}$-libres car M est projectif. En appliquant les lemmes 1 (de cette démonstration) et 4.4.3, on a un isomorphisme de corps entre $l(N \oplus M_{D-E(d)} \oplus M_{E(d)})^\pi$ et $l(N \oplus M_D)^\pi$ sur l^π. Mais ceci est tout simplement un isomorphisme $l(M(u))^\pi \cong l(M(v))^\pi$ sur l^π, puisque u et v sont les extrémités d'une même arête du graphe.
Finalement on est en mesure de démontrer le théorème:

Preuve du théorème: reprenons les notations $i(m)$ et $w(m)$ du lemme 3. Alors en appliquant le lemme 4 à $u = i(m)$, $v = w(m)$, on a $M(i(m)) = \underset{d|m}{\oplus} M/(\phi_d(\tau)M) \cong \underset{\rho}{\oplus} F_\rho(M)$ et $M(w(m)) = M$, ce qui donne l'isomorphisme entre $l(M)^\pi$ et $l(\underset{\rho}{\oplus} F_\rho(M))^\pi$ sur l^π. D'où le théorème. □

Nous en déduisons le corollaire suivant:

Corollaire 4.5.5. *F_ρ et isomorphismes 2*
Soit π un groupe abélien fini. Soit M un $\mathbb{Z}[\pi]$-module de type fini de la forme

$$M = \bigoplus_{\pi'} M_{\pi'}$$

où $M_{\pi'}$ est un $\mathbb{Z}[\pi']$-module projectif, π' décrivant les quotients cycliques de π. On a alors le l^π-isomorphisme de corps:

$$l(M)^\pi \cong l\left(\bigoplus_\rho F_\rho(M)\right)^\pi$$

ρ décrivant les quotients cycliques de π.

Preuve. Soit π' un quotient cyclique de π. Notons $\pi' = \pi/\pi''$. Le théorème précédent appliqué au groupe cyclique π', au module $M_{\pi'}$ et au corps $l^{\pi''}$ permet d'obtenir le l^π-isomorphisme de corps:

$$l(M_{\pi'})^\pi \cong l\left(\bigoplus_{\rho'} F_{\rho'}(M_{\pi'})\right)^\pi$$

où la somme est prise sur les quotients cycliques de π'. La proposition 4.5.1 permet alors d'écrire:

$$l(M_{\pi'})^\pi \cong l\left(\bigoplus_{\rho} F_{\rho}(M_{\pi'})\right)^\pi$$

où la somme est prise sur les quotients cycliques de π.
Montrons que cela implique que $l(M_{\pi'}) \cong l\left(\bigoplus_\rho F_\rho(M_{\pi'})\right)$. Pour ce faire, la bonne notion à introduire est celle des extensions linéairement disjointes. Cependant, afin de ne pas introduire de nouvelles notions qui ne serviront que dans cette preuve, nous allons donner une démonstration " à la main ".
Étudions d'abord $l(M_{\pi'})^\pi$. En appliquant le théorème de l'élément primitif, soit l_0 tel que $1, l_0, ..., l_0^{p-1}$ soit une base de l sur l^π, où p est l'ordre de π. Montrons que, dans le corps $l(M_{\pi'})$, $1, l_0, ..., l_0^{p-1}$ sont libres sur $l(M_{\pi'})^\pi$. Soient $a_1, ..., a_p \in l(M_{\pi'})^\pi$ tels que

$$\sum_{i=1}^{p} a_i l_0^{i-1} = 0$$

On a alors, pour tout $\sigma \in \pi$,

$$\sum_{i=1}^{p} a_i \sigma(l_0)^{i-1} = 0$$

Donc, si $\sigma_1, ..., \sigma_p$ sont les éléments de π et si $V(\sigma_1(l_0), ..., \sigma_p(l_0))$ est la matrice de Van der Monde associée à $\sigma_1(l_0), ..., \sigma_p(l_0)$, alors:

$$V(\sigma_1(l_0), ..., \sigma_p(l_0))^t(a_1, ..., a_p) = 0$$

On en déduit que $a_1 = ... = a_p = 0$, d'où la liberté de $1, l_0, ..., l_0^{p-1}$ sur $l(M_{\pi'})^\pi$.
On déduit immédiatement que l'application l^π-linéaire $l(M_{\pi'})^\pi \otimes_{l^\pi} l \to l(M_{\pi'})$ définie par $a \otimes b \to ab$ est injective. Munissons $l(M_{\pi'})^\pi \otimes_{l^\pi} l$ d'une structure d'anneau par $(a \otimes b)(a' \otimes b') = (aa' \otimes bb')$. L'application linéaire précédente est alors un morphisme d'anneaux injectif, dont l'image est

$$l(M_{\pi'})^\pi l = \left\{ \sum a_i b_i, a_i \in l(M_{\pi'})^\pi, b_i \in l \right\}$$

où les sommes prises sont toutes finies. On en déduit que $l(M_{\pi'})^\pi l$ est un $l(M_{\pi'})^\pi$-espace vectoriel de dimension p, inclus dans $l(M_{\pi'})$, qui est aussi un $l(M_{\pi'})^\pi$-espace vectoriel de dimension p. Par conséquent, $l(M_{\pi'})^\pi l = l(M_{\pi'})$. On en déduit que $l(M_{\pi'})^\pi \otimes_{l^\pi} l$ est un corps l-isomorphe à $l(M_{\pi'})$.
De manière analogue, $l\left(\bigoplus_\rho F_\rho(M_{\pi'})\right)^\pi \otimes_{l^\pi} l$ est muni d'une structure de corps l-isomorphe à $l\left(\bigoplus_\rho F_\rho(M_{\pi'})\right)$. Nous en déduisons un l-isomorphisme entre les corps $l(M_{\pi'}) \cong l\left(\bigoplus_\rho F_\rho(M_{\pi'})\right)$, qui commute avec l'action de π. On en déduit un isomorphisme

$$l(M) \cong \left(\bigoplus_\rho F_\rho(M) \right)$$

qui commute avec l'action de π, d'où le résultat.

□

Afin d'énoncer le résultat suivant, nous avons besoin de construire une notion de rang pour un $\mathbb{Z}[\pi']$-module projectif P de type fini où π' est un groupe cyclique. Pour A anneau commutatif, on notera $\mathrm{Spec}(A)$ le spectre de A, c'est à dire l'ensemble des idéaux premiers de A, que l'on munit de la topologie de Zariski. Commençons par montrer le lemme suivant:

Lemme 4.5.6. ***Spectre de*** $\mathbb{Z}[\pi']$
Soit π' un groupe cyclique. Alors Spec($\mathbb{Z}[\pi']$) est connexe.

Preuve. Il suffit de montrer que les seuls éléments idempotents de $\mathbb{Z}[\pi']$ sont 0 et 1. Cela revient à montrer que, si $P \in \mathbb{Z}[X]$ est tel que $X^n - 1 | P(P-1)$, alors $X^n - 1 | P$ ou $X^n - 1 | P - 1$. Soit ζ_n une racine primitive n-ième de l'unité. Notons $P = \sum_{k=0}^{+\infty} a_k X^k$ avec les a_k nuls à partir d'un certain rang. Alors $P(1) + P(\zeta_n) + ... + P(\zeta_n^{n-1}) = n(a_0 + a_n + a_{2n} + ...)$ est multiple de n. Or, chaque ζ_n^i est racine de P ou de $P - 1$, donc $P(\zeta_n^i) \in \{0, 1\}$. On en déduit que, soit $P(\zeta_n^i) = 0$ pour tout $i \in \{0, 1, ..., n-1\}$, soit $P(\zeta_n^i) = 1$ pour tout $i \in \{0, 1, ..., n-1\}$. Donc $X^n - 1 | P$ ou $X^n - 1 | P - 1$. □

Pour $\mathfrak{p}$ idéal premier de $\mathbb{Z}[\pi']$, montrons d'abord que $P_\mathfrak{p} = P \otimes_{\mathbb{Z}[\pi']} \mathbb{Z}[\pi']_\mathfrak{p}$ est un $\mathbb{Z}[\pi']_\mathfrak{p}$-module libre (où $\mathbb{Z}[\pi']_\mathfrak{p}$ désigne l'anneau localisé). P étant un $\mathbb{Z}[\pi']$-module projectif, $P_\mathfrak{p}$ est un $\mathbb{Z}[\pi']_\mathfrak{p}$-module projectif. Écrivons $P_\mathfrak{p} \oplus Q = \mathbb{Z}[\pi']_\mathfrak{p}^r$, où Q est un $\mathbb{Z}[\pi']_\mathfrak{p}$-module et r un entier naturel. On remarque que $\mathbb{Z}[\pi']_\mathfrak{p}$ est un anneau local d'idéal maximal $\mathfrak{m} = \mathfrak{p}\mathbb{Z}[\pi']_\mathfrak{p}$. On a $P_\mathfrak{p}/\mathfrak{m}P_\mathfrak{p} \oplus Q/\mathfrak{m}Q = (\mathbb{Z}[\pi']_\mathfrak{p}/\mathfrak{m})^r$. Notons $(p_i)_{i\in I}$ une famille d'éléments de $P_\mathfrak{p}$ dont les classes modulo $\mathfrak{m}P_\mathfrak{p}$ forment une base du $\mathbb{Z}[\pi']_\mathfrak{p}/\mathfrak{m}$-espace vectoriel $P_\mathfrak{p}/\mathfrak{m}P_\mathfrak{p}$. Notons $(q_j)_{j\in J}$ une famille d'éléments de Q dont les classes modulo $\mathfrak{m}Q$ forment une base du $\mathbb{Z}[\pi']_\mathfrak{p}/\mathfrak{m}$-espace vectoriel $Q/\mathfrak{m}Q$. Alors, d'après le lemme de Nakayama, la famille $(p_i)_{i\in I}$ engendre $P_\mathfrak{p}$ et la famille $(q_j)_{j\in J}$ engendre Q. Donc les p_i et les q_j engendrent $P_\mathfrak{p} \oplus Q = \mathbb{Z}[\pi']_\mathfrak{p}^r$, et, par dimension, $|I| + |J| = r$. On en déduit que les p_i et les q_j sont une base de $P_\mathfrak{p} \oplus Q = \mathbb{Z}[\pi']_\mathfrak{p}^r$. Donc la famille $(p_i)_i$ est libre et engendre $P_\mathfrak{p}$, et $P_\mathfrak{p}$ est un $\mathbb{Z}[\pi']_\mathfrak{p}$-module libre de type fini.
On note $\mathrm{rg}_\mathfrak{p}(P)$ le rang de $P_\mathfrak{p}$ en tant que $\mathbb{Z}[\pi']$-module libre, c'est à dire la dimension de $P_\mathfrak{p}/\mathfrak{p}P_\mathfrak{p}$ en tant que $\mathbb{Z}[\pi']_\mathfrak{p}/\mathfrak{p}\mathbb{Z}[\pi']_\mathfrak{p}$-espace vectoriel . Il suffit maintenant de montrer que $\mathrm{rg}_\mathfrak{p}(P)$ est indépendant du choix de $\mathfrak{p}$. Fixons donc $\mathfrak{p}_0$ un idéal premier de $\mathbb{Z}[\pi']$ et soit $\mathbb{I}$ l'ensemble des idéaux premiers $\mathfrak{q}$ de $\mathbb{Z}[\pi']$ tels qu'il existe $n \in \mathbb{N}$ et $\mathfrak{p}_1$,...,$\mathfrak{p}_{2n}$ des idéaux premiers vérifiant:

$$\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \supseteq \mathfrak{p}_2 \subseteq \mathfrak{p}_3 \supseteq ... \subseteq \mathfrak{p}_{2n-1} \supseteq \mathfrak{p}_{2n} = \mathfrak{q}$$

Montrons que $\mathbb{I} = \mathrm{Spec}(\mathbb{Z}[\pi'])$. Il est clair que si $\mathfrak{r}_1 \in \mathbb{I}$, $\mathfrak{r}_2 \in \mathrm{Spec}(A)$ et $\mathfrak{r}_1 \subseteq \mathfrak{r}_2$, alors $\mathfrak{r}_2 \in \mathbb{I}$. En notant $V(I) = \{\mathfrak{p} \in \mathrm{Spec}(\mathbb{Z}[\pi'])|I \subseteq \mathfrak{p}\}$ pour I idéal de $\mathbb{Z}[\pi']$, on en déduit que $\mathbb{I} = \bigcup_{\mathfrak{p}\in\mathbb{I}} V(\mathfrak{p}) = V(\prod_{\mathfrak{p}\in\mathbb{I}} \mathfrak{p})$ est fermé. On montre de manière analogue que $\mathbb{I}$ est ouvert. Par connexité de $\mathrm{Spec}(\mathbb{Z}[\pi'])$, on a bien $\mathbb{I} = \mathrm{Spec}(\mathbb{Z}[\pi'])$.
Il suffit donc maintenant de voir que $\mathrm{rg}_\mathfrak{p}(P) = \mathrm{rg}_{\mathfrak{p}'}(P)$ pour $\mathfrak{p} \subseteq \mathfrak{p}'$, ce qui est évident. Nous avons donc montré le lemme:

Lemme 4.5.7. ***Rang d'un*** $\mathbb{Z}[\pi']$ ***module projectif***
Soit π' un groupe cyclique. Soit P un $\mathbb{Z}[\pi']$-module projectif de type fini. L'entier $rg_\mathfrak{p}(P)$ est indépendant du choix de l'idéal premier $\mathfrak{p}$ de $\mathbb{Z}[\pi']$. On l'appellera ***rang du module P****.*

Nous pouvons maintenant établir le résultat suivant, qui jouera un rôle important dans la suite:

Théorème 4.5.8. ***Lien entre*** F_ρ ***et les extensions transcendantes pures***
Soit π un groupe abélien fini. Soit M un $\mathbb{Z}[\pi]$-module de type fini de la forme:

$$M = \bigoplus_{\pi'} M_{\pi'}$$

où $M_{\pi'}$ est un $\mathbb{Z}[\pi']$-module projectif, π' décrivant les quotients cycliques de π. Il y a alors équivalence entre les propriétés suivantes:

(i) Le corps $l(M)^\pi$ est une extension transcendante pure de l^π.

(ii) Il existe une extension transcendante pure L de $l(M)^\pi$, de degré de transcendance fini, qui est aussi transcendante pure sur l^π.

(iii) Pour tout quotient cyclique ρ de π, $F_\rho(M)$ est un $\mathbb{Z}(\rho)$-module libre.

Preuve. Supposons (ii). Le module M est un facteur direct de permutation sur $\mathbb{Z}[\pi]$, donc d'après 4.3.2, nous pouvons appliquer 4.4.6. Il existe donc des $\mathbb{Z}[\pi]$-modules de permutation de type fini N_1 et N_2 tels que $M \oplus N_1 \cong N_2$. D'après 4.5.3, pour tout quotient cyclique ρ de π, $F_\rho(N_1)$ et $F_\rho(N_2)$ sont des $\mathbb{Z}(\rho)$-modules libres tels que $F_\rho(M) \oplus F_\rho(N_1) \cong F_\rho(N_2)$. Comme $\mathbb{Z}(\rho)$ est un anneau de Dedekind, d'après le théorème de structure des modules de type fini sur un anneau de Dedekind, cela impose que $F_\rho(M)$ est un $\mathbb{Z}(\rho)$-module libre, d'où (iii).
Supposons maintenant (iii). Soit $r(\pi')$ le rang de $M_{\pi'}$ sur $\mathbb{Z}[\pi']$. Posons

$$N = \bigoplus_{\pi'} \mathbb{Z}[\pi']^{r(\pi')}$$

Soit ρ un quotient cyclique de π. Par hypothèse, $F_\rho(M)$ est libre. Soit $\mathcal{G}$ l'ensemble des quotients cycliques π' de π tels que ρ est un quotient de π'. Alors le rang de $F_\rho(M)$ est:

$$R = \sum_{\pi' \in \mathcal{G}} r(\pi')$$

D'autre part, il est clair que $F_\rho(N)$ est libre de rang R. Donc $F_\rho(M)$ et $F_\rho(N)$ sont des $\mathbb{Z}(\rho)$-modules isomorphes. Par conséquent,

$$\bigoplus_\rho F_\rho(M) \cong \bigoplus_\rho F_\rho(N)$$

Avec 4.5.5, on déduit les l^π-isomorphismes

$$l(M)^\pi \cong l\left(\bigoplus_\rho F_\rho(M)\right)^\pi \cong l\left(\bigoplus_\rho F_\rho(N)\right)^\pi \cong l(N)^\pi$$

Or, d'après 4.4.2, $l(N)^\pi$ est une extension transcendante pure de l^π, d'où (i). □

4.6 Étude des modules I_q et J_q

Soit p un nombre premier et posons $q = p^s$, où $s > 0$. On se donne un corps l, de caractéristique distincte de p, et contenant une racine primitive q-ième de l'unité, notée ζ_q. On considère aussi un groupe abélien fini π d'automorphismes de l. On

note alors $k = l^{\pi}$. L'extension $l|k$ est alors finie galoisienne de groupe de Galois π. Soient $\pi(q) = Gal(l|k(\zeta_q))$ et $\rho(q) = Gal(k(\zeta_q)/k)$. La théorie de Galois impose alors que $\rho(q) = \pi/\pi(q)$. L'application $\pi \to (\mathbb{Z}/q\mathbb{Z})^*, \sigma \mapsto t$ telle que $\sigma(\zeta_q) = \zeta_q^t$ est un morphisme de groupes dont le noyau est $\pi(q)$. Elle se factorise donc en un morphisme de groupes injectif $\varphi_q : \rho(q) \to (\mathbb{Z}/q\mathbb{Z})^*$. Ceci permet de munir $\mathbb{Z}/q\mathbb{Z}$ d'une structure de $\mathbb{Z}[\rho(q)]$-module, et donc aussi d'une structure de $\mathbb{Z}[\pi]$-module.

Supposons dans un premier temps que $\rho(q)$ n'est pas cyclique. On sait que, dès que p est impair ou $s < 3$, $(\mathbb{Z}/q\mathbb{Z})^*$ est cyclique. On en déduit que nécessairement $p = 2$ et $s \geq 3$. Notons $C(q) = (\mathbb{Z}/q\mathbb{Z}) - \{0\}$, et considérons $\mathbb{Z}^{C(q)}$ le $\mathbb{Z}[\rho(q)]$-module de permutation de $\mathbb{Z}$-base $(e_c)_{c \in C(q)}$ indexée par $C(q)$ tel que, pour $\sigma \in \rho(q)$ et $c \in C(q)$, $\sigma(e_c) = e_{\sigma c}$. Soit $i_q : \mathbb{Z}^{C(q)} \to \mathbb{Z}/q\mathbb{Z}$ le morphisme de $\mathbb{Z}[\rho(q)]$-modules tel que $i_q(e_c) = c$, pour $c \in C(q)$. Soit $I_q = Ker(i_q)$. On a alors la suite exacte:

$$0 \to I_q \to \mathbb{Z}^{C(q)} \to \mathbb{Z}/q\mathbb{Z} \to 0$$

Proposition 4.6.1. ***Cohomologie de*** I_q
Supposons $\rho(q)$ non cyclique.

(i) Pour tout sous-groupe ρ de π, $H^1(\rho, I_q) = 0$.

(ii) Il existe un sous-groupe ρ de π tel que $\widehat{H}^{-1}(\rho, I_q) \neq 0$.

Preuve.

(i) Soit ρ un sous-groupe de π. Écrivons la suite exacte de cohomologie:

$$0 \to I_q^{\rho} \to (\mathbb{Z}^{C(q)})^{\rho} \to (\mathbb{Z}/q\mathbb{Z})^{\rho} \to H^1(\rho, I_q) \to 0$$

car $\mathbb{Z}^{C(q)}$ est un module de permutation. La flèche $(\mathbb{Z}^{C(q)})^{\rho} \to (\mathbb{Z}/q\mathbb{Z})^{\rho}$ étant clairement surjective, on a bien $H^1(\rho, I_q) = 0$.

(ii) Montrons d'abord qu'il existe ρ_0 sous-groupe de $\rho(q)$ tel que $\widehat{H}^{-1}(\rho_0, I_q) \neq 0$. Par hypothèse, $\rho(q)$ n'est pas cyclique. De plus, il s'injecte dans $(\mathbb{Z}/q\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{s-2}\mathbb{Z}$. Par conséquent, on peut trouver ρ_0 un sous-groupe de $\rho(q)$ tel que $\varphi_q(\rho_0) = \{1, -1, u+1, u-1\} \cong (\mathbb{Z}/2\mathbb{Z})^2$, où $u = q/2$.
Soit $C = \{1, u-1, u, u+1, -1\} \subseteq \mathbb{Z}/q\mathbb{Z}$. Tout comme nous avons muni $\mathbb{Z}^{C(q)}$ d'une structure de $\mathbb{Z}[\rho(q)]$-module, on peut munir $\mathbb{Z}^C$ d'une structure de $\mathbb{Z}[\rho_0]$-module. En considérant la restriction de $\mathbb{Z}^{C(q)} \to \mathbb{Z}/q\mathbb{Z}$ à $\mathbb{Z}^C$, on obtient la suite exacte:

$$0 \to \mathbb{Z}^C \cap I_q \to \mathbb{Z}^C \to \mathbb{Z}/q\mathbb{Z} \to 0$$

Posons $M = \mathbb{Z}^C \cap I_q$. Montrons que $H^1(\rho_1, M) = 0$, pour ρ_1 l'un des cinq sous-groupes de $\rho_0 \cong (\mathbb{Z}/2\mathbb{Z})^2$. D'après la suite exacte de cohomologie, il suffit de montrer que la flèche $f_{\rho_1} : (\mathbb{Z}^C)^{\rho_1} \to (\mathbb{Z}/q\mathbb{Z})^{\rho_1}$ est surjective.
Si $\rho_1 = 1$, il est clair que f_{ρ_1} est surjective.
Si $\rho_1 = \rho_0$ ou $\rho_1 = \varphi_q^{-1}(\{1, -1\})$ ou $\rho_1 = \varphi_q^{-1}(\{1, u-1\})$, alors $(\mathbb{Z}/q\mathbb{Z})^{\rho_1} = \{0, u\}$ et $e_u \in (\mathbb{Z}^C)^{\rho_1}$, donc f_{ρ_1} est surjective.
Finalement, si $\rho_1 = \varphi_q^{-1}(\{1, u+1\})$, alors $(\mathbb{Z}/q\mathbb{Z})^{\rho_1} = \{0, 2, 4, ..., q-2\}$. Comme $(u+2)/2$ est impair, il est inversible dans $\mathbb{Z}/q\mathbb{Z}$. Soit donc $\lambda \in \mathbb{N}$ tel que $\lambda(u+2) \equiv 2 \pmod{q}$. Alors l'image de $k\lambda(e_1 + e_{u+1}) \in (\mathbb{Z}^C)^{\rho_1}$ par f_{ρ_1} est $2k$, d'où la surjectivité de f_{ρ_1}.
Ainsi, nous avons montré que, dans tous les cas, $H^1(\rho_1, M) = 0$.
Montrons à présent que $\widehat{H}^{-1}(\rho_0, M) \neq 0$. Considérons:

$$x = (1 - u/2)e_1 + (u/2)e_{-1} - e_{1+u}$$

Il est clair que $x \in M$, et on remarque que $\sum_{\sigma \in \rho_0} \sigma x = 0$. Montrons donc que x n'est pas dans $I_{\rho_0}M$, où I_{ρ_0} est l'idéal de $\mathbb{Z}[\rho_0]$ engendré par les $\sigma - 1$ pour $\sigma \in \rho_0$. Soit $\alpha = \sum_{c \in C} \alpha_c e_c$ un élément de M. Alors q divise $\sum_{c \in C} c\alpha_c$, et donc u divise $\alpha_1 - \alpha_{u-1} + \alpha_{u+1} - \alpha_{-1}$. Or, on remarque que les composantes selon e_{u-1} et e_{-1} de:
$*(\varphi_q^{-1}(u-1) - \varphi_q^{-1}(1))\alpha$ sont $\alpha_1 - \alpha_{u-1}$ et $\alpha_{u+1} - \alpha_{-1}$ respectivement.
$*(\varphi_q^{-1}(u+1) - \varphi_q^{-1}(1))\alpha$ sont $\alpha_{-1} - \alpha_{u-1}$ et $\alpha_{u-1} - \alpha_{-1}$ respectivement.
$*(\varphi_q^{-1}(-1) - \varphi_q^{-1}(1))\alpha$ sont $\alpha_{u+1} - \alpha_{u-1}$ et $\alpha_1 - \alpha_{-1}$ respectivement.
Dans les trois cas, la somme des coefficients de e_{u-1} et e_{-1} est donc multiple de u. On en déduit par linéarité que, pour tout élément de $I_{\rho_0}M$, la somme des coefficients de e_{u-1} et de e_{-1} est multiple de u. Or, pour x, cette somme vaut $u/2$, donc x n'appartient pas à $I_{\rho_0}M$. Ainsi, $\widehat{H}^{-1}(\rho_0, M) \neq 0$.
En composant la flèche $I_q \to \mathbb{Z}^{C(q)}$ avec la projection $\mathbb{Z}^{C(q)} \to \mathbb{Z}^{C(q)-C}$, on obtient une application $I_q \to \mathbb{Z}^{C(q)-C}$ rendant exacte la suite de $\mathbb{Z}[\rho_0]$-modules:

$$0 \to M \to I_q \to \mathbb{Z}^{C(q)-C} \to 0$$

Comme pour tout sous-groupe ρ_1 de ρ_0 on a $H^1(\rho_1, M) = 0$ et comme $\mathbb{Z}^{C(q)-C}$ est un facteur direct de permutation, d'après 4.3.3 la suite précédente est scindée. Donc $I_q = M \oplus \mathbb{Z}^{C(q)-C}$ et donc $\widehat{H}^{-1}(\rho_0, I_q) \neq 0$. Finalement, si l'on note ρ l'image réciproque de ρ_0 par la projection $\pi \to \rho(q)$, on obtient immédiatement que $\widehat{H}^{-1}(\rho, I_q) \neq 0$.

□

À partir d'ici, et jusqu'à la fin de cette partie, nous supposerons $\rho(q)$ cyclique. Notons J_q le noyau du morphisme $\mathbb{Z}[\rho(q)] \to \mathbb{Z}/q\mathbb{Z}$ induit par φ_q, de telle sorte

que la suite suivante de $\mathbb{Z}[\rho(q)]$-modules est exacte:

$$0 \to J_q \to \mathbb{Z}[\rho(q)] \to \mathbb{Z}/q\mathbb{Z} \to 0$$

Nous allons étudier le module J_q.

Proposition 4.6.2. ***Projectivité de*** J_q
Supposons $\rho(q)$ cyclique. Supposons de plus que 4 ne divise pas q ou que $\varphi_q(\rho(q))$ n'est pas égal à $\{1, -1\}$. Alors J_q est un $\mathbb{Z}[\rho(q)]$-module projectif.

Preuve. Notons $\rho = \varphi_q(\rho(q))$ et ρ_1 l'image réciproque de ρ par $(\mathbb{Z}/pq\mathbb{Z})^* \to (\mathbb{Z}/q\mathbb{Z})^*$. Notons aussi n l'ordre de ρ. Alors l'ordre de ρ_1 est np. Montrons par l'absurde que ρ_1 est cyclique.
Suposons donc que ρ_1 ne soit pas cyclique. Par conséquent, $(\mathbb{Z}/pq\mathbb{Z})^*$ n'est pas cyclique, et donc pq est une puissance de 2 supérieure ou égale à 8. Donc $p = 2$ et 4 divise q. On a alors $(\mathbb{Z}/pq\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{s-1}\mathbb{Z}$, et donc, comme ρ_1 n'est pas cyclique, nécessairement $-1 \in \rho_1$, d'où $-1 \in \rho$. Ainsi, ρ est un sous-groupe cyclique de $(\mathbb{Z}/q\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{s-2}\mathbb{Z}$ contenant -1. On en déduit que $\rho = \{1, -1\}$: c'est absurde! Donc ρ_1 est cyclique.
Soit $t \in \mathbb{Z}$ dont la classe dans $(\mathbb{Z}/pq\mathbb{Z})^*$ engendre ρ_1. L'ordre de ρ_1 étant strictement plus grand que n, pq ne divise pas $t^n - 1$. Or la classe de t dans $(\mathbb{Z}/q\mathbb{Z})^*$ engendre ρ, donc q divise $t^n - 1$. On peut donc écrire $t^n - 1 = aq$ avec $a \wedge q = 1$. On se donne alors $\tau \in \rho(q)$ tel que $\phi_q(\tau) = t \pmod q$. Alors τ engendre $\rho(q)$ et J_q est l'idéal de $\mathbb{Z}[\rho(q)]$ engendré par $\tau - t$ et q: pour le voir, il suffit de remarquer que les $(\tau - t)^k$ pour $0 \leq k \leq n - 1$ forment une base du groupe abélien libre $\mathbb{Z}[\rho(q)]$. Notons M l'idéal engendré par $\tau - t$ et a. Comme $a \wedge q = 1$, on a $J_q + M = \mathbb{Z}[\rho(q)]$, et donc $J_q M = J_q \cap M$, d'où la suite exacte de $\mathbb{Z}[\rho(q)]$-modules:

$$0 \to J_q M \to J_q \oplus M \to \mathbb{Z}[\rho(q)] \to 0$$

où l'application $J_q \oplus M \to \mathbb{Z}[\rho(q)]$ est donnée par $(j, m) \mapsto j - m$. Cette suite est scindée puisque $\mathbb{Z}[\rho(q)]$ est projectif. Donc $J_q \oplus M = J_q M \oplus \mathbb{Z}[\rho(q)]$.
Remarquons que l'idéal $J_q M$ est engendré par $(\tau - t)^2$, $a(\tau - t)$, $q(\tau - t)$ et aq. Comme $aq = t^n - \tau^n$ et $a \wedge q = 1$, on a $J_q M = (\tau - t)\mathbb{Z}[\rho(q)]$, qui est un $\mathbb{Z}[\rho(q)]$-module libre. Par conséquent, $J_q \oplus M$ est libre, et donc J_q est projectif. □

Pour la preuve de la proposition suivante, nous aurons besoin du petit lemme suivant:

Lemme 4.6.3. ***Idéaux d'indice une puissance de 2***
Soit I un idéal de $\mathbb{Z}[\zeta_{2^r}]$ d'indice $2^{r'}$. Alors $I = (1 - \zeta_{2^r})^{r'}$.

Preuve. L'anneau $\mathbb{Z}[\zeta_{2^r}]$ est un anneau de Dedekind. Écrivons $I = \mathfrak{p}_1^{n_1}...\mathfrak{p}_s^{n_s}$ avec les $\mathfrak{p}_i$ premiers non nuls deux à deux distincts et n_i entiers naturels non nuls. En calculant la norme, on a $\prod N(\mathfrak{p}_i)^{n_i} = 2^{r'}$. Donc pour tout i, $\mathfrak{p}_i \cap \mathbb{Z} = 2\mathbb{Z}$. La preuve du théorème 2.2.9 permet alors de conclure que $s = 1$ et que $\mathfrak{p}_1 = (1-\zeta_{2^r})$. Le calcul de la norme donne alors que $n_1 = r'$. □

Nous sommes à présent en mesure d'établir le résultat suivant:

Proposition 4.6.4. ***Lien entre J_q et les extensions transcendantes pures*** *Supposons $\rho(q)$ cyclique. Supposons de plus que $p = 2$. Alors $l(J_q)^\pi$ est une extension transcendante pure de l^π.*

Preuve. Quitte à remplacer l par $l^{\pi(q)}$, on peut supposer $\pi = \rho(q)$.
Supposons d'abord que 4 ne divise pas q ou que $\varphi_q(\rho(q)) \neq \{-1, 1\}$. Alors, d'après 4.6.2, J_q est un $\mathbb{Z}[\pi]$-module projectif. Donc, d'après 4.5.8, il suffit de voir que $F_\rho(J_q)$ est cyclique pour tout quotient ρ de π. Soit donc ρ un tel quotient, et notons 2^r son ordre. Comme $\mathbb{Z}[\pi]/J_q$ est un groupe de torsion, d'après 4.5.2, $F_\rho(J_q)$ est un sous-module de $F_\rho(\mathbb{Z}[\pi]) \cong \mathbb{Z}(\rho) \cong \mathbb{Z}[\zeta_{2^r}]$ d'indice une puissance de 2. D'après le lemme précédent, $F_\rho(J_q)$ est libre, d'où le résultat.
Supposons maintenant que 4 divise q et que $\varphi_q(\rho(q)) = \{-1, 1\}$. Notons $\rho(q) = \{1, \tau\}$, avec $\varphi_q(\tau) = -1$. Notons $x = 1 + \tau$ et $y = \frac{1}{2}q(1 - \tau)$. Une vérification immédiate montre que $J_q = \mathbb{Z}x \oplus \mathbb{Z}y$, et on a $\tau \cdot x = x$ et $\tau \cdot y = -y$. Donc $l(J_q) = l(x, y)$, où $\tau(x) = x$ et $\tau(y) = y^{-1}$. Soit $\alpha \in l$ tel que $\tau(\alpha) \neq \alpha$, et posons $z = \frac{\alpha y + \tau(\alpha)}{y+1}$. On a alors $\tau(z) = z$, et donc $l(x, y)^\pi = l^\pi(x, z)$, avec x et z algébriquement indépendants sur l^π. □

Pour $m \in \mathbb{Z}$, notons $ord(m)$ la valuation p-adique de p dans m. Nous aurons besoin dans la suite du lemme arithmétique suivant:

Lemme 4.6.5. ***Un lemme d'arithmétique élémentaire***
Supposons p impair. Soit $t \in \mathbb{Z}$ non divisible par p. Soit f l'ordre de sa classe modulo p dans $(\mathbb{Z}/p\mathbb{Z})^*$. Alors:

(i) $ord(\phi_f(t)) = ord(t^f - 1) > 0$,
$ord(\phi_{fp^i}(t)) = 1$ *pour* $i > 0$,
$ord(\phi_d(t)) = 0$ *pour d ne s'écrivant pas sous la forme fp^i pour $i \geq 0$.*

(ii) $ord(t^m - 1) = 0$ *si $m > 0$ n'est pas multiple de f,*
$ord(t^m - 1) = ord(t^f - 1) + ord(m)$ *si $m > 0$ est multiple de f.*

Preuve. Soit $m > 0$.
Si f ne divise pas m, alors $ord(t^m - 1) = 0$, et comme $\phi_m(t) \mid t^m - 1$, $ord(\phi_m(t)) = 0$.
Supposons à présent que f divise m. Écrivons $m = fp^i n$, avec n non multiple de

p. Notons $r = fp^i$.
Supposons d'abord $n > 1$. Avec la formule du binôme,

$$\frac{t^m - 1}{t^r - 1} = \frac{((t^r - 1) + 1)^n}{t^r - 1} = \sum_{0 \leq i \leq n-1} C_n^{i+1}(t^r - 1)^i \equiv n(mod p)$$

donc $ord(t^m - 1) = ord(t^r - 1)$. De plus, comme $\phi_m(t) | \frac{t^m-1}{t^r-1}$, $ord(\phi_m(t)) = 0$.
On est donc maintenant ramenés à étudier le cas où $n = 1$. Supposons que $i > 0$. Notons $s = fp^{i-1}$. Encore avec la formule du binôme, on a:

$$\frac{t^m - 1}{t^s - 1} = \frac{((t^s - 1) + 1)^p}{t^s - 1} = \sum_{0 \leq i \leq p-1} C_p^{i+1}(t^s - 1)^i \equiv p(mod p^2)$$

donc $ord(t^m - 1) = ord(t^s - 1) + 1$. De plus,

$$\frac{t^m - 1}{t^s - 1} = \prod_{d|m, d\nmid s} \phi_d(t)$$

et donc, comme le seul d tel que $f \mid d \mid m$ mais $d \nmid s$ est m, on a $ord(\phi_m(t)) = 1$. Finalement, une récurrence simple donne que $ord(t^m - 1) = ord(t^f - 1) + ord(m)$, et on a terminé. □

Si K est une extension cyclique de k contenue dans l, alors $Gal(K|k)$ est un quotient cyclique de π. Nous noterons F_K au lieu de $F_{Gal(K|k)}$. Nous pouvons maintenant montrer la proposition suivante:

Proposition 4.6.6. ***Calculs de*** $F_K(J_q)$
Supposons p impair. Soit τ un générateur de $\rho(q)$, et soit $t \in \mathbb{Z}$ tel que $\tau(\zeta_q) = \zeta_q^t$. Soit f l'ordre de $t \mod p$ dans $(\mathbb{Z}/p\mathbb{Z})^*$, et soit r tel que $p^r = q \wedge (t^f - 1)$. On a alors:

(a) Tout corps intermédiaire $k \subseteq K \subseteq k(\zeta_q)$ est uniquement déterminé par le degré $[K : k]$. De plus, le groupe $\rho_K = Gal(K|k)$ est cyclique, engendré par l'image τ_K de τ dans ρ_K.

(b) (i) Si $K = k(\zeta_p)$, alors $K = k(\zeta_{p^i})$ pour tout $1 \leq i \leq r$, $[K : k] = f$, et $F_K(J_q)$ est isomorphe à l'idéal $(p, \tau_K - t)^r$ en tant que $\mathbb{Z}(\rho_K)$-module.

(ii) Si $K = k(\zeta_{p^i})$ pour $r < i \leq s$, alors $[K : k] = fp^{i-r}$, et $F_K(J_q)$ est isomorphe à l'idéal $(p, \tau_K - t)$ en tant que $\mathbb{Z}(\rho_K)$-module.

(iii) Pour tous les autres corps intermédiaires $k \subseteq K \subseteq k(\zeta_q)$, $F_K(J_q)$ est isomorphe à $\mathbb{Z}(\rho_K)$ en tant que $\mathbb{Z}(\rho_K)$-module.

Preuve.

(a) Immédiat d'après la théorie de Galois et en tenant compte du fait que $k(\zeta_q)|k$ est cyclique.

(b) Soit $1 \leq i \leq s$. La théorie de Galois impose que $[k(\zeta_{p^i}) : k]$ est le plus petit entier strictement positif m tel que $\tau^m(\zeta_{p^i}) = \zeta_{p^i}$, c'est-à-dire tel que p^i divise $t^m - 1$. Avec le lemme précédent, on déduit que $[k(\zeta_{p^i}) : k] = f$ si $1 \leq i \leq r$, $[k(\zeta_{p^i}) : k] = fp^{i-r}$ sinon. En combinant avec (a), cela permet d'établir que si $K = k(\zeta_p)$, alors $K = k(\zeta_p^i)$ pour $1 \leq i \leq r$.
Soit K un corps intermédiaire entre k et $k(\zeta_q)$. Soit $d = [K : k]$. On a clairement $d|fp^{s-r}$. Rappelons que la suite $0 \to J_q \to \mathbb{Z}[\rho(q)] \to \mathbb{Z}/q\mathbb{Z} \to 0$ est exacte. En tensorisant par $\mathbb{Z}(\rho_K)$ au-dessus de $\mathbb{Z}[\rho(q)]$, on obtient la suite exacte de $\mathbb{Z}(\rho_K)$-modules suivante:

$$J_q \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \to \mathbb{Z}[\rho(q)] \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \to \mathbb{Z}/q\mathbb{Z} \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \to 0$$

D'après 4.6.2, J_q est projectif, donc $J_q \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) = F_K(J_q)$. De plus, $F_K(\mathbb{Z}[\rho(q)]) = \mathbb{Z}[\rho(q)] \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \cong \mathbb{Z}(\rho_K)$. Comme $\mathbb{Z}[\rho(q)]/J_q$ est un groupe de torsion, la proposition 4.5.2 impose que la flèche

$$J_q \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \to \mathbb{Z}[\rho(q)] \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K)$$

est injective, d'où l'exactitude de la suite:

$$0 \to J_q \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \to \mathbb{Z}[\rho(q)] \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \to \mathbb{Z}/q\mathbb{Z} \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \to 0$$

Comme $\mathbb{Z}(\rho_K) = \mathbb{Z}[\rho(q)]/\phi_d(\tau)\mathbb{Z}[\rho(q)]$, on a:

$$\mathbb{Z}/q\mathbb{Z} \otimes_{\mathbb{Z}[\rho(q)]} \mathbb{Z}(\rho_K) \cong (\mathbb{Z}/q\mathbb{Z})/\phi_d(\tau)(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q\mathbb{Z} + \phi_d(t)\mathbb{Z})$$

On en déduit la suite exacte:

$$0 \to F_K(J_q) \to \mathbb{Z}(\rho_K) \to \mathbb{Z}/(q\mathbb{Z} + \phi_d(t)\mathbb{Z}) \to 0$$

Dans le cas (iii), d'après le lemme précédent, $q \wedge \phi_d(t) = 1$, et donc $F_K(J_q) \cong \mathbb{Z}(\rho_K)$. Dans le cas (ii), encore d'après le lemme précédent, $q \wedge \phi_d(t) = p$, donc $F_K(J_q)$ est d'indice p dans $\mathbb{Z}(\rho_K)$. Comme il contient $(p, \tau_K - t)$ qui est d'indice au plus p, $F_K(J_q) \cong (p, \tau_K - t)$. Dans le cas (i), $q \wedge \phi_d(t) = p^r$, donc $F_K(J_q)$ est d'indice p^r dans $\mathbb{Z}(\rho_K)$. Comme il contient $(p, \tau_K - t)^r$ qui est d'indice au plus p^r, $F_K(J_q) \cong (p, \tau_K - t)^r$.

□

Nous pouvons finalement énoncer la proposition suivante, qui permet de relier le module $F_K(J_q)$ à l'idéal $\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z})$:

Corollaire 4.6.7. ***Lien entre*** $F_K(J_q)$ ***et l'idéal*** $\mathfrak{a}(\mathbb{Z}/q\mathbb{Z})$
Supposons $p \neq 2$. Soit K un corps intermédiaire $k \subset K \subset l$ tel que $\rho_K = Gal(K|k)$ est cyclique. Alors on a les isomorphismes de $\mathbb{Z}(\rho_K)$-modules suivants:

(i) Si $K \subseteq k(\zeta_q)$, $F_K(J_q) \cong \mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z})$.

(ii) Si $K \nsubseteq k(\zeta_q)$, $F_K(J_q) = 0$.

Preuve. Il s'agit ici de revenir à la définition de $\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z})$ et d'utiliser la proposition précédente. On reprend les notations de la proposition précédente.
Supposons que $K \subseteq k(\zeta_q)$. En reprenant les notations de la partie 4.2, on a

$$\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z}) = \prod_{(a,b)\in T} \mathfrak{a}_K(a^b)^{m(\mathbb{Z}/q\mathbb{Z},a,b)}$$

- Si $K = k(\zeta_p)$:
  *dès que $a \neq p$, $m(\mathbb{Z}/q\mathbb{Z}, a, b) = 0$.
  *si $1 \leq b \leq r$, $\mathfrak{a}_K(p^b) = (\tau_K - t, p)$ et $m(\mathbb{Z}/q\mathbb{Z}, p, b) = 1$.
  *si $r < b \leq s$, $\mathfrak{a}_K(p^b) = \mathbb{Z}(\rho_K)$.
  *si $s < b$, $m(\mathbb{Z}/q\mathbb{Z}, p, b) = 0$.
  Donc $\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z}) = (p, \tau_K - t)^r \cong F_K(J_q)$.

- Si $K = k(\zeta_{p^i})$ pour $r < i \leq s$:
  *dès que $a \neq p$, $m(\mathbb{Z}/q\mathbb{Z}, a, b) = 0$.
  *$\mathfrak{a}_K(p^i) = (\tau_K - t, p)$ et $m(\mathbb{Z}/q\mathbb{Z}, p, i) = 1$.
  *si $b \leq s$ et $b \neq i$, $\mathfrak{a}_K(p^b) = \mathbb{Z}(\rho_K)$.
  *si $s < b$, $m(\mathbb{Z}/q\mathbb{Z}, p, b) = 0$.
  Donc $\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z}) = (p, \tau_K - t) \cong F_K(J_q)$.

- Pour tous les autres $K \subseteq k(\zeta_q)$:
  *dès que $a \neq p$, $m(\mathbb{Z}/q\mathbb{Z}, a, b) = 0$.
  *si $1 \leq b \leq s$, $\mathfrak{a}_K(p^b) = \mathbb{Z}(\rho_K)$.
  *si $s < b$, $m(\mathbb{Z}/q\mathbb{Z}, p, b) = 0$.
  Donc $\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z}) = \mathbb{Z}(\rho_K) \cong F_K(J_q)$.

Par conséquent, pour terminer la preuve, il ne reste plus qu'à voir que, si $K \nsubseteq k(\zeta_q)$, alors $F_K(J_q) = 0$. Dans ce cas, J_q est un $\mathbb{Z}[\rho(q)]$-module, mais $Gal(K|k)$ n'est pas un quotient de $\rho(q)$. Donc, en vertu de 4.5.1, $F_K(J_q) = 0$. □

4.7 Un lemme pour se ramener au cas où $car(k)$ ne divise pas l'ordre de G

Dans cette partie, nous allons montrer un lemme qui nous permettra de nous ramener à un cas où la caractéristique de k ne divise pas l'ordre de G. Pour ce faire, nous devons d'abord établir quelques lemmes préliminaires.

Lemme 4.7.1. ***Existence d'un générateur***
Soit P un groupe fini qui agit sur un corps K par automorphismes. Supposons que P agit aussi sur l'anneau $K(X)$ par $\sigma(X) = X + \lambda_\sigma$ pour $\sigma \in P$, où $\lambda_\sigma \in K$. Alors il existe $Q \in K[X]^P$ tel que $K(K(X)^P) = K(Q)$.

Preuve. Montrons d'abord que le corps des fractions L de $K[X]^P$ est $K(X)^P$. Soit $R/S \in K(X)^P$, avec $R, S \in K[X]$. Montrons que $R/S \in L$ par récurence sur $degR + degS$. Si $degR = 0$ ou si $degS = 0$, le résultat est évident. Supposons donc $degR > 0$ et $degS > 0$. On suppose de plus que R et S sont premiers entre eux et que $degR \geq degS$. Pour $\sigma \in P$, $\sigma(R)$ et $\sigma(S)$ sont premiers entre eux et $\sigma(R)/\sigma(S) = R/S$, donc il existe $\chi(\sigma) \in K^*$ tel que $\sigma(R) = \chi(\sigma)R$ et $\sigma(S) = \chi(\sigma)S$. Il est alors clair que χ est un caractère $P \to K^*$. Écrivons la division euclidienne de R par S: $R = SU + V$, avec $degV < degR$. Alors, pour $\sigma \in P$, on a $\chi(\sigma)R = \chi(\sigma)S\sigma(U) + \sigma(V)$, et donc par unicité du quotient et du reste, $\sigma(U) = U$. Par hypothèse de récurrence, $V/S \in L$ et on conclut alors que $R/S = U + V/S \in L$. Le corps des fractions de $K[X]^P$ est donc bien $K(X)^P$.
Nous avons ainsi montré que, si $K[X]^P \subseteq K$, alors $K(X)^P \subseteq K$. Le lemme est donc évident lorsque $K[X]^P \subseteq K$. Supposons donc que $K[X]^P \nsubseteq K$. Soit alors $Q \in K[X]^P - K$ de degré minimal. Montrons à présent que $K[X]^P = K^P[Q]$. Soit $R \in K[X]^P$. Montrons que $R \in K^P[Q]$ par récurrence sur $degR$. Écrivons la division euclidienne de R par Q: $R = QU + V$, $degV < degQ$. Pour $\sigma \in P$, $R = Q\sigma(U) + \sigma(V)$. Donc $\sigma(U) = U$ et $\sigma(V) = V$. Par minimalité du degré de Q, $V \in K^P$. Par hypothèse de récurrence, $U \in K^P[Q]$. Par conséquent, $R = QU + V \in K^P[Q]$. Donc $K[X]^P = K^P[Q]$. □

Le lemme que nous venons de montrer ne servira que dans la preuve du lemme suivant, qui lui jouera un rôle important dans la suite:

Lemme 4.7.2. ***Existence de d générateurs***
Soit une suite de corps $K_0 \subseteq K_1 \subseteq ... \subseteq K_d$, tous de caractéristique $p \neq 0$, et tels que, pour tout i, il existe $x_i \in K_i$ tel que $K_i = K_{i-1}(x_i)$. Soit P un p-groupe fini de K_0-automorphismes de corps de K_d tel que, pour tout $1 \leq i \leq d$ et tout $\sigma \in P$, $\sigma(x_i) - x_i \in K_{i-1}$. Alors il existe $y_1, ..., y_d$ dans K_d tels que $K_d^P = K_0(y_1, ..., y_d)$.

Preuve. On procède par récurrence sur d. Pour $d = 0$, l'énoncé est trivial. Soit $d > 0$. Supposons d'abord que x_d est transcendant sur K_{d-1}. Par hypothèse de récurrence, $K_{d-1}^P = K_0(y_1, ..., y_{d-1})$ avec $y_i \in K_{d-1}$. D'après le lemme

précédent, on peut trouver $y_d \in K_d^P$ tel que $K_{d-1}(K_d^P) = K_{d-1}(y_d)$. Alors $K_d^P = (K_{d-1}(K_d^P))^P = K_{d-1}(y_d)^P = K_{d-1}^P(y_d) = K_0(y_1, ..., y_d)$.
Supposons maintenant que x_d est algébrique sur K_{d-1}. Soit Q son polynôme minimal. Alors $K_d \cong K_{d-1}[X]/(Q)$. Pour $\sigma \in P$, soit $\lambda_\sigma \in K_{d-1}$ tel que $\sigma(x_d) - x_d = \lambda_\sigma$. On peut alors faire agir P sur $K_{d-1}(X)$ par $\sigma(X) = X + \lambda_\sigma$. Comme avant, on trouve $y_1, ..., y_{d-1}, y'_d \in K_{d-1}(X)$ tels que $K_{d-1}(X)^P = K_0(y_1, ..., y_{d-1}, y'_d)$. Soit alors y_d la classe de y'_d dans K_d. Alors $K_d^P = K_0(y_1, ..., y_d)$. □

Finalement, nous aurons aussi besoin du petit lemme suivant:

Lemme 4.7.3. ***Existence d'un point fixe***
Soient K un corps de caractéristique $p \neq 0$ et P un p-groupe fini. Considérons M un $K[P]$-module non nul. Alors $M^P \neq 0$.

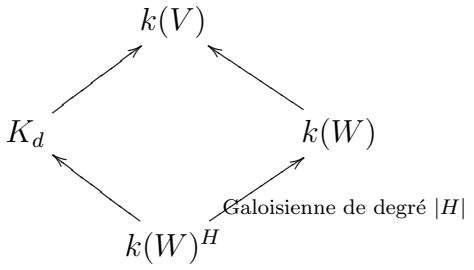
Preuve. Soit $m \in M$, non nul. Soit le sous-groupe $N = \sum_{g \in P}(gm)\mathbb{Z}$. Le groupe P agit sur N, qui est un $\mathbb{F}_p$-espace vectoriel non nul de dimension finie. Comme P est un p-groupe, $Card(N^P) \equiv Card(N) \pmod p$, donc p divise $Card(N^P)$. Par conséquent, N^P n'est pas trivial, donc $M^P \neq 0$. □

Supposons que k est de caractéristique non nulle. Notons $car(k) = p$. À l'aide de la classification des groupes abéliens de type fini, nous pouvons écrire $G = P \times H$ où P est un p-Sylow de G. Nous pouvons alors énoncer la proposition suivante:

Proposition 4.7.4. ***Un lemme pour éviter les problèmes de caractéristique***
Le corps k_G est k-isomorphe à une extension transcendante pure de k_H.

Preuve. Considérons V le sous-k-espace vectoriel de $k(V) = k(\{x_g, g \in G\})$ engendré par les x_g, pour $g \in G$. L'espace vectoriel V, vu comme un $k[G]$-module, est isomorphe à $k[G]$. On regarde le sous-espace W fixe par P (i.e. $W = V^P$), c'est un $k[H]$-module isomorphe à $k[H]$. On peut ainsi reformuler l'énoncé à montrer: $k(V)^G$ est une extension transcendante pure de $k(W)^H$, où $k(W)$ désigne le corps engendré par k et W dans $k(V)$. La codimension de W dans V est égale à $d = |G| - |H|$.
On note U le $k(W)$-espace vectoriel engendré par V dans $k(V)$, alors $dim_{k(W)}U = d + 1$, $1 \in U$, et H agit de façon semi-linéaire sur U. On note $T = U^H$. Alors par le lemme 4.4.1, T est un $k(W)^H$-espace vectoriel de dimension $d + 1$ contenant 1. Remarquons que T est un $k(W)^H[P]$-module car $\sigma T = T$ pour tout $\sigma \in P$. On note $Y_0 = k(W)^H.1$ et on veut trouver une suite $(Y_i)_{0 \leq i \leq d}$ de $k(W)^H[P]$-sous-modules de T telle que les $k(W)^H(Y_i)$ vérifient les conditions du lemme 4.7.2. Pour ce faire, on construit successivement les Y_i de telle sorte que $Y_{i-1} \subseteq Y_i$ et Y_i/Y_{i-1} est un $k(W)^H$-espace vectoriel de dimension 1 sur lequel P agit trivialement: il suffit d'appliquer le lemme précédent à $M = T/Y_{i-1}$ pour trouver Y_i. On a $Y_d = T$ pour des raisons de dimension.

Soit $u_i \in Y_{i-1}$ tel que $Y_i = Y_{i-1} + k(W)^H u_i$ pour $1 \leq i \leq d$. On note ensuite K_i le corps engendré par $k(W)^H$ et Y_i, pour $0 \leq i \leq d$. On a $K_0 = k(W)^H$, et montrons que $K_d = k(V)^H$. En effet, remarquons d'abord que $K_d = k(W)^H(T) = k(W)^H(U^H)$, donc $K_d \subseteq k(V)^H$. Avec 4.4.1, soit $(b_0, ..., b_d)$ une base du $k(W)$-espace vectoriel U fixée par H. Alors $(b_0, ..., b_d)$ est une base du $k(W)^H$-espace vectoriel U^H d'où $K_d = k(W)^H(b_0, ..., b_d)$. On a aussi $k(V) = k(W)(U) = k(W)(b_0, ..., b_d)$. On a donc le diagramme:



Avec le théorème de l'élément primitif, prenons z tel que $k(W) = k(W)^H(z)$. Alors $k(V) = K_d(z)$ et donc $[K(V) : K_d] \leq |H|$. Comme $[k(V) : k(V)^H] = |H|$, on a bien $K_d = k(V)^H$. Par le lemme 4.7.2, $K_d^P = K_0(z_1, \ldots, z_d)$, pour certains $z_1, \ldots, z_d \in K_d$. Or $k(V)^G = (k(V)^H)^P = k(W)^H(z_1, \ldots, z_d)$. En plus, le degré de transcendance de $k(V)^G$ (resp. $k(W)^H$) sur k est le même que celui de $k(V)$ (resp. $k(W)$) sur k, donc le degré de transcendance de $k(V)^G$ sur $k(W)^H$ est égal à $|G| - |H| = d$. Or $K_d^P = K_0(z_1, \ldots, z_d)$, donc $z_1, \ldots, z_d$ sont algébriquement indépendants, et on a montré que $k(V)^G$ est une extension transcendante pure de $k(W)^H$, d'où le théorème. □

4.8 Preuve du théorème de Lenstra

Comme dans la section précédente, on écrit $G = P \times H$ où P est un p-groupe ($p = car(k)$) et H d'ordre premier à p. On note e l'exposant de H et on considère le corps $l = k(\zeta_e)$ ainsi que le groupe de Galois $\pi = Gal(l/k)$. Par la réduction au-dessus, on s'intéresse d'abord au groupe H.
On considère alors le groupe dual $D = Hom(H, l^*)$ de H, qui est lui aussi un groupe abélien isomorphe à H. On voit D comme un π-module en définissant l'action par $(\sigma d)(g) = \sigma(d(g))$ pour $\sigma \in \pi$, $d \in D$ et $g \in H$. On définit ensuite un module de permutation $\mathbb{Z}^D$ qui en tant que groupe abélien libre est engendré par les éléments $(e_d)_{d \in D}$ sur $\mathbb{Z}$ et tel que $\sigma e_d = e_{\sigma d}$, pour $\sigma \in \pi$ et $d \in D$. On a alors une suite exacte $0 \to J \to \mathbb{Z}^D \to D \to 0$, où $J = Ker(\mathbb{Z}^D \underset{e_d \mapsto d}{\longrightarrow} D)$.

Proposition 4.8.1. ***Un premier isomorphisme***
On a $k_H \cong l(J)^\pi$ sur $k = l^\pi$.

Preuve. On définit $l(x) = l(\{x_g | g \in H\})$ et $k(x) = k(\{x_g | g \in H\})$. La méthode consiste à montrer que $l_H \cong l(J)$, puis descendre à k.
On s'intéresse donc à $l_H = l(x)^H$. On note, pour tout $d \in D$, l'expression $y_d = (\sum_{g \in H} d(g)^{-1} \cdot x_g) \in l(x)$. Cette transformation est inversible, donc $l(x) = l(\{y_d | d \in D\})$, et on vérifie facilement que l'action de H sur $l(\{y_d\})$ est donnée par $g(y_d) = d(g) \cdot y_d$ ($\forall g \in H$, $d \in D$). On note $F \subset l(x)^*$ le sous-groupe multiplicatif engendré par les $(y_d)_{d \in D}$. Alors F est libre et de rang $|D| = |H|$. On définit le morphisme $\phi : F \to D$ qui envoie y_d sur d, et on vérifie la relation: $g(y) = \phi(y)(g) \cdot y$ pour tout $y \in F$ et $g \in H$.
On a $l(ker(\phi)) \subset l_H \subset l(x) = l(F)$. En effet, si $y \in ker(\phi)$, alors $g(y) = y$ pour tout $y \in H$, i.e. $y \in l_H$. En plus, comme l'indice de $ker(\phi)$ dans F est égal à $|D|$, et alors $[l(F) : l(ker(\phi))] \leq |D|$ (en effet, considérons une base de $l(F)$ sur $l(ker(\phi))$ contenue dans une $\mathbb{Z}$-base de F; si son cardinal est plus grand que $|D|$, alors il existe deux élément qui sont dans la même classe, ce qui n'est pas possible). Mais on a aussi $[l(F) : l_H] = |D|$ par la théorie de Galois, ce qui montre que $l(ker(\phi)) = l_H$. Comme en plus une $\mathbb{Z}$-base de $ker(\phi)$ est algébriquement libre sur l, $l(ker(\phi))$ est le corps des fractions de $l[ker(\phi)]$.
On a décrit l_H, et maintenant on peut s'intéresser à k. L'action de π sur l induit une action sur $l(x) \cong l \otimes_k k(x)$. On vérifie que l'action de π et l'action de H sur $l(x)$ commutent. On en déduit que $k_H = (l(x)^\pi)^H = (l(x)^H)^\pi = (l_H)^\pi$. Un calcul montre que $\sigma(y_d) = y_{\sigma d}$ pour $\sigma \in \pi$ et $d \in D$, ce qui montre que $F \cong \mathbb{Z}^D$ en tant que sous-π-module de $l(x)^*$. Comme l'application $\phi : F \to D$ est π-linéaire, on a $ker(\phi) \cong J$, et alors on a $l_H = l(ker(\phi)) \cong l(J)$ sur l. Cet isomorphisme est bien compatible avec l'action de π, donc il induit un isomorphisme $k_H = (l_H)^\pi \cong l(J)^\pi$ sur $k = l^\pi$, et c'est bien ce que l'on cherchait à montrer. □

Il est temps de faire intervenir les modules I_q et J_q définis avant. On écrit l'isomorphisme de groupes

$$H \cong \underset{q}{\oplus} (\mathbb{Z}/q\mathbb{Z})^{n(q)}$$

où q décrit les puissances (distinctes de 1) des nombres premiers. Distinguons des cas selon la parité de q et la cyclicité de $\rho(q)$: définissons les π-modules I_1, I_2, I_3 par

$$I_1 = \bigoplus_{q \ impair} J_q^{n(q)}$$

$$I_2 = \bigoplus_{\rho(q) \ non \ cyclique} I_q^{n(q)}$$

$$I_3 = \bigoplus_{q \ pair, \ \rho(q) \ cyclique} J_q^{n(q)}$$

On note $I = I_1 \oplus I_2$. Dans la suite, nous trouverons des conditions pour que $I = I_1$.

Proposition 4.8.2. ***Un deuxième isomorphisme***
$l(J)^\pi$ est l^π-isomorphe à une extension transcendante pure de $l(I)^\pi$.

Preuve. On décompose $H \cong D = \bigoplus_q (\mathbb{Z}/q\mathbb{Z})^{n(q)}$, chaque composante étant munie d'une struture de π-module définie dans la partie 4.6. On adoptera les notations et résultats déjà introduits dans la partie 4.6.
On dit qu'un ensemble E est un π-ensemble si π agit sur E comme un groupe de permutations (on n'exige pas que cette action soit fidèle). Soit q une puissance d'un nombre premier. Distinguons alors les deux cas suivants:
• Cas 1: $\rho(q)$ est non cyclique.
Considérons une application injective $\mathbb{Z}/q\mathbb{Z} \to D$ qui identifie $\mathbb{Z}/q\mathbb{Z}$ à un facteur de D. Elle est π-linéaire, elle induit donc une injection de π-ensembles $C(q) \subset \mathbb{Z}/q\mathbb{Z} \to D$, et on peut alors définir une application π-linéaire $\mathbb{Z}^{C(q)} \to \mathbb{Z}^D$. On a donc le diagramme suivant, et on vérifie facilement qu'il est commutatif:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_q & \longrightarrow & \mathbb{Z}^{C(q)} & \longrightarrow & \mathbb{Z}/q\mathbb{Z} & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & J & \longrightarrow & \mathbb{Z}^D & \longrightarrow & D & \longrightarrow & 0 \end{array}$$

• Cas 2: $\rho(q)$ est cyclique.
Considérons une application injective $\mathbb{Z}/q\mathbb{Z} \to D$ qui identifie $\mathbb{Z}/q\mathbb{Z}$ à un facteur de D. Elle est π-linéaire, elle induit donc une injection de π-ensembles $\rho(q) \underset{\varphi_q}{\to} (\mathbb{Z}/q\mathbb{Z})^* \subset \mathbb{Z}/q\mathbb{Z} \to D$, et on peut alors définir une application π-linéaire $\mathbb{Z}[\rho(q)] \to \mathbb{Z}^D$. On a donc le diagramme suivant, et on vérifie facilement qu'il est commutatif:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J_q & \longrightarrow & \mathbb{Z}[\rho(q)] & \xrightarrow{\varphi_q} & \mathbb{Z}/q\mathbb{Z} & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & J & \longrightarrow & \mathbb{Z}^D & \longrightarrow & D & \longrightarrow & 0 \end{array}$$

• Finalement, en combinant ces deux diagrammes, on obtient le diagramme commutatif suivant:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_1 \oplus I_2 \oplus I_3 & \longrightarrow & \mathbb{Z}^E & \longrightarrow & \bigoplus_q (\mathbb{Z}/q\mathbb{Z})^{n(q)} & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow \cong & & \\ 0 & \longrightarrow & J & \longrightarrow & \mathbb{Z}^D & \longrightarrow & D & \longrightarrow & 0 \end{array}$$

E désigne ici un π-ensemble qui est en fait une réunion disjointe de $C(q)$ et $\rho(q)$ avec certaines multiplicités. On veut voir E comme un sous-π-ensemble de D, il

faut donc vérifier que les images de $C(q)$ et $\rho(q)$ ne superposent pas dans D. C'est effectivment le cas car $0 \notin C(q) \subset \mathbb{Z}/q\mathbb{Z}$ et $0 \notin \varphi_q[\rho(q)] \subset \mathbb{Z}/q\mathbb{Z}$. Ainsi l'injection $\mathbb{Z}^E \to \mathbb{Z}^D$ admet un co-noyau N qui est un module de permutation sur π. On obtient alors facilement une suite exacte de π-modules:

$$0 \to I \oplus I_3 \to J \to N \to 0$$

où N est un module de permutation. On applique le lemme 4.4.4, et $l(J)^\pi$ est donc isomorphe à une extension transcendante pure de $l(I \oplus I_3)^\pi$. Mais $l(I \oplus I_3)^\pi$ est une extension transcendante pure de $l(I)^\pi$ d'après le lemme 4.6.4. D'où la proposition. □

Proposition 4.8.3. ***Une extension transcendante pure***
k_G est k-isomorphe à une extension transcendante pure de $l(I)^\pi$.

Preuve. Immédiat à l'aide de 4.7.4, 4.8.1 et 4.8.2. □

Proposition 4.8.4. ***Cohomologie de I***
Pour tout sous-groupe $\pi' \subset \pi$ on a $H^1(\pi', I) = 0$.

Preuve. La preuve suit immédiatement des lemmes 4.6.1, 4.6.2 et de la définition de I. □

Proposition 4.8.5. ***Lien entre $F_K(I_1)$ et $\mathfrak{a}_K(G)$***
Soit K un corps intermédiaire entre k et l (i.e. $k \subset K \subset l$) tel que $\rho_K = Gal(K/k)$ est cyclique. Alors $F_K(I_1)$ est $\mathbb{Z}(\rho_K)$-libre ssi l'idéal $\mathfrak{a}_K(G)$ de $\mathbb{Z}(\rho_K)$ est principal.

Preuve. Pour obtenir ce résultat, on utilisera essentiellement un lemme sur les anneaux de Dedekind, facilement obtenu en utilisant par exemple la classification des modules sur un anneau de Dedekind.
Soient $\alpha_1, \ldots, \alpha_n$ des idéaux non nuls d'un anneau de Dedekind, alors leur somme directe est libre (sur cet anneau de Dedekind) ssi leur produit est un idéal principal. En effet, il suffit de voir que $\alpha_1 \oplus \cdots \oplus \alpha_n$ est isomorphe à la somme directe d'un module libre de rang $n-1$ et de $\alpha_1 ... \alpha_n$ d'après le lemme 2.1.10. À l'aide de la classification des modules de type fini sur un anneau de Dedekind, on déduit que $\alpha_1 \oplus \cdots \oplus \alpha_n$ est libre si, et seulement si, $\alpha_1 ... \alpha_n$ est libre, i.e principal.
Le reste de cette démonstration suit du lemme 4.6.7 qui met en relation F_K et $\mathfrak{a}_K$. En effet, $F_K(I_1)$ est somme directe de certains $\mathfrak{a}_K(\mathbb{Z}/q\mathbb{Z})$ par le lemme 4.6.7, et $\mathfrak{a}_K(G)$ est, par définition, le produit de ces mêmes $\mathbb{Z}(\rho_K)$-idéaux. Comme $\mathbb{Z}(\rho_K)$ est un anneau de Dedekind, la proposition découle immédiatement. □

Maintenant on est en mesure de reformuler la condition (i) dans l'énoncé du théorème principal.

Proposition 4.8.6. ***Équivalents de (i) du théorème de Lenstra***
Les assertions suivantes sont équivalentes:
(a) Le corps $l(I_1)^\pi$ est une extension transcendante pure de l^π.
(b) Il existe une extension transcendante pure L de $l(I_1)^\pi$, de degré de transcendance fini, qui est aussi transcendante pure sur l^π.
(c) La condition (i) du théorème de Lenstra est vérifiée.

Preuve. D'après le lemme 4.6.2, les hypothèses pour pouvoir appliquer le théorème 4.5.8 à $I_1 = M$ sont satisfaites. Il suffit donc de voir que 4.5.8(iii) est équivalente à (c). Or cela est une conséquence immédiate de 4.8.5. □

Maintenant il ne reste qu'à combiner tous les résultats pour démontrer le théorème de Lenstra. Pour nous débarrasser de I_2, nous nous intéresserons à $\widehat{H}^{-1}$.

Preuve. **Preuve du théorème de Lenstra**
Supposons d'abord que les conditions du théorème soient satisfaites. Alors $I = I_1$, et alors k_G est isomorphe à une extension transcendante pure de $l(I)^\pi$ sur l^π par la proposition 4.8.3, mais $l(I)^\pi$ est une extension transcendante pure de l^π par la proposition précédente. Donc k_G est une extension transcendante pure de k.
Réciproquement, si k_G est une extension transcendante pure de l^π, alors d'après 4.8.3 il existe une extension transcendante pure L de $l(I)^\pi$, de degré de transcendance fini, qui est aussi transcendante pure sur l^π en vertu de l'isomorphisme $k_G \cong l^\pi$ sur l^π. Nous pouvons appliquer le lemme 4.4.6 au I grâce lemme 4.8.4, ce qui montre l'existence de deux π-modules de permutation N_1 et N_2 (de type fini) tels que $I \oplus N_1 \cong N_2$. L'étude de la cohomologie $\widehat{H}^{-1}$ faite dans les lemmes 4.3.2 et 4.6.1 permet d'établir que $n(q) = 0$ dès que $\rho(q)$ n'est pas cyclique, ce qui montre la condition (ii) du théorème. On a donc $I \cong I_1$, et la proposition précédente nous permet de conclure que (i) est aussi satisfaite. □

De la preuve du théorème de Lenstra découle l'intéressante remarque suivante:

Remarque 4.8.7. *Soit G un groupe abélien fini. Si k_G admet une extension transcendante pure de degré de transcendance fini et qui est aussi transcendante pure sur k, alors $k_G|k$ est transcendante pure.*

5 Quelques conséquences lorsque le groupe est cyclique

Dans cette partie, on supposera que le groupe G est cyclique. Le théorème de la partie précédente se réécrit alors de la manière suivante:

Théorème 5.0.8. ***Théorème de Lenstra dans le cas cyclique***
Soit n l'ordre de G. Notons V l'ensemble des $k(\zeta_{p^s})$ avec p premier distinct de $car(k)$, s entier strictement positif, et $p^s|n$. Alors $k_G|k$ est transcendante pure si, et seulement si, pour tout $K \in V$, les conditions suivantes sont vérifiées:

(i) L'extension $K|k$ est cyclique.

(ii) Si σ_K est un générateur de $Gal(K|k)$, l'idéal $I_{k,K} = \prod(p, \zeta_{[K:k]} - t_p)$ de $\mathbb{Z}[\zeta_{[K:k]}]$ est principal, où le produit est pris sur les couples (p, s) tels que p premier distinct de $car(k)$, s entier strictement positif, $p^s|n$ et $K = k(\zeta_{p^s})$ et où t_p est tel que $\sigma_K(\zeta_p) = \zeta_p^{t_p}$.

Nous en déduisons le corollaire:

Corollaire 5.0.9. ***Les cas $k = \mathbb{R}$ et $k = \mathbb{C}$***
Supposons que $k = \mathbb{R}$ ou $\mathbb{C}$. Alors $k_G|k$ est transcendante pure.

Preuve. Si $k = \mathbb{C}$, $V = \{\mathbb{C}\}$, donc pour tout $K \in V$, $K|\mathbb{C}$ est cyclique et $\mathbb{Z}[\zeta_{[K:\mathbb{C}]}] = \mathbb{Z}$ est un anneau principal, d'où le résultat.
Si $k = \mathbb{R}$, $V = \{\mathbb{R}, \mathbb{C}\}$, donc pour tout $K \in V$, $K|\mathbb{R}$ est cyclique et $\mathbb{Z}[\zeta_{[K:\mathbb{C}]}] = \mathbb{Z}$ est un anneau principal, d'où le résultat. □

Remarque 5.0.10. *On peut montrer directement ce résultat. Se référer à [Len80] (partie 2).*

Nous allons à partir de maintenant étudier le cas du corps des rationnels:

Corollaire 5.0.11. ***Le cas $n = 8$***
$\mathbb{Q}(x_1, ..., x_8)^{\mathbb{Z}/8\mathbb{Z}}$ n'est pas une extension transcendante pure de $\mathbb{Q}$.

Preuve. Dans le cas $n = 8$ et $k = \mathbb{Q}$, $\mathbb{Q}(\zeta_8)$ est dans V. Mais $Gal(\mathbb{Q}(\zeta_8)|\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ n'est pas cyclique. Donc $\mathbb{Q}_G|\mathbb{Q}$ n'est pas transcendante pure. □

Remarque 5.0.12. *De même, lorsque $k = \mathbb{Q}$, dès que n est multiple de 8, $\mathbb{Q}_G|\mathbb{Q}$ n'est pas transcendante pure.*

Le théorème suivant permet de ramener l'étude d'une extension de corps à l'étude des idéaux dans un anneau de Dedekind:

Théorème 5.0.13. ***Le cas rationnel***
Soit n l'ordre de G. Les trois propositions suivantes sont équivalentes:

(i) $\mathbb{Q}_G|\mathbb{Q}$ est trancendante pure.

(ii) Pour tout corps k, $k_G|k$ est transcendante pure.

(iii) n n'est pas multiple de 8 et pour tout nombre premier p et tout entier strictement positif s tel que n est multiple de p^s mais pas de p^{s+1}, l'anneau $\mathbb{Z}[\zeta_{(p-1)p^{s-1}}]$ a un idéal principal de norme p.

Preuve. Supposons (i). Avec la remarque 5.0.12, il est clair que n n'est pas multiple de 8. De plus, l'idéal $I_{\mathbb{Q},\mathbb{Q}(\zeta_{p^s})} = (p, \zeta_{(p-1)p^{s-1}} - t_p)$ de $\mathbb{Z}[\zeta_{(p-1)p^{s-1}}]$ est principal de norme p, d'où (iii).
Supposons (iii). Soient p et s comme décrits dans (iii). Soit $K = k(\zeta_{p^r})$ pour $r \leq s$. On sait que 8 ne divise pas n, donc $Gal(K|k)$ s'injecte dans le groupe cyclique $(\mathbb{Z}/n\mathbb{Z})^*$. Donc $K|k$ est une extension cyclique. Soit $\mathfrak{p}$ un idéal principal de $\mathbb{Z}[\zeta_{(p-1)p^{s-1}}]$ de norme p. Il est clair que $[K : k]$ divise $(p-1)p^{s-1}$, et donc, en prenant la norme de $\mathfrak{p}$ par rapport à $\mathbb{Z}[\zeta_{[K:k]}]$, on obtient un idéal principal $\mathfrak{q}$ de $\mathbb{Z}[\zeta_{[K:k]}]$ de norme p. Comme tous les idéaux de norme p de $\mathbb{Z}[\zeta_{[K:k]}]$ sont conjugués par l'action du groupe de Galois, ils sont tous principaux, donc $I_{k,K}$ est un produit d'idéaux principaux, donc principal. Donc, d'après le théorème 5.0.8, la propriété (ii) est prouvée. □

Remarque 5.0.14. *C'est ici que l'on voit clairement le lien entre le théorème de Lenstra et le contre-exemple de Swan. En effet, dans la propriété "47 est un nombre magique" (3.3.2), Swan prouve que $\mathbb{Z}[\zeta_{46}]$ ne contient pas d'idéal principal de norme 47. Il prouve donc exactement que le (iii) du théorème précédent n'est pas vérifié lorsque $n = 47$.*

Nous pouvons maintenant déduire:

Corollaire 5.0.15. ***Une simplification***
Soit n l'ordre de G. Écrivons sa décomposition en produit de facteurs premiers: $n = \prod_p p^{s_p}$. Alors $\mathbb{Q}_G|\mathbb{Q}$ est transcendante pure si, et seulement si, pour tout nombre premier p, $\mathbb{Q}_{(\mathbb{Z}/p^{s_p}\mathbb{Z})}|\mathbb{Q}$ l'est.

Preuve. Il suffit d'appliquer l'équivalence $(i) \Leftrightarrow (iii)$ du théorème précédent. □

Il suffit donc de s'intéresser au cas où l'ordre de G est une puissance d'un nombre premier.

Corollaire 5.0.16. ***Une condition suffisante pour que l'extension soit transcendante pure***
Supposons que l'ordre de G divise $2^2 \cdot 3^m \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 67 \cdot 71$ pour un certain entier naturel m. Alors $k_G|k$ est transcendante pure.

Preuve. En tenant compte des résultats précédents, il suffit de voir que pour $p^s = 2, 3^m, 4, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41, 43, 49, 61, 67, 71,$ il existe $\alpha \in \mathbb{Z}[\zeta_{(p-1)p^{s-1}}]$ de norme p. On vérifie par le calcul que les α suivants conviennent,

avec $\zeta = \zeta_{(p-1)p^{s-1}}$:

p^s	α
2	2
3^m	$1-\zeta^2$
4	2
5	$\zeta^2+\zeta-1$
7	$\zeta^3-\zeta-1$
11	$\zeta^3+\zeta^2-1$
13	$\zeta^4-\zeta-1$
17	$\zeta^3-\zeta^2-1$
19	$\zeta^4+\zeta+1$
23	$\zeta^5-\zeta^3+1$
25	$\zeta^5-\zeta^3+1$
29	$\zeta^5-\zeta^2+1$
31	$\zeta^3+\zeta+1$
37	$\zeta^5+\zeta^2+1$
41	$\zeta^8-\zeta^5+1$
43	$\zeta^6+\zeta-1$
49	$\zeta^4-\zeta-1$
61	$\zeta^6-\zeta-1$
67	$\zeta^6+\zeta+1$
71	$\zeta^7-\zeta^3+1$

Par exemple, pour $p^s = 5$, la norme de $\zeta^2+\zeta-1$ est le déterminant de $\begin{pmatrix} -2 & -1 \\ 1 & -2 \end{pmatrix}$ c'est-à-dire 5. □

Le corollaire suivant permet de traiter le cas où l'ordre de G est une puissance d'un nombre premier sans être un nombre premier:

Corollaire 5.0.17. ***Une condition nécessaire et suffisante dans un cas particulier***
Soient p un nombre premier et $s \geq 2$ un entier. Soit $G = \mathbb{Z}/p^s\mathbb{Z}$. Alors $\mathbb{Q}_G|\mathbb{Q}$ est transcendante pure si, et seulement si,

$$p^s \in \left\{2^2, 3^m, 5^2, 7^2 : m \geq 2\right\}$$

Preuve. La réciproque a déjà été montrée. La propriété directe découle immédiatement du lemme suivant et de 5.0.13. □

Lemme 5.0.18. ***Éléments de norme*** p

(i) Soit $p \geq 5$ *un nombre premier. Alors* $\mathbb{Z}[\zeta_{(p-1)p^2}]$ *n'a pas d'élément de norme* p*.*

(ii) Soit $p \geq 11$ *un nombre premier. Alors* $\mathbb{Z}[\zeta_{(p-1)p}]$ *n'a pas d'élément de norme* p*.*

Nous admettrons ce lemme dont la démonstration est indépendante de ce qui a été fait jusqu'ici. Elle se trouve dans [Len80] (lemme 5).
À ce stade, afin de résoudre le problème de Noether dans le cas d'un groupe cyclique, il ne nous reste plus qu'à étudier le cas où $G = \mathbb{Z}/p\mathbb{Z}$ avec p premier. Nous savons que la réponse est affirmative lorsque p est 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 61, 67, 71. Avec le contre-exemple de Swan, nous savons aussi que la réponse est négative lorsque $p = 47$. En fait, la preuve de Swan marche aussi de la même manière pour $p = 113$ et pour $p = 233$, ce qui prouve que pour ces nombres premiers le problème de Noether admet aussi une réponse négative. Il y a aussi des nombres premiers pour lesquels le problème est toujours ouvert: c'est par exemple le cas de 53, 59 ou 73. Essayons d'expliquer pourquoi dans ces cas-là, malgré les résultats de Swan et de Lenstra, le problème reste ouvert. D'une part, le raisonnement de Swan tombe en défaut pour ces trois valeurs. En effet, à l'exception de la proposition 3.3.2, toute la preuve de Swan reste valable pour 53, 59 et 73 au lieu de 47. Mais ces trois nombres-là ne sont pas magiques comme 47. Pour 53, on a $\mathbb{Q}(\sqrt{13}) \subset \mathbb{Q}(\zeta_{52})$, et donc par le raisonnement de Swan, il faut résoudre l'équation $x^2 - 13y^2 = 4 \cdot 53$ dans les entiers avec $x \equiv y(mod 2)$. Mais $(678, 188)$ est bien solution de cette équation et donc on n'arrive pas à une contradiction comme dans le cas 47. De même, pour 59 et 73, on obtient les équations $x^2 - 29y^2 = 4 \cdot 59$ et $x^2 + 3y^2 = 4 \cdot 73$, qui ont pour solutions respectives $(56, 10)$ et $(10, 8)$. D'autre part, le théorème de Lenstra permet de se ramener à la recherche d'un idéal principal de norme 53, 59 et 73 respectivement dans $\mathbb{Z}[\zeta_{52}]$, $\mathbb{Z}[\zeta_{58}]$ et $\mathbb{Z}[\zeta_{72}]$, mais ce nouveau problème n'est pas simple. Même si le problème reste toujours ouvert, on peut au moins se demander s'il y a beaucoup de nombres premiers pour lesquels $\mathbb{Q}_{(\mathbb{Z}/p\mathbb{Z})}$ est une extension transcendante pure de $\mathbb{Q}$. Dans [Len74] (corollaire 7.6), Lenstra a montré le théorème suivant:

Théorème 5.0.19. ***Il y a peu de nombres premiers pour lesquels l'extension est transcendante pure***
Pour $x \in \mathbb{R}$*, soit* $\pi(x)$ *le nombre de nombres premiers inférieurs ou égaux à* x*, et soit* $\pi^*(x)$ *le nombre de nombres premiers* $p \leq x$ *tels que* $\mathbb{Q}_{(\mathbb{Z}/p\mathbb{Z})}$ *est une extension transcendante pure de* $\mathbb{Q}$*. Alors*

$$\frac{\pi^*(x)}{\pi(x)} \to 0$$

Plus précisément,

$$\frac{\pi^*(x)}{\pi(x)} = O((\log\log\log x)^{-1/2})$$

Pour clore cette partie, nous pouvons faire la jolie petite remarque suivante:

Remarque 5.0.20. ***Le cas*** $k = \mathbb{F}_2$
Prenons $k = \mathbb{F}_2$. Si p est un nombre premier de Mersenne ou de Fermat, alors $k_{(\mathbb{Z}/p\mathbb{Z})}$ est une extension transcendante pure de k.

Preuve. Soit $p = 2^q - 1$ un nombre premier de Mersenne. Alors $[\mathbb{F}_2(\zeta_p) : \mathbb{F}_2] = q$. Comme $Gal(\mathbb{F}_{2^q}|\mathbb{F}_2)$ est cyclique engendré par le morphisme de Frobenius, on a $I_{\mathbb{F}_2,\mathbb{F}_2(\zeta_p)} = (p, \zeta_q - 2)$. Or $\phi_q(2) = 2^p - 1 \in (\zeta_q - 2)$, donc $I_{\mathbb{F}_2,\mathbb{F}_2(\zeta_p)} = (\zeta_q - 2)$ est principal. Donc $k_{(\mathbb{Z}/p\mathbb{Z})}$ est une extension transcendante pure de k, pour $k = \mathbb{F}_2$.
Soit maintenant $p = 2^{2^n} + 1$ un nombre premier de Fermat. Alors $[\mathbb{F}_2(\zeta_p) : \mathbb{F}_2] = [\mathbb{F}_2(\zeta_{2^{2^{n+1}}-1}) : \mathbb{F}_2] = 2^{n+1}$. Comme $Gal(\mathbb{F}_{2^{2^{n+1}}}|\mathbb{F}_2)$ est cyclique engendré par le morphisme de Frobenius, on a $I_{\mathbb{F}_2,\mathbb{F}_2(\zeta_p)} = (p, \zeta_{2^{n+1}} - 2)$. Or $\phi_{2^{n+1}}(2) = 2^{2^n} + 1 \in (\zeta_{2^{n+1}} - 2)$, donc $I_{\mathbb{F}_2,\mathbb{F}_2(\zeta_p)} = (\zeta_{2^{n+1}} - 2)$ est principal. Donc $k_{(\mathbb{Z}/p\mathbb{Z})}$ est une extension transcendante pure de k, pour $k = \mathbb{F}_2$. □

Références

[Art55] Emil Artin. The orders of the linear groups. *Comm. Pure Appl. Math.*, 8:355–365, 1955.

[CF667] *Algebraic number theory.* Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the Inter national Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press, London, 1967.

[EM73] Shizuo Endô and Takehiko Miyata. Invariants of finite abelian groups. *J. Math. Soc. Japan*, 25:7–26, 1973.

[Fis15] E. Fischer. Die isomorphie der invariantenkörper der endlichen abelschen gruppen linearer transformationen. *Nachr. Königl. Ges. Wiss., Göttingen*, 1915.

[Ker75] Michel Kervaire. Fractions rationnelles invariantes (d'après H. W. Lenstra). In *Séminaire Bourbaki, Vol. 1973/1974, 26ème année, Exp. No. 445*, pages 170–189. Lecture Notes in Math., Vol. 431. Springer, Berlin, 1975.

[Kun56] Hideo Kuniyoshi. Certain subfields of rational function fields. In *Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955*, pages 241–243, Tokyo, 1956. Science Council of Japan.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Len74] H. W. Lenstra, Jr. Rational functions invariant under a finite abelian group. *Invent. Math.*, 25:299–325, 1974.

[Len80] H. W. Lenstra, Jr. Rational functions invariant under a cyclic group. In *Proceedings of the Queen's Number Theory Conference, 1979 (Kingston, Ont., 1979)*, volume 54 of *Queen's Papers in Pure and Appl. Math.*, pages 91–99, Kingston, Ont., 1980. Queen's Univ.

[Mar71] Jacques Martinet. Un contre-exemple à une conjecture d'E. Noether d'après R. Swan. In *Séminaire Bourbaki, Vol. 1969/1970, 22ème année, Exp. No. 372*, pages 145–154. Lecture Notes in Math., Vol. 180. Springer, Berlin, 1971.

[Mas55] Katsuhiko Masuda. On a problem of Chevalley. *Nagoya Math. J.*, 8:59–63, 1955.

[Mas68] Katsuhiko Masuda. Application of the theory of the group of classes of projective modules to the existance problem of independent parameters of invariant. *J. Math. Soc. Japan*, 20:223–232, 1968.

[Mat64] Ryuuki Matsuda. On purely-transcendency of certain fields. *Tôhoku Math. J. (2)*, 16:189–202, 1964.

[Mil08] J.S. Milne. Class field theory, 2008.

[Miy71] Takehiko Miyata. Invariants of Certain Groups. *I. Nagaya Math.*, 41:69–73, 1971.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Ser58] Jean-Pierre Serre. Modules projectifs et espaces fibrés à fibre vectorielle. In *Séminaire Dubreil, Algèbre et théorie des nombres, tome 11 no.2 (1957/1958), Exp. No. 23*, pages 1–18. 1958.

[Ser68] Jean-Pierre Serre. *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Swa69] Richard G. Swan. Invariant rational functions and a problem of Steenrod. *Invent. Math.*, 7:148–158, 1969.