II- Représentations en différentes caractéristiques

Par : El-Asri Noureddine

À Aix-Marseille Université (AMU)

Sous la direction de : M. Heiermann Volker

Aristote rapporte qu'on demanda un jour à Anaxagore de Clazomène pour quelles raisons on devrait choisir de naître que de ne pas naître: "Pour connaître le ciel et l'ordre de ce qui nous entour", répondit le philosophe.
Quelqu'un d'autre lui demanda: "Ta patrie ne t'intéresse-t-elle pas?", le philosophe répondit, montrant le ciel: "Tu ne saurais mieux dire car justement je ne fais que m'occuper de ma patrie."

Aristote sur Anaxagore

Contents

Chapter 1

Rappels de quelques notions importantes

Nous allons introduire ici, de manière pragmatique, les notions dont nous aurons besoin pour comprendre la suite du cours. Ainsi, nous démontrons les résultats principaux, et laissons d'autres que nous jugeons triviaux.

1.1 Modules sur un anneau.

Nous commençons par introduire la notion très importante de module sur un anneau. Cette notion ne généralise pas uniquement la notion d'espace vectoriel sur un corps, mais nous donne une famille d'objets très variés et diverses, comme nous allons le voire dans cette petite section de rappels.

Définition (Modules): Soit A un anneau unitaire. Un ensemble M est dit un A-Module à gauche (ou module sur A) s'il est muni:
1/ D'une loi interne + telle que $(M,+)$ soit un groupe abélien.
2/ D'une loi externe $. : A \times M \to M$ vérifiant :
i/ $\forall a \in A, \forall (x,y) \in M^2,\ a.(x+y) = a.x + a.y.$
ii/ $\forall (a,b) \in A^2, \forall x \in M,\ (a+b).x = a.x + b.x.$
iii/ $\forall (a,b) \in A^2, \forall x \in M, a.(b.x) = (ab).x.$
iv/ $\forall x \in M, 1_A.x = x$ où 1_A l'unité de A.

Remarques :
1/ On définit de façon analogue la notion de module à droite.
2/ On voit que les espace vectoriels sur un corps K, sont aussi des modules sur K. On peut donc appliquer certaines propriétés des modules aux espaces vectoriels.

Exemples :
1/ Tout anneau A, est un module sur lui même.
2/ On peut facilement montrer que tout groupe abélien $(G,+)$ est, en effet, un $\mathbb{Z}$-module, en considérant l'action $\mathbb{Z} \times G \to G,\ (m,g) \mapsto m.g = g + .. + g$ m fois.

Propriétés : Soit A un anneau unitaire.
1/ Produit cartésien : Soient M, N deux A-Modules. Alors $M \times N$ muni de : $\begin{cases} (m,n) + (m',n') = (m+m', n+n') \\ a.(m,n) = (a.m, a.n) \end{cases}$ est un A-Module. On peut généraliser par récurrence à un produit de n espaces. Particulièrement $A^n,\ n \in \mathbb{N}$ est un A-Module.

2/ Matrices : $M_n(A)$ est un anneau, c'est donc un $M_n(A)$-Module, c'est aussi un

A-Module avec l'action :

$$A \times M_n(A) \to M_n(A)$$
$$a.(a_{i,j})_{i,j} = (a.a_{i,j})_{i,j}$$

3/ Polynômes : Si A est un anneau commutatif, alors $A[X]$ est un A-module.

4/ Ideal et Anneaux quotient : Si I est un ideal de A, alors I est un A-Module. l'anneau quotient A/I est aussi un A-Module en considérant l'action $a.\bar{b} = \bar{a.b}$.

5/ Définition (Algèbre) : Un A-Module M muni d'une loi externe $\times$ telle que $(M, +, \times)$ soit un anneau, est appelé un $A-$Algèbre (ou Algèbre sur A) lorsque $\forall a \in A, \forall (x, y) \in M^2,\ a.(xy) = (a.x)y = x(a.y)$.

Exemples : $M_n(A)$ et $A[X]$ munis de leurs lois usuelles sont des A-Algèbres. Par contre, A n'est pas forcément une algèbre sur lui-même, la dernière relation n'est valable que si A est commutatif.

6/ Soient A, B deux anneaux et $f : A \to B$ un morphisme d'anneaux. Alors on peut munir B d'un structure de A-Module en considérant l'action $(a, b) \mapsto f(a).b$. La plupart des constructions qu'on vient de voir découlent de cette propriété, par exemple celle de l'anneau quotient.
En effet, si A est intègre, on peut munir $K(A)$ le corps des fractions de A d'une structure de A-Module grâce à l'inclusion.

7/ Structure de $K[X]$-Module sur un K-Espace vectoriel : Soit E un K-espace vectoriel et f un endomorphisme de E. On peut munir E d'une structure de $K[X]$-Module de la manière suivante $\begin{cases} K[X] \times E \to E \\ (P, x) \mapsto P(f)(x) \end{cases}$ et on note cet espace E_f.

Morphisme : Soient M, N deux A-Modules et $f : M \to N$. f est dite morphisme de A-modules (Morphisme) lorsque $\begin{cases} 1/f \text{ est un morphisme de groupes de} \\ (M, +) \text{ dans } (N, +). \\ 2/\forall (a, m) \in A \times M, f(a.m) = a.f(m) \end{cases}$
de manière équivalente, $\forall (m, m') \in M^2, \forall a \in A, f(a.m + m') = a.f(m) + f(m')$.
On note $Hom_A(M, N)$ l'ensemble des morphismes de A-Modules de M dans N. si A est commutatif, alors c'est encore un $A - Module$.

Définition (Sous-Module) : Soient A un anneau, M un A-Module et $N \subset M$. N est dit un sous-A-module de M lorsque $\begin{cases} \forall (m,n) \in N^2,\ m+n \in N \\ \forall (a,n) \in A \times N, a.n \in N \end{cases}$ ou, de manière équivalente, $\forall (x,y) \in N^2,\ \forall (a,b) \in A^2,\ a.x + b.y \in N$. En particulier, cela insiste sur le fait qu'un sous-A-module de M est un sous groupe du groupe $(M,+)$.

Exemples :

1/ Soit A un anneau. Les sous-A-modules de A sont exactement les ses idéaux. En effet, I ideal de A $\Longleftrightarrow I$ sous groupe de $(A,+)$ et $\forall (a,i) \in A \times I,\ a.i \in I$ $\Longleftrightarrow \forall (a,b) \in A^2,\ \forall (m,n) \in I^2,\ a.m + b.n \in I$

2/ Un groupe abélien $(G,+)$ est un $\mathbb{Z}$-module et ses sous-$\mathbb{Z}$-modules sont ses sous groupes.

définition (Modules simples): Un A-Module M non nul est dit simple lorsque ses seuls sous-A-modules sont $\{0\}$ et lui-même.

Exemple :

1/ Soit V un espace vectoriel sur un corps K. Un sous-K-module de V n'est tout simplement qu'un sous-K-espace vectoriel de V. l'espace vectoriel V est simple si et seulement si il est de dimension 1.

2/ un groupe abélien G est un $\mathbb{Z}$-Module. Et est simple si et seulement si G est un groupe simple.

Proposition : Soient V un K-espace vectoriel et $T : V \to V$ un endomorphisme de V. Pour la structure $K[X]$-module sur V, noté, V_T, Un sous-$K[X]$-module n'est rien qu'un sous espace-K-vectoriel de V T-invariant.

Remarque : On aura besoin de cette notion pour comprendre le lien entre une représentation d'un groupe fini dans un K-espace vectoriel et sa correspondance comme $K[G]$-Module.

Preuve : Soit W un sous-K-espace vectoriel de V. W est un sous-$K[X]$-module si et seulement si W est stable par l'action introduite dans les exemples

précédents, c'est-à-dire, $\forall P \in K[X], P(T)(W) \subset W$, i.e, $\forall n \in \mathbb{N}, T^n(W) \subset W$ ce qui équivaut à dire que W est T-invariant.

Indépendance linéaire, Base, Module libre Soit B un sous ensemble d'un A-Module M.
1/ On dit que les éléments de B sont linéairement indépendants (A-libre) sur A lorsque $\forall (a_1, .., a_n) \subset A,\ \forall (b_1, .., b_n) \subset B,\ a_1b_1 + ... + a_nb_n = 0 \Longrightarrow a_1 = .. = a_n = 0$

2/ B est dit une base du A-module M lorsque B est linéairement indépendant sur A et B engendre M en tantvque $A-$Module.

3/ On dit que M est un A-Module libre s'il admet une base.
Par convention, le module $\{0\}$ est libre de base l'ensemble vide.
En quelque sorte, la notion de liberté est analogue de celle de dimension.

Exemples :
1/ Soient A un anneau et $n \in \mathbb{N}$. Le A-module A^n est libre, en effet la famille $\begin{bmatrix}1\\0\\.\\.\\0\end{bmatrix}, .., \begin{bmatrix}0\\0\\.\\.\\1\end{bmatrix}$ en est une base (Claire).

Lemme: Toute base d'un A-module M est un ensemble engendrant minimal.

Preuve : Soit B une base de M et B' un sous-espace strict de B. soit $b \in B$. Si on peut écrire b comme combinaison A-linéaire d'éléments de B', alors comme $B' \subset B$, alors B n'est pas libre. Donc $B = B'$

Lemme: Toute base d'un A-Module libre de type fini est finie.

Preuve : Soit B une base du A-module de type fini $M = A.m_1 + .. + A.m_n$ où $\{m_1, .., m_n\} \subset M$. Comme chaque m_i est combinaison A-linéaire finie d'éléments de B, et que $n < +\infty$, alors il existe un sous ensemble fini S de B tel que $\{m_1, .., m_n\} \subset < S >$, ainsi S engendre M. Par le lemme précédent, comme $S \subset B$, on a que $B = S$.

Remarques: En Algèbre linéaire, on a appris que chaque espace vectoriel a une base et que toutes les bases ont la même cardinalité. On défini ensuite la notion de dimension comme étant le cardinal d'une base quelconque de l'espace. Cela n'est en général pas vrai lorsqu'on parle de modules. D'abord, il existe des modules qui n'ont pas de bases (ne sont pas libres). Deuxièmement, même si un A-module est libre, il peut avoir des bases de cardinalités différentes!

Exemples :

1/ Soit K un corps de nombres sur $\mathbb{Q}$, de degré n. Alors l'ensemble des entiers de K O_K sur $\mathbb{Z}$ est un $\mathbb{Z}$-module libre de type fini de rang n, i.e, $O_K = \mathbb{Z}.x_1 + .. + \mathbb{Z}.x_n$ où $\{x_1, .., x_n\} \subset O_K$. Un exemple est $K = \mathbb{Q}[j] = \mathbb{Q}[\sqrt{-3}]$ et on trouve que $(1, j)$ est une $\mathbb{Z}$-base de O_K.

2/ $\mathbb{Q}$ n'a pas de bases en tant que $\mathbb{Z} - module$.

Somme direct : soient $M_1, .., M_k$ des sous modules d'un A-module M. On dit que leur somme est direct lorsque $\forall (u_1, .., u_k) \in M_1 \times .. \times M_k$, on a $u_1 + .. + u_k = 0 \Longrightarrow u_1 = .. = u_k = 0$. Et on écrit la somme $M_1 + .. + M_k$ comme $M_1 \oplus .. \oplus M_k$. M est dite une somme direct de $M_1, .., M_k$ lorsque $M = M_1 \oplus .. \oplus M_k$.

Proposition : soient $M_1, .., M_k$ des sous modules d'un A-module M. Alors, $M = M_1 \oplus .. \oplus M_k \Longleftrightarrow \forall u \in M,\ \exists!(u_1, .., u_k) \in M_1 \times .. \times M_k,\ u = u_1 + .. + u_k$

Preuve : Assez évidente.

Définition (Module semi-simple): Soit M un A-Module. M est dit semi simple si tout sous-A-module de M admet un sous$-A-$module supplémentaire, ou, de manière équivalente, lorsqu'il est somme (possiblement infinie) directe de sous-modules simples.

Lemme : Soit M un A-module semi simple. Alors les sous-A-module de M et ses modules quotients sont semi simples.

Preuve :

o Soit S un sous-A-module de M, soit P un sous-A-module de S. Comme P est un sous-A-module de M, il admet donc un supplémentaire dans M car ce dernier

est semi simple. L'intersection de ce supplémentaire et S est un supplémentaire de P dans S. Ainsi S est semi simple.
o Soit M/N un quotient de M. Il est isomorphe à un supplémentaire S de N dans M, ce qui termine la preuve.

Lemme : Tout module semi simple non nul possède un sous-module simple.

Preuve (Partielle !) : Soit M un A-module semi simple non nul et T un sous-A-module propre maximal de M(lemme de Zorn). Soit P un supplémentaire de T dans M. T est simple, car sinon le complémentaire de son sous module propre contiendrait T, or T est maximal.

1.2 Algèbres sur un anneau

Dans cette section nous allons développer la notion d'algèbre sur un anneau, avec cela nous perrons attaquer le chapitre sur l'algèbre su groupe. En tant que rappels, on ne va pas beaucoup développer cette notion, mais nous donnons les résultats nécessaires pour comprendre la suite.

Remarques :

1/ Cela donne un quadruplé $(E, +, ., \times)$ tel que $(E, +, .)$ est un A-Module et $(E, +, \times)$ est un anneau tels que . et $\times$ vérifient la condition de stabilité ci-dessus.

2/ On confond très souvent les notations des deux lois . et $\times$. La différence se fait au niveau des éléments et leur appartenance.

3/ On peut considérer des structures algébriques définies, sur un ensemble E, muni de deux lois internes et d'une loi externe induite par une action d'un anneau. On a bien une structure d'algèbre sur cet anneau, et on appelle ce structure 'algèbre non associative'.

4/ On peut généraliser la définition en supposant que A est non associatif. Mais cela n'est pas intéressant pour la suite.

5/ Il arrive souvent de munir l'algèbre E d'une structure de module en prenant l'action d'un sous anneau quelconque de l'anneau $(E, +, \times)$. On parle bien d'une sorte de double module.., et donc E est une algèbre sur ce sous anneau.

6/ En considérant, sur un anneau quelconque $(E, +, .)$, l'action $\mathbb{Z} \times E$ telle que $(n, x) \mapsto n.x = x + .. + x)$, alors on obtient sur E une structure de $\mathbb{Z}$-Algèbre.

7/ Si B est un sous-anneau de A ayant la même unité , alors si on restreint la loi externe d'une algèbre E sur B, alors on obtiendra encore une structure de B-algèbre, qu'on distingue de celle de A-algèbre.

Exemples :

1/ Tout anneau A d'unité 1 peut être muni d'une structure d'algèbre sur son centre. En effet, le centre $Z(A) = \{a \in A,\ \forall x \in A,\ a.x = xa\}$ est un sous-anneau de A, commutatif et A est naturellement un $Z(A)$-Module. L'action $. : Z(A) \times A \to A$ vérifie, par construction de $Z(A)$ la condition de stabilité.

2/ Un autre exemple, qui est classique est celui de la K-Algèbre des matrices $M_n(K)$ où K est un corps. $(M_n(K), +, .)$ où "." est la multiplication par un scalaire, est

un K-espace vectoriel et muni de la multiplication

$$M_n(K) \times M_n(K) \to M_n(K),\ (A, B) \mapsto AB$$

. L'algèbre des matrices admet une base finie en tant que K-espace vectoriel.

3/ Dans l'exemple précédent, on peut remplacer le corps K par l'anneau $\mathbb{Z}$ et obtenir une algèbre des matrices sur $\mathbb{Z}$, d'une base fini.

Bases d'algèbres Les algèbres les plus intéressantes sont celles qui ont une base en tant que A-modules. C'est même toujours dans le cas d'algèbres sur un corps, et sont celles qu'on rencontre le plus souvent.

Soit E une A-algèbre ayant une base sur l'anneau A

Définition (Algèbres simples) :
Une A-algèbre $(M, +, \times, .)$ est dit simple lorsque l'anneau $(M, +, \times)$ n'a que deux idéaux bilatères, $\{0\}$ et lui-même.

Exemples :
1/ L'anneau $\mathbb{Z}$ muni d'une structure d'algèbre sur lui-même n'est pas simple. En effet $\mathbb{Z}$ possède une infinité d'idéaux bilatères.

2/ L'ensemble des A-endomorphismes $\mathcal{L}_A(M)$ d'un A-module M muni de la composition est une A-algèbre simple, mais admet toujours des sous-A-algèbres, par exemple si p est un projecteur, l'ensemble $\{p \circ f \mid f \in \mathcal{L}_A(M)\}$ est un sous-A-algèbre de $\mathcal{L}_A(M)$! Donc définir la simplicité d'une algèbre comme on a fait avec les modules (au sens des sous-algèbres) n'est pas suffisante. D'où notre définition.

3/ Un corps non nécessairement commutatif est considéré comme une algèbre simple sur lui-même.

Définition : Les idéaux d'une A-algèbre M sont appelés facteurs invariants de M.

Exemples :
1/ $\mathbb{C}$ est une $\mathbb{R}$-algèbre simple, car $\mathbb{C}$ est un corps, i.e, ses seuls idéaux propres sont $\{0\}$. Mais n'est simple en tant que sous-$\mathbb{R}$-module, car $\mathbb{R}$ en est un sous-module simple.

Définition : Soit F un facteur invariant d'une algèbre M. F est dit un facteur direct lorsque son supplémentaire est encore un facteur invariant.

Définition : Une A-algèbre M est dite semi-simple lorsque tout M-module est semi-simple.

1.3 Anneaux des entiers

Dans la suite, A est un anneau intègre commutatif et unitaire.

Éléments entiers : $B \subset A$ deux anneaux. $b \in B$ est dit entier sur A si $\exists P \in A[X]$ unitaire tel que $P(b) = 0$.

Définition : l'ensemble des éléments de B entiers sur A est appelé fermeture intégrale de A dans B, et noté $E(B/A)$.

Exemples :
1/ $i \in \mathbb{C}$ est entier sur $\mathbb{Z}$, par le polynôme $P = X^2 + 1$.

2/ $\frac{i}{2}$ n'est pas entier sur $\mathbb{Z}$.

3/ $E(\mathbb{Q}/\mathbb{Z}) = \mathbb{Z}$: En effet, $\frac{p}{q} \in E(\mathbb{Q}/\mathbb{Z})$ et $pgcd(p,q) = 1, q \neq 0$ équivaut à $\exists n \in \mathbb{N}, (a_0, .., a_{n-1}) \in \mathbb{Z}$ tels que $\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + .. + a_1\frac{p}{q} + a_0 = 0$, donc, q divise p^n. Or $pgcd(p,q) = 1$, alors $pgcd(p^n, q) = 1$ et donc $q = 1$ et donc $\frac{p}{q} = p \in \mathbb{Z}$.
On peut faire la même chose et montrer que tout anneau à PGCD possède la propriété d'être intégralement clos :

Définition (Intégralement clos): Si on note $K(A)$ le corps des fractions de l'anneau A, alors A est dit intégralement clos lorsque $A = E(K(A)/A)$.

Proposition : $A \subset B$ des anneaux. On a l'équivalence entre :
1/ $b \in B$ est entier sur A,
2/ $A[b]$ est un A-module de type fini,
3/ $\exists M$ sous-anneau de B contenant $A[b]$ qui soit un A-module de type fini.

Preuve :
- 1$\Longrightarrow$2 : Soit $b \in B$ entier sur A de polynôme annulateur sur A $P = (1, a_{n-1}, .., a_0)$. On a donc $b^n \in A + A.b + .. + A.b^{n-1} = M$. Ainsi, $M \subset A[b]$.L'autre inclusion étant triviale, on a donc $A[b] = M$.
- 2$\Longrightarrow$3 : Comme $A[b]$ est de type fini, alors lui même fait l'affaire.
- 3$\Longrightarrow$1 : $M = A + A.x_1 + .. + A.x_n$ l'anneau de type fini contenant $A[b]$. On a que $b.M \subset M$, i.e, $b.x_i = \sum_{j=1}^{n} a_{i,j}.x_j$, on aura $0 = (a_{i,i} - b).x_i + \sum_{j \neq i} a_{i,j}.x_j$, i.e, $(T - b.I_n).\begin{vmatrix} x_1 \\ . \\ . \\ x_n \end{vmatrix} = 0$ avec $T = (a_{i,j})$. Le développement de Laplace $\Longrightarrow$ que $det(T - b.I_n)$ annule b, et c'est bien un polynôme sur A unitaire.
Ce qui termine la preuve.

Proposition : $(b_1, .., b_n) \subset B$ sont entiers sur A si et seulement si $A[b_1, .., b_n]$ un A-module de type fini.

Preuve : Un sens est immédiat.
L'autre sens par récurrence sur n en remarquant que $A[a, b] = (A[a])[b]$.

Définition : Soient $A \subset B$ deux anneaux. B est dit entier sur A lorsque tout element de B est entier sur A, autrement dit, $B = E(B/A)$

Proposition : $A \subset B \subset C$ des anneaux. C est entier sur A si et seulement si C est entier sur B et B sur A.

Preuve : Claire.

Ce qu'on a introduit suffit largement pour comprendre la suite.

Chapter 2

L'algèbre du groupe.

Introduire la notion d'algèbre sur un groupe nous donne un nouveau angle pour étudier et comprendre les représentations des groupes, comme nous allons le voir plus loin, la notion d'algèbre du groupe est très liée à aux représentations de ce groupe. cette approche nous permettra d'établir de très fort théorèmes.
Dans la suite, les groupes considérés sont finis et tous les espaces vectoriels seront de dimension finies sur le corps $C = \mathbb{C}$ des nombres complexes

2.1 Représentations et modules

Soient G un groupe fini d'ordre $|G|$ et A un anneau commutatif.
On remarque quelque chose de très intéressant, c'est que toute application $f : G \to A$ est totalement déterminée par l'image de chaque élément de G par f car G est fini. Ainsi, $f = \sum_{g\in G} f(g)\delta_g$ où $\delta_g(s) = \begin{cases} 1 \ si \ g = s \\ 0 \ sinon \end{cases}$. $(\delta_g)_{g\in G}$ est donc une base sur le groupe additif $(A^G, +)$, d'où la définition :

Définition: On peut définir A^G comme $\{\sum_{g\in G} f_g.\delta_g \mid (f_g) \subset A\}$, et $(A^G, +, .)$ est un anneau, où, si $f = \sum_{g\in G} f_g\delta_g$ et $h = \sum_{g\in G} h_g\delta_g$ deux éléments de A^G, on a

$$\begin{cases} f + g = \sum_{g\in G}(f_g + h_g).\delta_g \\ f.h = \sum_{(g,g')\in G^2} f_g.h_g.\delta_{g.g'}. \end{cases}$$

Cet anneau peut être muni d'une structure de A-module par l'action $a.\sum_{g\in G} f_g.\delta_g = \sum_{g\in G} a.f_g.\delta_g$. On se retrouve alors avec une structure de A-algèbre sur A^G, cet algèbre est appelé **L'algèbre de G sur A.**

Remarque : Généralement, une algèbre d'un groupe fini est la donnée d'un groupe fini, d'un module libre de type fini de base indexée par le groupe.

Dans la suite, on identifie δ_g et g et on a $\delta_g.\delta_s = g.s$
où $g.s$ est la loi interne de G. Aussi on se limite à $A = C = \mathbb{C}$ le corps des complexes.
On a ainsi que $C[G] = \bigoplus_{g\in G} C.g$(La représentation régulière en quelque sorte), et on a les propriétés suivantes :

proposition :
1/ $1_{C[G]} = 1_G$
2/ $dim_C(C[G]) = |G|$
3/ La C-algèbre $C[G]$ est commutative (loi de l'anneau) si et seulement si G est abélien.
4/ Tout $C[G]$-module est en particulier un C-espace vectoriel.

Preuve :
Le 1 et le 2 sont assez évidentes.
3/ Vient de la formule $f.h = (\sum_{g\in G} f_g.g)(\sum_{s\in G} h_s.s) = \sum_{(g,s)\in G^2} f_g.h_s.g.s$ Or G est abélien, on a donc $f.h = \sum_{(g,s)\in G^2} h_g.f_s.g.s$ ce qui termine la preuve.
4/ Assez simple vu que $C \subset C[G]$, cette inclusion est à prendre au sens où $\forall z \in C,\ z = z.1_G$

Remarque : Dans toute la suite, tout $C[G]$-module sera considéré comme un $C[G]$-module à gauche. la transition au cas à droite se fera facilement car $C[G] \to C[G],\ g \mapsto g^{-1}$ est un automorphisme.

Exemples :
1/ si $G = \mathbb{Z}/2\mathbb{Z}$, alors $\mathbb{R}[G] = \mathbb{R}.\bar{0} + \mathbb{R}.\bar{1}$,
2/ Si $f = \sum_{i=1}^n f_i g_i$ et $h = \sum_{i=1}^n h_i g_i$ (f_i valeur de f en g_i) alors $f.h = \sum_{i=1}^n \sum_{j=1}^n f_i h_j g_i.g_j$,
3/ $C[\mathbb{Z}/n\mathbb{Z}] \simeq C[X]/ < X^n >$ Suffit de voir que

$$C[X]/ < X^n >= \{\sum_{k=0}^{n-1} a_k.\bar{X^k} \mid (a_0, .., a_{n-1}) \subset C\}$$

et $\bar{X^n} = \bar{0}$. L'isomorphisme est naturellement celle qui laisse stable C et qui $\bar{k} \in \mathbb{Z}/n\mathbb{Z} \mapsto \bar{X^k}$.

Proposition:
La donnée d'une C-représentation est équivalente à la donnée d'un $C[G]$-module.

Remarque : On a même une correspondance entre les deux notions, qu'on va préciser dans ce paragraphe.

Preuve :
1/ Si (p, V) est une C-représentation de G alors l'action

$$C[G] \times V \to V$$

$$(\sum_{g\in G} f_g.g, x) \mapsto \sum_{g\in G} f_g.p_g(x)$$

fait bien de V un $C[G]$-module.
2/ Si V est un $C[G]$-module par l'action $*$, alors

$$p : G \to GL(V)$$

$$g \mapsto p_g : x \mapsto p_g(x) = g * x$$

est bien une C représentation de G.

Exemples :
1/ Le corps C peut lui-même être vu comme $C[G]$-module par l'action $G \times C \to C$, $(g, z) \mapsto g.z = z$ qu'on peut étendre par linéarité sur tout $C[G]$. Et, ça correspond à la C-représentation trivial de G dans C :

$$p : G \to C^*$$

$$g \mapsto p_g : z \mapsto z$$

Correspondance entre les C-représentations et les $C[G]$-modules :
1/ C-représentation de $G \leftrightarrow C[G]$-module,
2/ Degré de la représentation $V \leftrightarrow$ dimension du C-espace vectoriel V,
3/ morphisme de représentations $\leftrightarrow$ morphisme de $C[G]$-modules,
4/ Sous-représentation $\leftrightarrow$ sous-$C[G]$-module,
5/ $(p^1 \oplus p^2, V_1 \oplus V_2) \leftrightarrow V_1 \oplus V_2$ en tant que $C[G]$-modules,
6/ Représentation irréductible $\leftrightarrow$ $C[G]$-module simple,
7/Représentation semi-simple $\leftrightarrow$ $C[G]$-module semi-simple,

Proposition: L'algèbre $C[G]$ est semi simple (vraie pour un corps K de caractéristique $= 0$).

Preuve : Dire que $C[G]$ est une Algèbre semi-simple revient à dire que tout $C[G]$-module V est semi-simple,i.e,tout sous-$C[G]$-module de V admet un supplémentaire.
Soient M un $C[G]$-module et N un sous-$C[G]$-module de M. En particulier, M est un espace vectoriel sur C et N est un sous-C-espace vectoriel de M, et donc

admet un supplémentaire en N' en tant qu'espace vectoriel, i.e, $M = N \oplus_C N'$ et il existe donc un projecteur $p : M \to N$ C-linéaire. Soit $a : G \to GL(M),\ g \mapsto a_g : m \mapsto g.m$ et considérons $p^o = \frac{1}{|G|} \sum_{g \in G} a_g \circ p \circ a_{g^{-1}}$. p^o est $C[G]$-linéaire. En plus, son image est le $C[G]$-espace-vectoriel N et de noyau un sous-$C[G]$-module de M noté N^o. Cela conclut la preuve.

Remarque : Vue les propriété précédentes, on peut transporter les propriétés des C-représentations sur les $C[G]$-Modules et inversement. et donc avoir des propriété sur le C-algèbre $C[G]$.
Généralement, on a que :

Proposition :(Théorème de Maschke) Soit K un corps de caractéristique $p > 0$. Supposons que p ne divise pas $|G|$. Alors pour toute représentation V de G, et toute sous-représentation W de V, W admet un supplémentaire G-stable.

langage Modulaire: Soit K un corps de caractéristique p premier ne divisant pas $|G|$. Alors tout $K[G]$-module est semi-simple, i.e, l'algèbre $K[G]$ est semi-simple.

Preuve : On s'inspire de ce qu'on a fait avant, on choisit n'importe quel projecteur p sur W, et par le procédure de normalisation (Possible parce que p ne divise pas $|G|$, et donc on peut écrire $\frac{1}{|G|}$ dans la formule de normalisation)..

Corollaire : Dès que $Car(K)$ ne divise pas $|G|$, on a que $K[G]$ est semi-simple.

Remarques : Le théorème est faux si p divise $|G|$:
Par exemple la représentation (Forme matricielle) $q : Z/pZ \to GL_2(F_p)$ où $\forall \bar{n} \in Z/pZ$, $q_{\bar{n}} = \begin{bmatrix} 1 & \bar{n} \\ 0 & 1 \end{bmatrix}$ n'est pas irreductible car $Vect(\begin{bmatrix} 1 \\ 0 \end{bmatrix})$ est stable par q. Mais cette représentation n'admet aucune autre sous-représentation! donc impossible de la décomposer en somme d'irreductibles. (En effet, en dimension 1, un vecteur (x, y) est q-stable ssi $y = 0$).

Corollaire : L'algèbre $C[G]$ est un produit d'algèbres de matrices sur des corps (gauches) de degré fini sur C.

Preuve : Détaillons dans le paragraph suivant :

2.2 Décomposition de $C[G]$

Soient $(p^i : G \to GL(W_i))_{i=1:h}$ les différentes sous représentations irréductibles de G (à isomorphisme près), $n_i = dim(W_i)$ de sorte que les anneaux $End(W_i) \simeq GL_{n_i}(C)$.
Les C-représentations $p^i : G \to GL(W_i)$ se prolongent par linéarité en un morphisme d'algèbres $P^i : C[G] \to End(W_i) \simeq M_{n_i}(C)$ et la famille $(P^i)_{i=1:h}$ définie un morphisme de C-algèbres :

$$P : C[G] \to \prod_{i=1}^{h} End(W_i)$$

$$f \mapsto P_f = (P^i(f) = \sum_{g \in G} f_g p_g^i)_{i=1:h}$$

$C[G] \simeq M_{n_1}(C) \times .. \times M_{n_h}(C)$

Proposition : P est un isomorphisme.

Preuve : Comme

$$dim(\prod_{i=1}^{h} End(W_i)) = \sum_{i=1}^{h} dim(End(W_i))$$

$$= \sum_{i=1}^{h} dim(W_i)^2 = |G| = dim(C[G])$$

Alors il suffit de montrer que p' est surjective.
On a a la surjectivité qui vienne d'après la proposition suivante :

Proposition (Formule d'inversion de Fourier): $(u_1, .., u_k) \in End(W_1) \times .. \times End(W_k)$ et $f = \sum_{g\in G} f_g.g \in C[G]$ tel que $P^i(f) = \sum_{g\in G} f_g p^i_g = u_i$. On a que $f_g = \frac{1}{|G|} \sum_{i=1}^{k} n_i Tr_{W_i}(p^i_{g^{-1}} \circ u_i)$.

Preuve : Il suffit de démontrer ça pour $f = 1_{C[G]}.g = g \in G$,i.e, $f_g = 1_{C[G]}$, i.e, $P^i(f) = \sum_g f_g.p^i_g = p^i_g = u_i$ On a que $\frac{1}{|G|} \sum_{g\in G} n_i.Tr_{W_i}(p^i_{g^{-1}} \circ u_i$ Or $p^i_{g^{-1}} = (p^i_g)^{-1} = u_i^{-1}$. Et donc on a $\frac{1}{|G|} \sum_{g\in G} n_i.Tr_{W_i}(I_{n_i}) = \frac{1}{|G|} \sum_{g\in G} n_i^2 = \frac{1}{|G|}.|G| = 1 = f_g$. Et par linéarité.. Ce qui termine la preuve.

le centre de $C[G]$:

Définition : Le centre de $C[G]$ est l'ensemble $\{f \in C[G],\ \forall h \in C[G],\ f.g = g.f\}$.

Proposition : Soient $\bar{g}$ une classe de conjugaison de G et notons $e_{\bar{g}} = \sum_{s\in\bar{g}} s$. Alors l'ensemble $\{e_{\bar{g}}\}$ forment une base du centre de $C[G]$.

Preuve : On a clairement que $\{\sum_{g\in G} g.u.g^{-1} \mid u \in G\}$ est inclus dans le centre de $C[G]$: en effet, $f. \sum_{s\in G} s.u.s^{-1} = (\sum_{g\in G} f_g.g). \sum_{s\in G} s.u.s^{-1}$
$= \sum_{g\in G} \sum_{s\in G} f_g.g.s.u.s^{-1}$
$= \sum_{g\in G} f_g \sum_{s\in G} s.u.s^{-1}.g$
$= \sum_{s\in G} s.u.s^{-1}. \sum_{g\in G} f_g.g = (\sum_{s\in G} s.u.s^{-1}).f.$
C'est bien une base : $f = \sum_{g\in G} f_g.g$ est dans le centre de $C[G]$ ssi $\forall s \in G,\ f.s = s.f$ ssi $f = \sum_{g\in G} f_g.s.g.s^{-1}$ et comme $s.g.s^{-1} \in \bar{g}$ et en additionnant on a que $|G|.f = \sum_{g\in G} f_g.e_{\bar{g}}$. Ce qui termine la preuve.

Corollaire : Le C-espace-vectoriel, qui est le centre de $C[G]$ est de dimension h, le nombre de classes de conjugaison de G.

Preuve : Immédiate.

Proposition : Soit $p^i : G \to GL(W_i)$ une représentation irréductible de G de caractère X_i et de relevé (morphisme de C-algèbres) $P^i : C[G] \to End(W_i)$.

P^i envoie le centre de $C[G]$ dans l'ensemble des homothéties de W_i, et définit un morphisme de C-algèbre

$$\omega_i : Z(C[G]) \to C$$
$$f = \sum_g f_g.g \mapsto \frac{1}{n_i} Tr_{W_i}(P^i(f)) = \frac{1}{n_i} \sum_{g \in G} f_g.X_i(g)$$

Preuve: Il suffit de montrer ça pour un élément de la base de $Z(C[G])$. Soit $g \in G$, on a que $e_g = \sum_{s \in G} s.g.s^{-1}$ est un élément de la base, et, $P^i(e_g) = \sum_{s \in G} p^i_{s.g.s-1}$. Or comme $\forall h \in G$, $\sum_{s \in G} p^i_{s.g.s-1} \circ p^i_h = \sum_{s \in G} p^i_{s.g.s-1.h} =_{s^{-1}.q} \sum_{q \in G} p^i_{h.q^{-1}.g.q} = p^i_h \circ \sum_{s \in G} p^i_{s.g.s-1}$. Alors d'après le lemme de Schur, $P^i(e_g)$ est une homothétie de W_i. C'est le résultat voulue. Pour la formule de w_i, cela résulte du corollaire du lemme de Schur.

Proposition : $(\omega_i)_{i=1:h}$ définie un isomorphisme entre $Z(C[G])$ et C^h, i.e, $Z(C[G]) \simeq C^h$ où h le nombre de classes de conjugaisons de G.

Preuve : Par l'isomorphisme précédente, le centre de $C[G]$ est isomorphe au centre de $GL_{n_1}(C) \times .. \times GL_{n_h}(C)$. Or, le centre de chaque $GL_{n_i}(C)$ est exactement l'ensemble des homothéties de W_i (Voir la preuve sur bibmath). Cela conclut la preuve.

Définition (Entier algébrique):
Tout $x \in \mathbb{C}$ entier sur $\mathbb{Z}$ est dit entier algébrique.

Proposition : Soit X le caractère d'une C-représentation (p, V) d'un groupe fini G. On a que $\forall g \in G,\ X(g)$ est un entier algébrique.

Preuve : Comme $X(g) = Tr(p_g) = \sum_{\lambda\ v.propre} \lambda$. Or comme p est un morphisme de groupes et que $\forall g \in G,\ g^{|G|} = e$, alors $p_g^{|G|} = Id$ et on passant à l'écriture matricielle de p_g, on a que chaque valeur propre de p_g est racine de l'unité, i.e, c'est un entier, et donc par somme, $X(g)$ est entier.

Proposition : $f = \sum_{g \in G} f_g.g$ un élément du centre de $C[G]$ tel que chaque f_g est un entier algébrique. Alors f est entier sur $\mathbb{Z}$ (En prenant l'anneau commutatif $Z(C[G])$)

Preuve : Soit $f = \sum_{i=1}^{h} f_g.e_g \in Z(C[G])$. Il suffit de montrer que chaque e_g est entier vu que cette propriété est stable par somme et produit. Pour cela montrons qu'il existe un sois-$\mathbb{Z}$-module de $Z(C[G])$ de type fini contenant chacun : On a que $\mathbb{Z}[e_{g_1}, .., e_{g_h}] \subset A = \mathbb{Z}.e_{g_1} + ..\mathbb{Z}.e_{g_h}$ comme A est un sous-anneau de $Z(C[G])$ car $e_{g_i}.e_{g_k}$ est combinaison $\mathbb{Z}$-linéaire des e_{g_i}, c'est donc un sous-$\mathbb{Z}$-module du centre. Ce qui conclut la preuve.

Corollaire: p une représentation irréductible de degré n, de caractère X d'un groupe fini G et $f = (f_g) \in Z(C[G])$ entier. Alors $\frac{1}{n}\sum_{g\in G} f_g.X(g)$ est un entier algébrique.

Preuve: C'est l'image de f par le morphisme $\omega : Z(C[G]) \to C$ associé à p, qui est entier : il suffit de prendre l'image de son polynôme annulateur à coefficients dans $\mathbb{Z}$.

Corollaire : Les degrés des représentations irréductibles de G divisent son ordre. On va utiliser le fait que $E(\mathbb{Q}/\mathbb{Z}) = O_{\mathbb{Q}} = \mathbb{Z}$:

Preuve : avec les mêmes notations que le corollaire précédent, L'élément $f = \sum_{g\in G} X(g^{-1}).g$ est un entier algébrique car chaque $X(g^{-1})$ l'est. Ainsi, d'après le corollaire précédent, $\omega(f) = \frac{1}{n}\sum_{g\in G} X(g^{-1}).X(g) = \frac{1}{n}|G| = \frac{|G|}{n}$ (car $1 =< X, X >= \frac{1}{|G|}\sum_{g\in G} |X(g)|^2$) est un entier. Or ce dernier est rationnel, et que les entier de $O_{\mathbb{Q}} = \mathbb{Z}$. alors $\frac{|G|}{n} \in \mathbb{Z}$. Voilà .

Proposition : Les degrés des représentations irréductibles de G divisent $|G/Z(G)|$

Preuve (Donnée par M.John Tate) : Reprenons les notations des deux corollaires. On a que pour $g \in Z(G)$ p_g commute avec tous les p_s car $p_g \circ p_s = p_{s.g}$, et donc d'après le lemme de Schur, elle est une homothétie de rapport $\lambda(g)$. Notons $\lambda : Z(G) \to C^*,\ g \mapsto \lambda(g)$, c'est un morphisme de groupes : $\forall g, g' \in Z(G), p_{g.g'} = p_g \circ p_{g'}$, i.e, $\lambda(g.g') = \lambda(g).\lambda(g')$.
Considérons maintenant le produit tensoriel de p suivant $p^m : G^m \to GL(W \otimes .. \otimes W)$. D'après la partie 1, p^m est encore une représentation irréductible du groupe G^m et si $(g_1, .., g_m) \in Z(G)^m$ alors $p^m(g_1, .., g_m) = p_{g_1} \otimes .. \otimes p_{g_m} = \lambda(g_1).Id_W \otimes$

$.. \otimes \lambda(g_m).Id_W$ est l'homothétie de rapport $\lambda(g_1)..\lambda(g_m) = \lambda(g_1..g_m)$. Le noyau de λ contient l'ensemble $\{(g_1, .., g_m)|g_1..g_m = e\}$.

Corollaire : Si G est un groupe abelien, alors ses representations irreductibles sont de degré 1.

Preuve : On a que $Z(G) = G$ donc d'après la proposition précédente, les degrés divisent $1 = |G/G| = |G/Z(G)|$.

Chapter 3

Représentations induites, Critère de Makey et Relation de Nakayama

On va d'abord reprendre certaines notions de la première partie :

Représentations induites :

$p : G \to GV(V)$ une représentation linéaire du groupe fini G.
Soit H un sous-groupe de G et soit $\bar{p}$ la restriction de p sur H.
Si W est H-stable, i.e, sous représentation de $\bar{p}$, alors on que $\forall \bar{g} \in G/H, p_{\bar{g}}(W) = p_g(W)$, càd, ne dépend pas du choix d'un représentant de $\bar{g}$. Et nous notons donc $W_g = p_{\bar{g}}(W)$ le sous-espace vectoriel de V. Considérons $\sum_{\bar{g}\in G/H} W_g$. Il est un sous-espace vectoriel de V G-stable. Ça donne quoi si cette somme est direct et égale à V?

Définition : Soit $p : G \to GL(V)$ une représentation de G. Elle est dite induite par la représentation $\theta : H \to GL(W)$ lorsque
1/ H est un sous groupe de G,
2/ W est un sous-espace vectoriel de V,
3/ $V = \bigoplus_{\bar{g}\in G/H} p_{\bar{g}}(W) = \bigoplus_{\bar{g}\in G/H} W_g$,

Propriétés :
1/ $dim_C(V) = |G/H|.dim_C(W)$. (La preuve est facile),
2/ Si $(p,V)_G$ est la représentation régulière de G et $W = Vect_C(e_h|h \in H)$, alors $\theta : H \to GL(W)$ est la représentation régulière de H et (p,V) est induite par (θ, V).
Preuve : $\bigotimes_{\bar{g}\in G/H} p_g(W) = \bigotimes_{\bar{g}\in G/H} Vect_C(e_{g.h}|h \in H) = V$ car $\sum_{\bar{g}/H} Vect_C(e_{g.h}|h \in H) = \sum \bar{g} \in G/H \sum_{h\in H} Vect_C(e_{g.h}) =_{s=g.h} \sum_{\bar{g}\in G/H} \sum_{s\in\bar{g}} Vect_C(e_s) = \sum_{g\in G} Vect_C(e_g)$ car les classes modulo H forment une partition de G.
3/ Si p_1 (resp. p_2) est induite par θ_1 (resp. θ_2), alors $p_1 \oplus p_2$ est induite par $\theta_1 \oplus \theta_2$.
4/ Si p est induite par θ, p' une représentation de G, de restriction p'_H sur H, alors $p \otimes p'$ est induite par $\theta \otimes p'_H$.

Lemme : Soit (p,V) une représentation de G induite par (θ, W). Soit (G, V') une autre représentation de G et $f : W \to V'$ linéaire telle que $\forall h \in H,\ p'_h \circ f = f \circ \theta_h$. Il existe alors une unique application linéaire $F : V \to V'$ prolongeant f vérifiant $\forall g \in G, p'_g \circ F = F \circ p_g$.

Preuve : D'abord on a que $V = \bigoplus_{\bar{g}\in G/H} W_g$,
Si $x \in W_g$, alors $p_{barg^{-1}}(x) \in W$ et donc si F vérifie $p'_g \circ F = F \circ p_g^{-1}$, alors on a $F = p'_g \circ F \circ p_g^{-1}$ et donc $F(x) = p'_g \circ F \circ p_g^{-1}(x) = F = p'_g \circ f \circ p_g^{-1}$ car $F_W = f$. Cela détermine F sur chaque W_g, et donc sur V, et on a donc l'unicité.
Pour l'existence, on a une candidate : $F(x) = p'_g \circ F \circ p_g^{-1}(x)$ où $g \in \bar{g}$ et $x \in W_g$. En effet cette définition ne dépend pas du choix du représentant $g \in \bar{g}$, regardons, $p'_{g.h} \circ f \circ p_{g.h}^{-1}(x) = p'_g \circ g'_h \circ f \circ p_h^{-1} \circ p_g^{-1}(x) = p'_g \circ g'_h \circ f \circ \theta_h^{-1} \circ p_g^{-1}(x) = p'_g \circ f \circ p_g^{-1}(x)$. Ainsi, en faisant la même chose sur chaque W_g, on obtient une unique application F, sur V, vérifiant ce qu'on veut.

Théorème (Existence et unicité des représentations induites): Soit (θ, W) une représentation linéaire d'un sous groupe distingué H du groupe fini G. Alors il existe une, et une seule, à isomorphisme près, représentation linéaire de G, (p,V) induite par (θ, W).

Preuve :
1/ Existence : Vu les propriétés, supposons que θ est irréductible. θ est donc isomorphe à une sous représentation de la représentation régulière de H, cette sous-représentation induit la représentation régulière de G. Ainsi, par les propriétés, θ induit une représentation de G.

2/ L'unicité : soient (p, V) et (p', V') deux représentations induites par θ. D'après le lemme précédent, $\exists! F : V \to V'$ prolongeant l'inclusion de W dans V', vérifiant $F \circ p_g = p'_g \circ F \ \forall g \in G$. En effet, F est un isomorphisme, d'abord $\forall g \in G, p'_g(W) \subset Im(F)$, donc $Im(F) = V'$, et deuxièmement $Dim_C(V) = dim_C(V') = |G/H|.dim_C(W)$ d'après les propriétés. Ainsi, F vérifie toutes les conditions pour être un isomorphisme entre les deux représentations p et p'.

Théorème (Caractère d'une représentation induite) : Supposons que $(\theta, W)_H$ induit $(p, V)_G$. On a que $\forall g \in G$,

$$X_p(g) = \sum_{\substack{\bar{s} \in G/H \\ s^{-1}.g.s \in H^{=G/H \cap C(g)}}} X_\theta(s^{-1}.g.s) = \frac{1}{|H|} \sum_{\substack{s \in G \\ s.g.s^{-1} \in H}} X_\theta(s.g.s^{-1})$$

Preuve : Soit $(p, V)_G$ la représentation induite par $(\theta, W)_H$, i.e, $V = \bigoplus_{\bar{g} \in G/H} p_g(W) = \bigoplus_{\bar{g} \in G/H} W_g$.
Soit $u \in G$. p_u est un automorphisme de V permutant les $p_g(W)$, en effet, $p_u(p_g(W)) = p_{g.u}(W)$ et si $u.g = g_u.h$ avec $u_g \notin H,\ h \in H$, alors $p_u(W_g) = W_{g_u}$ et $g_u \notin H$.
La trace de p_u n'est donc rien d'autre que la somme des traces de ses restrictions sur les W_g qu'il laisse invariant! Or W_g est invariant par p_u ssi $p_u(p_g(W)) = p_g(W)$ ssi $p_{g^{-1}.u.g}(W) = P_1(W) = W$ ssi $g^{-1}.u.g \in H$. Ainsi, si on note X_V le caractère de V, on a $X_V(u) = \sum_{\bar{g} \in G/H \ g^{-1}.u.g \in H} Tr((p_u)_{|W_g})$.
Or si $g^{-1}.u.g \in H$ alors $\forall w \in W \ p_{g^{-1}} \circ p_u \circ p_g = p_{g^{-1}.u.g}(w) = \theta_{g^{-1}.u.g}(w)$, i.e, $Tr((p_u)_{|W_g}) = Tr(\theta_{g^{-1}.u.g}) = X_\theta(g^{-1}.u.g)$.Ce qui fini la preuve.

Langage modulaire :

Définition : Soient V un $C[G]$-module (représentation linéaire de G)et W un sous-$C[H]$-module de V. On dit que V est induit par W lorsque $V = \bigoplus_{\bar{g} \in G/H} g.W$.

Remarque : Cette définition traduit celle qu'on a vue avant, en effet, la représentation linéaire de G associée au $C[G]$-module V est

$$p : G \to GL(V)$$

$$g \mapsto p_g : x \mapsto g.x$$

Ainsi, V est induite par W lorsque $V = \bigotimes_{\bar{g} \in G/H} p_g(W) = \bigotimes_{\bar{g} \in G/H} g.W$.

Si on note $W' = C[G] \bigotimes_{C[H]} W$ le $C[G]$-module induit de W par extension de l'action de $C[H]$ à $C[G]$, i.e, les scalaires de $C[H]$ à $C[G]$, alors l'inclusion $W \to V$ se prolonge en un $C[G]$-morphisme (Application $C[G]$-linéaire) $i : W' \to V$, et on a la caractérisation suivante :

Proposition : V est induit par W si, et seulement si, $i : W' = C[G] \bigotimes_{C[H]} W \to V$ est un isomorphisme de $C[G]$-modules.

Cette caractérisation repose sur la notion de produit tensoriel de deux modules au dessus d'un autre module, juste pour rappel :

Définition (Produit tensoriel) Le produit tensoriel du module $C[G]$ et du $C[H]$-module W au dessus de $C[H]$, et noté $C[G] \bigotimes_{C[H]} W$, est définit sur l'espace $C[G] \times W$ par les trois propriétés suivantes :
1/ $\forall f, f' \in C[G], \forall x \in W,\ (f + f') \otimes x = f \otimes x + f' \otimes x$,
2/ $\forall f \in C[G], \forall x, x' \in W,\ f \otimes (x + x') = f \otimes x + f \otimes x'$,
3/ $\forall f \in C[G], \forall h \in C[H], \forall x \in W,\ f.h \otimes x = f \otimes h.x$,
La proposition précédente se résume au fait de pouvoir confondre "$\otimes$" et ".".

Preuve de la caractérisation :
Supposons que V est induit par W, alors :
La surjectivité de l'inclusion est claire.
Et on a la bijection car $dim_C(C[G] \bigotimes_{C[H]} W) = dim_C(V) = |G/H|.dim_C(W)$. en effet, si $x = f \otimes x \in W'$ alors $x = (\sum_{g \in G} f_g.g) \otimes x = (\sum_{\bar{g} \in G/H} \sum_{h \in H} f_{g.h}.g.h) \otimes x = \sum_{\bar{g} \in G/H} g \otimes (\sum_{h \in H} f_{g.h}.h.x)$ ainsi, on a pour la partie gauche $|G/H|$ degré de liberté. En multipliant ces degré par celles d'adroite, i.e, celles de W, on a ce qu'on veut.

Inversement, si i est un isomorphisme, alors par définition de la représentation induite, on a ce qu'on veut.

On vient de voir qu'une représentation induite existe toujours et est unique, on remarquant cela et avec la caractérisation, on peut donner la définition suivante :

Definition : Soit W un $C[H]$-module. alors le $C[G]$-module induit par W est défini comme $Ind_H^G(W) = C[G] \bigotimes_{C[H]} W$ où $C[G]$ est vu comme $C[H]$-module.

Remarques :
1/ Cette caractérisation de la représentation induite par W met en évidence don existence et son unicité.

On notera dans la suite $Ind_H^G(W)$ ou simplement $Ind(W)$ la représentation de G induite par W.
2/ Si V est induite par W et E un $C[G]$-module, alors $Hom^H(W, E) \simeq Hom^G(V, E)$ où $Hom^G(V, E)$ est l'ensemble des $C[G]$-morphismes.. Cela est un résultat direct du lemme introduit dans le début de ce chapitre.

3/ Transitivité : $K \subset H \subset G$ des groupes, alors $Ind_H^G(Ind_K^H(W)) = Ind_K^G(W)$.

Cela vient du fait que $C[G] \bigotimes_{C[H]} (C[H] \bigotimes_{C[K]} W) = C[G] \bigotimes_{C[K]} W$, c'est un calcul simple..

Proposition : Soit V un $C[G]$-module décompose en somme direct $V = \bigotimes_{i \in I} W_i$ de sous-espaces vectoriels permutés transitivement par G (i.e, $\forall i, j \in I, \exists g \in G,\ W_i = g.W_j$). Soit $j \in I$ et $W = W_j$. Notons H le sous-groupe de G stabilisant W. Alors W est H-stable et le $C[G]$-module V est induit par le $C[H]$-module H.

Remarque : On peut voir ça dans le cas où $V = \otimes_{g \in G} g.W$ où W est sous-C-espace vectoriel de V, soit H le sous groupe de G stabilisant W. Alors on tombe dans la définition.

Exemples : Si les $\forall i \in I, dim_C(W) = 1$, alors la représentation V associée au $C[G]$-module V est dite monomiale.

Caractère d'une représentation induite :

Définition : Soit $f : H \to C$ une fonction central sur H, et soit $f' : G \to C$ définie par :

$$f'(g) = \frac{1}{|H|} \sum_{\substack{s \in G \\ s.g.s^{-1} \in H}} f(s.g.s^{-1})$$

. On dit que f' est induite par f, on la note $f' = Ind_H^G(f) = Ind(f)$.

Proposition :
1/ f' est une fonction centrale sur de G. (Preuve : Claire, avec un changement de variable dans la somme..)
2/ Si f est le caractère d'une représentation W de H, alors $Ind(f)$ est le caractère de la représentation induite $Ind(W)$ de G.
Preuve : Faite dans la première partie.

Remarque : Rappelons que si $f, h : G \to C$ sont deux fonctions centrales de G, on note $< f|h >_G = \frac{1}{|G|} \sum_{g \in G} f(g^{-1}).h(g)$.
Maintenant,

Définition : si V, V' sont deux $C[G]$-modules, on pose $< V|V' >_G = dim_C(Hom^G(V, V'))$.

Lemme : si X, X' sont les caractères de V, V', alors $< V|V' >_G = < X|X' >_G$.

Preuve : On décompose les deux en somme d'irréductibles : $V = \sum_i n_i.W_i$ et $V' = \sum_j m_j.W'_j$, on a que $< X|X' >_G = \sum_i \sum_j n_i.m_j$ d'après la première partie. De plus, $< V|V' >_G = dim_C(Hom^H(V, V')) = dim_C(V).dim_C(V') = (\sum_i n_i).(\sum_j m_j) = \sum_i \sum_j n_i.m_j = < X|X' >_G$.

Notation : Si f est une fonction sur G, V une représentation de G, on note alors $Res_H(f)$ sa restriction au sous-groupe H, et $Res_H(V)$ de même.

Théorème (Formule de réciprocité de Frobenius): Soient f une fonction centrale se G et h une fonction centrale sur H. Alors on a que $< h|Res(f) >_H = < Ind(h)|f >_G$.
De manière équivalente, si V est un $C[G]$-module et W un $C[H]$-module. Alors $Hom^H(W, Res(V)) \simeq Hom^G(Ind(W), V)$.

Preuve :
On limitera notre raisonnement au caractères, vu qu'ils forment des bases de nos espaces. On suppose que f est le caractère d'un $C[G]$-module E et h est le caractère d'un $C[H]$-module W.
On a vu que $Hom^H(W, Res(E)) \simeq Hom^G(ind(W), E)$, ainsi, ils ont les mêmes dimensions, ce qui termine la preuve.

Remarques :
1/ Cela veut dire que Ind_H^G et Res_H^G sont des opérateurs adjoints.
2/ On utilise parfois la formule : $Ind_H^G(h.Res_H(f)) = Ind_H^G(h).f$
C'est un résultat direct du fait que $Ind_H^G(W \bigotimes_C Res_H^G(V)) \simeq Ind_H^G(W) \bigotimes_C V$.

Proposition : Soient W une représentation irréductible de H et V une représentation irréductible de G. Alors le nombre de fois qu'apparaît W dans $Res(V)$ est égale au nombre de fois que V apparaît dans $Ind(W)$.

Preuve : on regarde leurs caractères et on utilise le résultat de la première partie en regardant leur produit au sens $< .|. >$.

3.1 Restriction aux sous-groupes et d'irréductibilité de Mackey

Soient maintenant H, K deux sous-groupes de G, $p : H \to GL(W)$ une représentation de H et notons $V = Ind_H^G(W) = C[G] \bigotimes_{C[H]} W$. On veut déterminer la restriction $Res_K(V)$ de V à K.

Définition (Double classe): La relation d'équivalence : $g, g' \in G,\ gRg' \Longleftrightarrow \exists (h,k) \in H \times K,\ g' = h.g.k$ nous permet de définir la partition de G suivante : $G/(H,K) = \{H.g.K \mid g \in G\}$, et un élément $\bar{g} = H.g.K$ est appelé Double classe de g modulo (H,K).

Pour $\bar{g} \in G/(K,H)$ notons $H_g = g.H.g^{-1} \cap K$. C'est un sous groupe de G comme intersection, et est inclus dans K, c'est donc un sous groupe de K. Maintenant on pose, pour un $x \in H_g$, $p^g_x = p_{g^{-1}.x.g}$, et on obtient une suite fini de représentations linéaires $(p^g : H_g \to GL(W_g))_{g \in G}$.

H_g étant un sous groupe de K, on peut donc parler de la représentation induite $Ind^K_{H_g}(W_g)$ avec $\bar{g} \in G/(K,H)$.

Proposition :

$$Res_K(Ind^G_H(W)) \simeq \bigoplus_{\bar{g} \in G/(K,H)} Ind^K_{H_g}(W_g)$$

Preuve : On a que $V = \bigoplus_{\bar{x} \in G/H} x.W$.
Soient $\bar{s} \in G/(K,H)$ et V_s le sous-C-espace vectoriel de V engendré par les $x.W$ où $x \in \bar{s}$. Et par construction $V = \bigoplus_{\bar{s} \in G/(K,H)} V_s$ (on a juste regroupé certains $x.V$ par paquets..).
De plus, chaque V_s est stable par K : $K.k.s.h.W = K.s.h.W \subset x.W$
Il suffit donc de montrer que chaque V_s est K-isomorphe à $Ind^K_{H_s}(W_s)$.
Or comme le sous-groupe de K stabilisant $s.W$ est exactement H_s : En effet, $x.s.W = sW \Longleftrightarrow s^{-1}.x.s.W = W \Longleftrightarrow s^{-1}.x.s \in H \Longleftrightarrow x \in s.H.s^{-1}$ et comme $x \in K$ on a que $x \in s.H.s^{-1} \cap K$.
Ainsi, V_s est somme directe des $x.s.W$ où $x \in K/H_s$, i.e, $V_s = Ind^K_{H_s}(s.W)$ d'après le lemme de la phase précédente.
$s : W_s \to s.W$ étant un isomorphisme, ainsi, $V_s \simeq Ind^K_{H_s}(W_s)$.
Ce qui termine la preuve.

Remarque : V_s ne dépend que de $\bar{s} \in G/(K,H)$. Et donc, à isomorphisme près, $Ind^K_{H_s}(W_s)$ ne dépend que de $\bar{s} \in G/(K,H)$.

Critère de Mackey : On s'intéresse maintenant au cas où $K = H$, c'est-à-dire, des doubles classes modulo (H,H), et donc pour $\bar{g} \in G/(H,H)$, $H_g = g.H.g^{-1} \cap H$

qui est un sous groupe de H. La représentation p de H restreinte à H_g, noté $Res_g(p)$ est encore une représentation de H_g. On a ainsi :

Proposition (Critère d'irréductibilité de Mackey): La représentation $V = Ind_H^G(W)$ est irréductible si, et seulement si,
1/ W est irréductible,
- ET,
2/ $\forall g \in G - H$, les deux représentations p^g et Res_g sont premiers entre eux, i.e, n'ont aucun composante irréductible commune, i.e, $< p^g | Res_g >_{H_g} = 0$.

Preuve : D'après la première partie, V est irréductible ssi $< V|V >_G = 1$.
On a aussi que $< V|V >_G = < W|Res_H^G(V) >_H$
Or d'après la formule de Frobenius, $Res_H^G(V) = \bigoplus_{\bar{s} \in G/(HmH)} Ind_{H_s}^H(p^s)$
car $V = Ind_H^G(W)$.
En appliquant encore la formule de Frobenius,
$< V|V >_G = \sum_{\bar{s} \in G/(H,H)} < W|Ind_{H_s}^H(p^s) >_H$
$= \sum_{\bar{s} \in G/(H,H)} < Res_{H_s}(W)|p^s >_{H_s}$.
Comme $< Res_{H_e}(W)|p^e >_{H_e} = < W, W >_H \geq 1$, alors $< V|V >_G = 1$
ssi $< Res_{H_e}(W)|p^e >_{H_e} = < W|W >_H = 1$
et $< Res_{H_s}(W)|p^s >_{H_s} = 0 \ \forall \bar{s} \neq \bar{e}, \ i.e, \ s \notin H$,
i.e, ssi W est irréductible et que W et $Res_{H_s}(W)$ sont premiers entre eux.

Corollaire : Si H est distingué dans G, alors $Ind_H^G(W)$ est irréductible si et seulement si p (W) est irréductible et n'est isomorphe à aucune des p^g où $g \in G - H$.

Preuve : Car $\forall \bar{s} \in G/(H,H)$, $H_s = H$ et $Res_{H_s}(W) = W$, i.e, ssi $\bar{s} = \bar{e}$ est l'unique qui donne $< Res_{H_s}(W)|p^s >_{H_s} = 1$.

La paragraphe suivante est consacrée à des exemples d'applications de ce qu'on vient de faire.

Chapter 4

Exemples classiques de représentations induites

4.1 Sous groupes distingués, degré de représentations irréductibles

Définition : Une représentation est dite isotypique si elle est somme directe de représentations irréductibles deux à deux isomorphes.

Proposition (Une classification :) Soient $A \triangleright G$ et (p, V) une représentation irréductible de G. Alors :
1/ Ou bien il existe un sous groupe H propre de G contenant A et une représentation irréductible θ de H tel que $p = Ind_H^G(\theta)$,
2/ Ou bien $Res_A(p)$ est isotypique.

Preuve : Soit $V = \bigoplus_i V_i$ la décomposition canonique (Voir partie 1) de $(p_{|A}, V)$, c'est à dire, la restriction de p à A qui est encore une representation de A dans V.
(en effet, V_i est somme isotypique de representations irreductibles de A, en effet, $V_i = \bigoplus_j W_{i,j}$ où $W_{i,j} \simeq W_{i,k}$.)
Soit $g \in G$,
On a que $V = p_g(V) = \sum_i p_g(V_i)$. Cette somme est direct, car si $x \in p_g(V_i) \cap p_g(v_j)$, alors $\exists x_i \in V_i,\ x_j \in V_j$ tels que $p_g(x_i) = x = p_g(x_j)$, et comme p_g est

un automorphisme, alors $x_i = x_j$, i.e, $x_j = x_i \in V_i \cap V_j = \{0\}$ si $i \neq j$, i.e, $\bigoplus_i V_i = V = \bigoplus_i p_g(V_i)$ et par unicité de la decomposition canonique, on a que $\forall i, \exists j, V_i = p_g(V_j)$, ainsi, p_g permute les V_i, et en notant l'une d'entre eux V_0,
On a deux cas :
1/ $V_0 = V$ et donc V est somme isotypique (des $W_{0,j}$), et on trouve le cas 2 du théorème.
2/ Soit H le sous-groupe de G stabilisant V_0 (contient donc A car les V_i Sont A-stables). On a que $V = \bigoplus_{\bar{g} \in G/H} p_g(V_0)$, ainsi, p est induite par $(p_{|H}, V_0)_H$, et on trouve le cas 1.

Remarque : Si de plus A est commutatif, alors si $a \in A$, alors p_b et p_a cummutent $\forall b \in A$. ainsi, la restriction de p_a sur chaque V_i est une homothetie de rapport l'une de ses valeurs propres. Si les V_i sont isomorphes, et donc on est dans le cas 1 du théorème, alors les restrictions de p_a sur chaque V_i ont le meme valeur propre, i.e, p_a est une homothétie. Pour illuster ça, on a que la matrice de p_a est par bloques (4 bloques $(A_1, .., A_4)$ par exemple, chaque bloque correspont à la matrice de p_a sur V_i) $\begin{bmatrix} A_1 & O & O & O \\ O & A_2 & O & O \\ O & O & A_3 & O \\ O & O & O & A_4 \end{bmatrix}$. Si A est commutatif, alors chaque A_i est de la forme $\lambda_1 I_{dim(V_i)} = \lambda_i I_{n_i}$. Si depluis les V_i sont isomorphes, alors $\lambda_1 = .. = \lambda_2 = \lambda$, et donc $\begin{bmatrix} A_1 & O & O & O \\ O & A_2 & O & O \\ O & O & A_3 & O \\ O & O & O & A_4 \end{bmatrix} = \begin{bmatrix} \lambda_1 . I_{n_1} & O & O & O \\ O & \lambda_2 I_{n_2} & O & O \\ O & O & \lambda_3 I_{n_3} & O \\ O & O & O & A\lambda_4 I_{n_4} \end{bmatrix}$
$= \begin{bmatrix} \lambda I_{n_1} & O & O & O \\ O & \lambda I_{n_2} & O & O \\ O & O & \lambda I_{n_3} & O \\ O & O & O & \lambda I_{n_4} \end{bmatrix} = \lambda . \begin{bmatrix} I_{n_1} & O & O & O \\ O & I_{n_2} & O & O \\ O & O & I_{n_3} & O \\ O & O & O & I_{n_4} \end{bmatrix} = \lambda I_n$ avec $n = dim_C(V)$.

Corollaire : $A \triangleright G$ avec A commutatif. Alors le degré de toute représentation irréductible de G divise $|G/A|$.

Preuve: Par récurrence sur $n = |G|$. Donc supposons que la proposition est vraie pour $n + 1$.
On utilise la proposition précédente :
Si on est dans le cas a, alors le degré de θ divise $|H/A|$ et comme $|G/A| =$

$|G/H|.|H/A|$ alors le degré de θ divise $|G/A|$.
Si on est dans le cas b, Alors si on note $M = p(G)$ et $N = p(A)$ qui sont encore des groupes de $GL(V)$, et comme l'application usuelle $G/A \to M/N$ est surjective, alors M/N divise G/A. Or comme tout élément de N sont des homothéties, alors $N \subset Z(M)$ et d'après le chapitre 2, le degré de p divise $|M/N|$, ainsi, divise $|G/A|$.

Corollaire : Si G est un groupe abelien, alors ses représentations irreductibles sont de degré 1.

Preuve : on prend $A = G$ dans le corollaire précédent.

4.2 Représentations linéaires des groupes hyper-résolubles

4.2.1 Rappel :

Pour toute autre precision, voir "Serge Lang Algèbre"

Définition (Groupes résolubles) : Un groupe G est dit résoluble s'il existe une suite de sous groupes $(G_i)_{i=1:n}$ tels que $\{e\} = G_0 \subset G_1 \subset .. \subset G_n = G$, $\forall i = 1 : n,\ G_{i-1} \triangleright G_i$ et G_i/G_{i-1} est un groupe commutatif.
On dit que G est hyper-résoluble si de plus $\forall i,\ G_i \triangleright G$ et G_i/G_{i-1} est cyclique.(On imite $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$..)

Définition (Groupe nilpotent): même définition sauf qu'on exige que les $G_i/G_{i-1} \subset Z(G/G_{i-1})$.

Remarque : On a clairement que Nilpotent $\Longrightarrow$ Hyper-résoluble $\Longrightarrow$ Résoluble . En effet tout groupe cyclique est commutatif)

Théorème : Tout p-groupe G est nilpotent, donc hyper-résoluble et donc résoluble.

Preuve : En effet, le centre de G est de cardinal au moins p, i.e, $|Z(G)| \geq p$. Cela vient des equations aux classes et que $Z(G)$ est non trivial. (Un exercice intéressant)

Propriétés :
1/ Tout sous groupe d'un groupe nilpotent est encore nilpotent.
2/ Tout groupe quotient d'un groupe résoluble est résoluble.
3/ Un groupe simple est résoluble si et seulement si il est abélien (i.e, ssi c'est un groupe d'ordre premier p, i.e, $\simeq \mathbb{Z}/p\mathbb{Z}$).

Preuve : Voir polycopie sur les groupes de M. J.P.Serre.

Proposition : Soit V un K-espace vectoriel avec K de caractéristique p et soit $p : G \to GL(V)$ une représentation linéaire de G, un p-groupe. Alors $\exists 0 \neq x \in V$ tel que $\forall g \in G,\ p_g(x) = x$.

Preuve : Soit $x \neq 0 \in V$, et soit X le sous groupe du groupe additif V, engendré par $\{p_g(x) | g \in G\}$, i.e, c'est un $\mathbb{Z}$-module de type fini et de torsion. Ainsi, X est fini, de cardinal divisible par p et en appliquant les résultats sur les groupes finis, on a que $|X| - |X^G| \in p\mathbb{Z}$, i.e,$p$ divise $|X^G|$ et ce dernier contient $\{0\}$, i.e, $|X^G| \geq p \geq 2$. Ce qui termine la preuve.

Corollaire : La seule représentation d'un p-groupe G en caractéristique p est la représentation trivial.

Lemme : Soit G un groupe hyper-résoluble non commutatif. Il existe un sous-groupe commutatif distingué de G non contenu dans $Z(G)$ (Autrement, il existe des éléments de G qui commute entre eux de G et qui ne commutent pas avec tout les éléments de G).

Preuve : Le groupe $G/Z(G)$ est hyper-résoluble. Soit G_2 le deuxième sous-groupe de sa suite résoluble, et est cyclique distingué de $G/Z(G)$. On prend l'image réciproque de G_2 par la projection canonique. Cela termine la preuve.

Théorème (Représentation des groupes hyper résolubles) : Toute représentation irréductible d'un groupe hyper-résoluble G est induite par une représentation de degré 1 d'un sous groupe de G.

Preuve : Par récurrence sur l'ordre de $n = |G|$ de G. Supposons sans perte de généralité que la représentation est fidèle, i.e, $Ker(p) = \{e\}$.
Si G est abélien, alors d'après la première partie tout représentation irréductible de G est de degré au plus $|G/G| = 1$.
Sinon, d'après le lemme, il existe un sous groupe commutatif A distingué non contenu dans $Z(G)$.
Comme p est fidèle, $p(A)$ n'est pas contenue dans le centre de $p(G)$, i.e, $\exists a \in A$, p_a n'est pas une homothétie, i.e, p^A n'est pas isotypique d'après la classification établie auparavant, et par la même classification, Soit H le sous-groupe contenant A distinct de G dont la représentation irréductible θ induit p. En appliquant l'hypothèse de récurrence sur H, θ est induite par un degré 1 représentation, i.e, comme θ est irréductible, alors elle est de degré 1, ce qui termine la preuve.

Remarque : Soit G un groupe hyper-résoluble. Comme $C[G] \simeq n_1.W_1 \oplus .. \oplus n_h.W_h$, et d'après le théorème précèdent, on a $\forall i = 1 : h$, $\exists A_i \triangleright G$,$x_i \in W_i$ tels que $C[G] \simeq \bigoplus_{i=1}^{h} |G/A_i|.Ind_{A_i}^{G}(C.x_i)$.

Chapter 5

Théorème d'Artin

Commençons par introduire certains notions nécessaires pour annoncer le théorème d'Artin :

5.1 L'anneau des caractères virtuels

Définition (L'anneau des caractères virtuels) Soient G un groupe fini, $X_1, .., X_h$ ses différents caractères irréductibles. $R_+(G) = \mathbb{N}.X_1 + .. + \mathbb{N}.X_h$ est l'ensemble des caractères de G (Une définition naturelle des caractères de G, comme le montre la proposition suivante). On note $R(G) = \mathbb{Z}.X_1 + .. + \mathbb{Z}.X_h$, appelé l'ensemble des caractères virtuels de G.

Proposition : $(R(G), +, .)$ est un anneau commutatif.

Preuve : C'est en effet un sous-anneau de l'anneau $F_C(G)$ des fonctions centrales de G, car comme on a vu dans la première partie, le produit de deux caractères est encore un caractère.

Proposition : Si H est un sous-groupe de G, alors l'opérateur $Res_H^G : R(G) \to R(H)$ est un morphisme d'anneaux et l'opérateur $Ind_H^G : R(H) \to R(G)$ est un morphisme de groupes abéliens.

Preuve : Res_H^G étant un morphisme d'anneaux est claire.
En ce qui concerne la deuxième proposition, cela résulte du fait que $C[G] \bigotimes_{C[H]} W + C[G] \bigotimes_{C[H]W'} = C[G] \bigotimes_{C[H]}(W + W')$.

Corollaire : $Ind_H^G(R(H))$ est un idéal de l'anneau $R(G)$.

Preuve : On a que $Ind_H^G(h.Res_H^G(f)) = f.Ind_H^G(h)$. Ainsi, si $h \in R(H), f \in R(G)$ alors $f.Ind_H^G(h) = Ind_H^G(Res_H^G(f).h) \in Im(Ind_H^G)$.

5.2 Théorème d'Artin

Annonçons maintenant le grand théorème du chapitre, ce théorème nous donne une façon de construire $R(G)$:

Théorème (d'Artin): Soient G un groupe fini, X une famille de sous-groupes de G et

$$Ind : \bigoplus_{H \in X} R(H) \to R(G)$$

$$\sum_{H \in X} f_H \mapsto \sum_{H \in X} Ind_H^G(f_H)$$

Où

$$Ind_H^G(f_H) : x \in G \mapsto \frac{1}{|G|} \sum_{\begin{cases} g \in G \\ g.x.g^{-1} \in H \end{cases}} f_H(g.x.g^{-1})$$

On a l'équivalence suivante :
1/ G est réunion des conjugués des sous-groupes appartenant à X, i.e,

$$G = \bigcup_{\substack{g \in G \\ H \in X}} g.H.g^{-1}$$

,
2/ Le conoyau de Ind est un anneau fini.

Remarques :
1/ Rappel : Le conoyau de Ind est l'ensemble quotient $R(G)/Im(Ind)$, et on a vu que $Im(Ind)$ est un idéal de $R(G)$,
4/ Pour comprendre le conoyau de Ind, on introduit la règle suivante : pour un élément $n_k.X_k$ de $R(G)$, s'il est induit (ou somme d'éléments induits) par un sous-groupe (des sous-groupes) dans X, alors on l'enlève (On le réduit à 0), ainsi, la classe d'un élément $n_1.X_1 + .. + n_h.X_h$ de $R(G)$ modulo $Im(Ind)$ n'est rien qu'un élément après avoir fait la règle précédente.

Remarque : Nous allons voir qu'il y a une autre version de ce corollaire dans le chapitre suivant..

Preuve de 2$\Longrightarrow$1 : Soit $S = \cup_{(g,H)\in G\times X} g.H.g^{-1}$, donc il suffit de montrer que les fonctions centrales de S coïncident avec celles de G, car $F_c(G) = C \otimes R(G)$, et donc $R(G) = R(S)$. D'après l'hypothèse 2, il suffit de montrer cela pour les fonctions du type $Ind_H^G(f_H)$ avec $f_H \in R(H)$, or d'après la formule, $Ind_H^G(f_H)(x) = \frac{1}{|H|}\sum_{g\in G, g.x.g^{-1}\in H} f_H(g.x.g^{-1})$,i.e, si $x \notin S$ alors $Ind_H^G(f_H)(x) = 0$. Ce qui termine la preuve.

Pour l'autre implication, nous aurons besoin d'introduire une fonction :

Définition : Soit A un groupe cyclique. On défini la fonction

$$\theta_A : A \to \{0, |A|\}$$

$$x \mapsto \begin{cases} |A| \ si \ \ < x >= A \\ 0 \ sinon \end{cases}$$

.

Intéressant à remarquer : On peut voir que $\frac{1}{|A|}\sum_{x\in A}\theta_A(x) = \phi(|A|)$ où ϕ est la caractéristique d'Euler.

Proposition : Si G est un groupe fini, alors $|G| = \sum_{A\subset G \ cyclique} Ind_A^G(\theta_A)$.

Preuve : D'après ce qu'on vient de voir sur les caractères induits, on a que

$$Ind_A^G(\theta_A)(x) = \frac{1}{|A|} \sum_{\substack{g \in G \\ g.x.g^{-1} \in A}} \theta_A(g.x.g^{-1})$$

=

$$\frac{1}{|A|} \sum_{\substack{g \in G \\ < g.x.g^{-1} >= A}} |A|$$

=

$$\sum_{\substack{g \in G \\ < g.x.g^{-1} >= A}} 1$$

.
Or, si $g.x.g^{-1}$ et $s.x.s^{-1}$ engendrent A, alors $g^{-1}.A.g = s^{-1}.A.s = \{e, x, x^2, .., x^{|A|-1}\}$, i.e, $s = g$. Ainsi, tout les engendrants de A de la forme $g.x.g^{-1}$ sont égaux,et $\forall g \in G \exists! A$ sous-groupe cyclique de G engendré par g, i.e,

$$\sum_{\substack{g \in G \\ < g.x.g^{-1} >= A}} 1 = \sum_{g \in G} 1 = |G|$$

.
Ce qui termine la preuve.

Proposition : Si A est un groupe cyclique, alors $\theta_A \in R(A)$.

Preuve : Par récurrence sur l'ordre du groupe A:
On a que $|A| = \sum_{P \subset A \ cyc} Ind_P^A(\theta_P^A) = \theta_A + \sum_{P \subsetneq A \ cyc} Ind_P^A(\theta_P)$,
et par récurrence,pour $P \neq A$, $\theta_P \in R(P)$ et donc $Ind_P^A(\theta_P) \in R(A)$ et comme $|A| \in R(A)$, on a le résultat souhaité.

Proposition : Comme $R(G)$ est un groupe de type fini, alors la condition (2) est équivalente à : Pour tout caractère X de G, il existe des caractères virtuels $X_H \in R(H),\ H \in X$ et $d \geq 1 \in \mathbb{N}$ tels que $d.X = \sum_{H \in X} Ind_H^G(X_H)$,

Preuve :
- En effet, si $R(G) + Ind(\bigoplus_{H\in X} R(H))$ est fini, égale à $\{\bar{F}_1, .., \bar{F}_k\}$ alors si X est un caractère de G, alors $\exists i \in [|1, k|]$ tel que $X - F_i \in Ind(\bigoplus_{H\in X} R(H))$, et donc il existe des $f_H \in R(H)$ tels que $X = F_i + \sum_H Ind_H^G(f_H)$.
Le conoyau étant un groupe fini (et tout groupe fini est de torsion!), alors $\exists d \geq 1$ tel que $d.\bar{F}_i = \bar{0}$, i.e, $d.F_i \in Ind(\bigoplus_{H\in X} R(H))$, et donc $d.X \in Ind(\bigoplus_{H\in X} R(H))$. Voilà.

Corollaire : Tout caractère de G est combinaison linéaire rationnel de caractères induits par des caractères de sous-groupes cycliques de G.

Preuve : La famille des sous-groupes cycliques vérifie (1),en effet, $G = \cup_{g\in G} < g >$, et d'après la proposition dans la preuve.

Proposition : Si $\exists g \in G$ tel que $A' \subset g.A.g^{-1}$, alors $Ind_{A'}^G(R(A')) \subset Ind_A^G(R(A))$.

Preuve : Cela vient de la formule : Si $X \in R(G)$ tel que $X(x) = Ind_{A'}^G(f'_A)(x) = \frac{1}{|A'|} \sum_{s\in G,\ s.x.s^{-1}\in A'} f_A(s.x.s^-)$ avec un changement de variables et en multipliant par $\frac{|A'|}{|A|}$, alors en utilisant le corollaire précédent, on termine la preuve.

Prouvons maintenant l'implication :

D'après la proposition précédente, On peut supposer que X est la famille de tout les sous-groupes cycliques de G. On a donc $|G| = \sum_{P\in X} Ind_P^G(\theta_P)$, i.e, $|G| \in Im(Ind)$, or ceci est un idéal de $R(G)$, alors les éléments de la forme $|G|.f_G$ où $f_G \in R(G)$ sont dans $Im(Ind)$. Ce qui termine la preuve de l'implication.

Chapter 6

Théorème de Brauer et applications

Dans la suite, p désigne souvent un nombre premier.
Comme la paragraphe précédente, nous aurons besoin de définir certaines notions pour annoncer le théorème de Brauer :

6.1 Définitions et lemmes

Définition (p-élément et p'-élément): Soit G un groupe fini. $g \in G$ est dit un p-élément (ou p-unipotent) si g est d'ordre une puissance de p (Analogie aux p-groupes), et est dit p'-élément (p-régulier) si son ordre est premier à p.

Proposition : Tout élément $g \in G$ s'écrit de façon unique comme $g = g_u.g_r$ où g_u est p-unipotent, g_r est p-régulier et g_u, g_r commutent. De plus, g_u, g_r sont des puissances de g.

Preuve : g est forcement d'ordre $p^r.m$ où $pgcd(m,p) = 1$. Alors d'après le théorème de Bezout, $1 = a.p^r + b.m$, et on a que $g = g^1 = g^{a.p^r+b.m} = (g^{p^r})^a.(g^m)^b = g_u.g_r$, et l'unicité est claire. Ce qui prouve tout ce qu'on a dit.

Définition (Sous-groupes p-élémentaires): Un sous-groupe H de G est dit p-élémentaire s'il est produit direct d'un groupe cyclique C d'ordre premier à p par

un p-groupe P, i.e, $H = C \times P$.
Un tel groupe est nilpotent et sa décomposition en $C \times P$ est unique, de plus, C est l'ensemble des p'-éléments et P l'ensemble des p-éléments.

Nous admettons dans la suite les deux lemmes techniques suivants :

Lemme 1 **:** Soit G un groupe fini, V_p le sous-groupe du groupe additif $R(G)$ des caractères induits par des sous-groupes p-élémentaires de G. Alors, $R(G)/V_p$ est un groupe fini d'ordre non divisible par p.

Pour la preuve : La preuve détaillée se trouve dans le livre de J-P.Serre sur les représentation ainsi que sur le livre Algebra de Serge Lang.

Remarque : Si on note X_p l'ensemble des sous-groupes p-élémentaires de G, alors V_p est l'image du morphisme $Ind : \bigoplus_{H \in X_p} R(H) \to R(G)$. Ainsi, V_p est un idéal de $R(G)$ et donc comme dans la preuve du théorème d'Artin, pour démontrer le lemme, il suffit de montrer qu'il existe $m \in \mathbb{N}$ non divisible par p et tel que $m.1_{C[G]} \in V_p$. D'où le lemme :

Lemme 2 : Supposons que $|G| = p^n.l$ tel que p et l sont premiers entre eux. Alors $l.1_{C[G]} = l \in V_p$.

Pour la preuve : même remarque précédente.

Annonçons maintenant le grand théorème de la partie :

Théorème de Brauer : Tout caractère de G est combinaison linéaire entière de caractères induits par des caractères des sous-groupes élémentaires (p-élémentaires pour un p premier).

Remarque : Autrement, $\forall X \in R_+(G), \exists H_{p_1}, .., Hp_n$ des sous-groupes p_i-élémentaires de G, $(m_1, .., m_n) \subset \mathbb{Z}$ et des $X_{H_{p_i}} \in R_+(H_{p_i})$ tels que $X = \sum_{i=1}^{n} m_i.Ind_{H_{p_i}}^{G}(X_{H_{p_i}})$.

Remarque BIS : On peut même montrer que la famille des sous-groupes élémentaires de G est la plus petite pour laquelle le théorème de Brauer soit vrai. (Voir le livre de J-P.Serre sur les représentations)

Preuve :

Soit V_p le sous groupe de $R(G)$ formé des caractère induits par des sous groupes p-élémentaires de G. Montrons que $V = \sum_{p\ premier} V_p = R(G)$: Comme V contient V_p, alors $|R(G)/V_p|$ est fini et premier à p (d'après le lemme 1), d'autre part on a que $|R(G)/V_p| = |R(G)/V|.|V/V_p|$, donc $|R(G)/V|$ est premier avec p, comme p étant un premier quelconque, alors on a forcément $|R(G)/V| = 1$ ainsi $R(G) = V$, Ce qui termine la preuve.

Théorème : Tout caractère de G est combinaison linaire entière de caractères de dimension 1 (dits monomiaux).

Preuve :

On utilise le théorème de Brauer. En , Soit $X \in R(G)$, alors $X = \sum_{i=1}^{h} X_i$ où $(X_1, .., X_h)$ sont les différents caractères irréductibles de G. On applique le théorème de Brauer sur chaque X_i, on va le faire sur X_1 et on fait la même chose avec le reste pour économiser notre matière grise. On a que $X_1 = \sum_{i=1}^{n} m_i Ind_{H_{p_i}}^{G}(f_i)$ où H_{p_i} est un sous-groupe p-élémentaire de G et $f_i \in R(H_{p_i})$. Soient $(C_{1,i}, .., C_{q_i,i})$ les différents caractères irréductibles de H_{p_i}, on a donc $f_i = \sum_{j=1}^{q_i} h_j.C_{j,1}$ On va se concentrer comme on l'a fait précédemment sur $C_{1,i}$. Comme H_{p_i} est nilpotent (car élémentaire), i.e, hyper-résoluble, alors d'après la section sur les Représentations des groupes hyper-résolubles, et comme $C_{1,i}$ est une caractère irréductible de H_{p_i}, il est induit par un caractère d'une représentation monomiale (de degré 1).
La formule de transitivité $Ind_K^G = Ind_H^G(Ind_K^H)$ et le fait que l'induction est un morphisme de groupes additifs nous permet de conclure la preuve.

Remarques : Le théorème précédent est très important et intervient dans plusieurs applications dans la théorie des représentations, par exemple on peut se restreint au cas où les caractères sont de degré 1 qui sont induit par des caractères de sous-groupes cycliques.

6.2 Exemples d'application du théorème de Brauer

6.2.1 Un théorème de Frobenius

Soit maintenant B un sous-anneau de C et G un groupe fini.

Théorème : Soit f une fonction centrale sur G, et supposons que $\forall H$ sous-groupe élémentaire de G, $Res^G_H(f) \in B \otimes R(H)$. Alors f est à valeurs dans $B \otimes R(G)$.

Preuve : Notons X l'ensemble des sous-groupes élémentaires de G. Le théorème de Brauer (Corollaire) implique que $1_{C[G]} = \sum_{H\in X} Ind^G_H(f_H)$ où $f_H \in R(H)$. ainsi, on a que $f = \sum_{H\in X} f.Ind^G_H(f_H) = \sum_{H\in X} Ind^G_H(Res^G_H(f).f_H)$. Comme $f_H \in R(H)$ et $Res^G_H(f) \in B \otimes R(H)$, alors $Res^G_H(f).f_H \in B \otimes R(H)$, ainsi, $Ind^G_H(Res^G_H(f).f_H) \in B \otimes R(G)$. Ceci termine la preuve.

Théorème : Supposons que B contient $\mathbb{Q}$ et que $\forall H$ sous-groupe cyclique de G $Res^G_H(f) \in B \otimes R(H)$. Alors, $f \in B \otimes R(G)$.

Preuve : Cela résulte du théorème d'Artin. En effet supposons que X est l'ensemble des sous groupes cycliques de G. On a que $1_{C[G]} \in R_+(G)$, et donc il est combinaison rationnelle de caractères induits par les sous-groupes cycliques de G , i.e, $1_{C[G]} = \sum_{H\in X} q_H.Ind^G_H(f_H)$ où $f_H \in R(H)$ et $q_H \in \mathbb{Q}$. Comme on a supposé que B contient $\mathbb{Q}$, alors cette combinaison linaire rationnelle est aussi combinaison linéaire á valeurs dans B, i.e, $q_H.Ind^G_H(f_H) \in B \otimes R(H)$. Et de manière analogue que la preuve du théorème précédent, on trouve le résultat voulu.

Soient maintenant A le sous-anneau de C engendré par les Racines $|G|$-ièmes de l'unité et $n \in \mathbb{N}^*$.

Définition : Soit f une fonction centrale sur G. Nous définissons l'opérateur ψ^n

$$\psi^n : f \mapsto \psi^n f : x \mapsto f(x^n)$$

.

Remarque : On a clairement que $\psi^n : R(G) \to R(G)$. Et :

Théorème : Si $f : G \to A$ est une fonction centrale sur G à valeurs dans A, alors $\frac{|G|}{pgcd(|G|,n)}.\psi^n f \in A \otimes R(G)$.

Preuve (Partielle) : D'après les deux théorèmes précédent (le premier), il suffit de vérifie que la restriction $Res^G_H(\frac{|G|}{pgcd(|G|,n)}\psi^n.f) \in A \otimes R(H)$ pour tout sous-groupe H élémentaire de G. Or d'après les propriétés sur l'ordre d'un élément d'un groupe cyclique, comme $|H|$ divise $|G|$ (Th. Lagrange), alors $\frac{|H|}{pgcd(|H|,n)}$ divise $\frac{|G|}{pgcd(|G|,n)}$, ainsi, Il suffit de montrer que $\frac{|H|}{pgcd(|H|,n)}.\psi^n(Res^G_H(f)) \in A \otimes R(H)$. On est donc ramené à montrer le théorème pour $G = H$ un groupe élémentaire. On peut se restreindre au cas où G est un p-groupe, et en utilisant le fait que ses caractères irréductibles sont induit par des caractères de degré 1..

Définition : Si g est une classe de conjugaison de G, on défini la fonction caractéristique de cette classe comme $f_g : x \mapsto \begin{cases} 1 \ si \ x \in g \\ 0 \ sinon \end{cases}$ et on a que $\psi^n f_g(x) = \begin{cases} 1 \ si \ x^n \in g \\ 0 \ sinon \end{cases}$.

Toute fonction centrale $f : G \to A$ sur G étant combinaison linéaire des f_g, on a donc :

Théorème : La fonction $\frac{|G|}{pgcd(|G|,n)}.\psi^n f_g \in A \otimes R(G)$. Ou, de manière équivalente, pour tout caractère X de G, $\frac{1}{pgcd(|G|,n)} \sum_{x^n \in g} X(x) \in A$.

Preuve : la première énoncée est claire, et pour l'équivalence, On a que $< \frac{|G|}{pgcd(|G|,n)}\psi^n(f_g)|X >_G = \frac{|G|}{pgcd(|G|,n)} < \psi^n(f_g)|X >_G \in A$, i.e, $\frac{1}{pgcd(|G|,n)} \sum_{x^n \in g} X(x) \in A$.

On prend $X = 1_{C[G]}$ et on trouve :

Corollaire 1 : Pour toute classe de conjugaison g de G, le nombre d'éléments $x \in G$ tels que $x^n \in g$ est un multiple de $pgcd(|G|, n)$.

Preuve : On trouve que $\frac{1}{pgcd(|G|,n)} \sum_{x^n \in g} 1 \in A$, i.e, $\frac{Card(\{x \in G \mid x^n \in g\})}{pgcd(|G|,n)} \in A$.

On prend $g = 1$ la classe du neutre 1 de G, on a que :

Corollaire 2 : $\forall n|_{|G|}$, $n|_{Card(\{x \in G \mid x^n = 1\})}$ (i.e, $Card(\{x \in G \mid x^n = 1\}) \in n.\mathbb{Z}$)

Preuve : Claire, et la condition $n|_{|G|}$ est nécessaire car tout élément n vérifiant $x^n = 1$ divise forcement l'ordre de G.

6.2.2 Spectre de $A \otimes R(G)$ et sa topologie

Rappels sur les spectres:

A sera un anneau commutatif quelconque,

Définition (Spectre) : Soit A un anneau commutatif. Le spectre de A, noté $Spec(A)$, est l'ensemble des idéaux premiers de A.

Remarques : Un élément de $Spec(A)$ est appelé "point" de $Spec(A)$.

Définition : Soit $f \in A$. L'ensemble des éléments de $Spec(A)$ contenant f est appelé l'ensemble des zéros de f, noté $O(f)$.

Remarque : C'est en effet l'ensemble des idéaux premiers P de A tel que $\pi_P : A \to A/P$ s'annule en f.

Définition : Soit a un idéal de A. $O(a)$ sera l'ensemble des zéros des éléments de a (L'ensemble des éléments de $Spec(A)$ contenant l'idéal a).

Définition : Nous Rappelons que si a est un idéal de A, le radical de a, noté $Rad(a)$ est l'ensemble $\{x \in A \mid \exists n \in \mathbb{N},\ x^n \in a\}$.

Proposition : Soit a et b deux idéaux de A. On a :
1/ $O(a.b) = O(a) \cup O(b)$,
2/ Si $(a_i)_i$ est une famille d'idéaux de A, alors $O(\sum_i a_i) = \cap_i O(a_i)$,
3/ $O(a) \subset O(b)$ si et seulement si $Rad(b) \subset Rad(a)$,

Preuve :
1/ Si un idéal premier P contient $a.b$, alors par définition d'un idéal premier, P contient a ou b.
Inversement, si P contient a, alors il contient $a.b$ par définition d'un idéal.
2/ $\sum_i a_i$ est l'idéal engendré par $\cup_i a_i$, et on raisonne de manière similaire qu'en 1.
3/ Croyez-moi !(Je rigole)
En effet, cela résulte du lemme facile à prouver : $x \in A$ est nilpotent ssi il est contenu dans tout point du $Spec(A)$.
et puis on l'applique sur l'anneau A/P.

Définition : Un ensemble C de $Spec(A)$, est dit fermé s'il existe un idéal a de A tels que C est l'ensemble des idéaux premier de A contenant a, i.e, $C = O(a)$. Le complémentaire d'un tel ensemble est dit ouvert de $Spec(A)$.

Proposition (Zariski?): L'ensemble des $\{C_C^{Spec(A)} \mid C\ fermé\ de\ Spec(A)\}$ est une topologie sur $Spec(A)$, appelée topologie de Zariski.

Preuve : par construction, et par la proposition précédente.

Remarque : Cet espace topologique n'est pas séparable.

Proposition : Soient A et B deux anneaux commutatifs, $\phi : A \to B$ un morphisme d'anneaux. Alors ϕ induit une fonction $Spec(\phi) : Spec(B) \to Spec(A)$ qui à un idéal premier P de B, associe $\phi^{-1}(P)$.

Preuve : En effet il est facile de vérifie que $\phi^{-1}(P)$ est un idéal premier de A. C'est clairement un idéal. Si $\phi(x).\phi(y) = \phi(x.y) \in P$, alors $\phi(x) \in P$ ou $\phi(y) \in P$. Ce qui termine la preuve.

Corollaire : $Spec(\phi)$ est continue pour la topologie de Zariski correspondant au deux espace topologique.

Preuve : C'est une application ouverte. Si $C = O(a)$ où a est un idéal de A, alors $Spec(\phi)(C) = \phi^{-1}(C)$ c'est l'image inverse d'une union, qui est l'union des images inverses, qui sont des idéaux premiers, c'est une union de fermé! donc C'est encore un fermé. Ce qui termine la preuve.

lorsque A est l'anneau $|G|$-cyclotomique?

A sera désormais le sous-anneau de C engendré par les racines G-ièmes de l'unité, i.e :

Définition : Si w_g est une racine $|G|$-ième de l'unité, alors $A = \mathbb{Z}[w_g]$.

Constructions : Notons $Cl(G)$ l'ensemble des classes de conjugaisons de G. On sait que chaque fonctions centrale $f : G \to A$ est totalement déterminée par ses valeur en un représentant de chaque classe, ainsi, l'anneau $A^{Cl(G)}$ s'identifie à l'anneau des fonctions centrales de G à valeurs dans A.
Ainsi, pour f centrale de G dans A, et $c \in Cl(G)$, $f(c)$ est la valeur de f en un élément $g \in c$ (Ce qui est légitime).

Proposition : Les injections $A \to A \otimes R(G) \to A^{Cl(G)}$ définissent les surjections $Spec(A^{Cl(G)}) \to Spec(A \otimes R(G)) \to Spec(A)$.

Preuve : C'est immédiat d'après une proposition précédente.(Voir rappel sur le spectre)
La surjection est clairement le spectre de l'injection..

Proposition : Si M est un idéal maximal de A, alors le corps A/M est fini, sa caractéristique est appelée caractéristique résiduelle de M.

Preuve : C'est un $\mathbb{Z}$-module de type fini, et si M est un idéal maximal de A, soit $M_i = M \cap \mathbb{Z}.w_g^i$, c'est isomorphe à un idéal $N_i = n_i.\mathbb{Z}$ de $\mathbb{Z}$ i.e, $A/M \simeq \mathbb{Z}.w_g/M_1 \times .. \times \mathbb{Z}.w_g^{|G|}/M_{|G|} \simeq \prod_{i=1}^{|G|} \mathbb{Z}/n_i.\mathbb{Z}$. Ce qui termine la preuve.

Corollaire : $Spec(A^{Cl(G)}) \simeq Cl(G) \times Spec(A)$.

Preuve : L'identification est la suivante :
À $(c, P) \in Cl(G) \times Spec(A)$ on associe l'idéal premier (Claire) $\{f \in A^{Cl(G) \mid f(c) \in P}\} = P_c$.
L'image de P_c dans $Spec(A \otimes R(G))$ est l'idéal premier (L'image réciproque de P_c par l'inclusion de $A \otimes R(G)$ dans $A^{Cl(G)}$, voir rappel précédent sur les spectres) $M_{P,c} = P_c \cap (A \otimes R(G))$.

On a donc une classification complète du spectre de $\mathbb{Z}[w_g] \otimes R(G)$:

Proposition : Si :
1/ À toute classe c de $Cl(G)$ on associe, on associe $M_{0,c} = \{f : Cl(G) \to A \mid f(0) \in P\} \cap (A \otimes R(G))$,
et,
2/ À toute classe c formée d'éléments p'-régulier, et à tout idéal maximal P de A de caractéristique résiduelle p, on associe $M_{P,c}$,
Alors on obtient le spectre $Spec(A \otimes R(G))$

Remarque : Comme $Spec(A^{Cl(G)}) \to Spec(A \otimes R(G))$ est surjective, alors tout idéal premier I de $A \otimes R(G)$ est de la forme $M_{P,c}$, et comme $I \cap A = P$, alors I détermine P, ainsi, tout revient à déterminer quand deux classes c_1, c_2 font que $M_{P,c_1} = M_{P,c_2}$. Ainsi il suffit de démonter le lemme suivant :

Lemme :
1/ Si $P = 0$, alors $c_1 = c_2 \Longleftrightarrow M_{0,c_1} = M_{0,c_2}$ (dans ce cas P_c sont les fonctions centrales annulant c)

2/ Si $P \neq 0$, p sa caractéristique résiduelle et c_1', c_2' les p'-éléments des classes c_1, c_2. Alors $c_1' = c_2' \Longleftrightarrow M_{P,c_1} = M_{P,c_2}$.

Preuve :

1/ Supposons que $P = 0$. Si $c_1 \neq c_2$ alors la fonction $f \in A^{Cl(G)}$ qui prend 1 en c_1 et 0 partout, annule c_1 mais pas c_2. Réciproquement, si les annulateurs de c_1 différent de ceux de c_2, alors $c_1 \neq c_2$.

2/ Soit p la caractéristique résiduelle de P. Les deux implications résultent des deux lemmes dans la partie "Construction des caractères".

Remarques :

1/ Pour montrer qu'un idéal de $A \otimes R(G)$ lui est égale, il suffit de montrer qu'il n'est divisible par aucun idéal premier $M_{P,c}$ de $A \otimes R(G)$.

2/ On peut représenter graphiquement $Spec(A \otimes R(G))$ comme une réunion de droites D_c où $c \in Cl(G)$, et chaque D_c est une copie de $Spec(A)$. La règle du jeux est :
a/ étant donné $P \in Spec(P)$, alors D_{c_1} et D_{c_2} s'intersectent au dessus de P si et seulement si $c_1' = c_2'$.
b/ étant donné un nombre premier p, alors D_{c_1} et D_{c_2} s'intersectent au dessus de p ssi il existe un $P \in Spec(A)$ de caractéristique résiduelle p tel que D_{c_1} et D_{c_2} intersectent au dessus de P.

Connexité de Spec(A⊗R(G)) : $Spec(A \otimes R(G))$ est connexe pour la topologie de Zariski.

Preuve : Soit $x \in G$, d'ordre $p_1^{n_1}..p_k^{n_k}$. Comme nous l'avons vu, x se décompose en un produit $x = x_1..x_k$ où chaque x_i est un p_i-élément (d'ordre $p_i^{n_i}$), ainsi, les classes de x et ceux de $x_2..x_k$ ont même composante p_1-régulière, les droites correspondant dans $spec(A \otimes R(G))$ s'intersectent donc, en plus ces droites sont connexes (des copies de $Spec(A)$). On re-étère le procédé jusqu'à la classe unité, et on fini la preuve.

Corollaire : $Spec(R(G))$ est connexe pour la topologie de Zariski.

Preuve : C'est l'image de $Spec(A \otimes R(G))$ par l'application continue $spec \circ i$ où i est l'inclusion. (La continuité a été prouvé dans la partie Rappel de ce chapitre)

Chapter 7

Un peu plus loin (Si on travail sur d'autres corps que C?)

Jusqu'à maintenant on s'est intéressé au corps C des nombres complexes, en particulier, aux corps algébriquement clos et en caractéristiques non divisant l'ordre du groupe G. C'est toujours intéressant d'essayer de généraliser les choses! qu'allons nous trouver si le corps n'est plus algébriquement clos? qu'est-ce qui change et qu'est-ce qui ne change pas?

Ce petit chapitre est surtout une introduction, nous n'allons pas démontrer tout les théorèmes.

7.1 de $R(G)$ à $R_K(G)$

Soit K un corps de caractéristique 0 et $\bar{K}$ une clôture algébrique de K.
Si V est un K-espace vectoriel, on note $V_{\bar{K}} = \bar{K} \bigotimes_K V$ le $\bar{K}$-espace-vectoriel induit de V par extension des scalaires.
Si G est un groupe fini, alors toute K-représentation linéaire (p, V) de G, définie une $\bar{K}$-représentation linéaire $(p_{\bar{K}}, V_{\bar{K}})$ de G. Ainsi, $V_{\bar{K}} = \bar{K}[G] \bigotimes_{K[G]} V$.
À noter que le caractère $X_p = Tr \circ p$ est le même que $X_{p_{\bar{K}}} = Tr \circ p_{\bar{K}}$, c'est une fonction centrale sur G à valeurs dans K.
à partir du maintenant, et pour économiser nos matière grise en écrivant en Latex,

on va écrire $\bar{K} = C$ (Et dans tous les cas, nous se limitons à des sous-corps du corps C des complexes).

Définition : Nous notons $R_K(G)$ le $\mathbb{Z}$-module de type fini engendré par les caractères des représentations irréductibles de G sur K,que nous appelons K-caractères irréductibles de G.

Proposition : $R_K(G)$ est un sous-anneau de l'anneau $R(G) = R_C(G)$.

Preuve : Les caractères des $K[G]$-modules sont des caractères du $C[G]$-module correspondant.

On trouve dès maintenant quelque chose qui ne change pas du passage de $R(G)$ à $R_K(G)$:

Proposition : Soient $(X_1, .., X_h)$ les différents K-caractères irréductibles de G. Alors $(X_1, .., X_h)$ forme une base orthogonale de $R_K(G)$ (Par rapport à la forme bilinéaire habituelle $< | >_G$).

Preuve : C'est claire que $(X_1, .., X_h)$ est une famille engendrante de $R_K(G)$ car toute représentation est semi simple. L'orthogonalité de la famille, et donc la liberté de la famille s'obtient : $< X_i | X_j >_G = dim_K(Hom^G(V_i, V_j))$
$= dim_C(Hom^G(V_{i_C}, V_{j_C}))$ et on a donc ce qu'on veut d'après le chapitre sur le critère de Makey.

Définition (K-Réalisabilité des représentations) : Une C-représentation de G est dite K-réalisable si elle est isomorphe à une représentation de la forme p_C où p est une K-représentation linéaire de G.

Proposition : Une C-représentation de G est K-réalisable si et seulement si son caractère est dans $R_K(G)$.

Preuve :
- Si q est K-réalisable, alors q est isomorphe à une C-représentation de la forme p_C, et on a $Tr \circ q = Tr \circ p_C = Tr \circ p$ et $Tr \circ p \in R_K(G)$.
- Supposons que X dans $R_K(G)$, alors par définition de ce dernier, on a $X = \sum_i n_i.X_i$ et on a que $< X|X_j >_G = \sum_i n_i < X_i|X_j >_G = n_j. < X_j|X_j >_G \ \forall j$, et comme $(< X|X_j >_G, < X_j|X_j >_G) \in \mathbb{N}^2, \forall j$, alors $\forall j, n_j \geq 0$, et donc la représentation V associé à X est isomorphe à la somme directe $V \simeq \bigoplus_i n_i.V_i$ où V_i la représentation irréductible associée à X_i. Ce qui termine la preuve.

D'après la partie 1, le chapitre sur la décomposition canonique, on a l'unicité :

Corollaire : La K-réalisation p_C est unique à isomorphisme près.

Définition : Notons $\bar{R}_K(G)$ le sous-anneau de $R_C(G)$ formé des éléments de $R(G)$ à valeurs dans K.

Remarque : On a clairement que $R_K(G) \subset \bar{R}_K(G)$.

À noter d'abord que toute C-représentation est L-réalisable pour L une extension fini de K, i.e, $R_L(G) = R(G)$ (Celle engendrée par K et les coefficient des représentations matricielles correspondantes), et soit $d = [L : K]$. On a :

Théorème : $d.\bar{R}_K(G) \subset R_K(G)$.

Preuve : Soit V une L-représentation de G, de caractère X. On se restreint à K, et on peut voir V comme un K-espace vectoriel de dimension d plus grand (Car le degré de l'extension d est en particulier la dimension du K-ev L), et on peut voir donc V une K-représentation de G, et le caractère de cette K-représentation est $Tr_{L:K} \circ X$ et donc comme $Tr_{L:K}$ est L-linéaire et à valeurs dans K (d'après la théorie des nombres) et $X \in R_L(G)$ on a alors que $Tr_{L:K} \circ X \in R_K(G)$. Si X est à valeurs dans K (i.e, $X \in \bar{R}_K(G)$), alors $Tr_{L:K} \circ X = X.Tr_{L:K}(1_{C[G]}) = X.d$ et donc $d.X \in R_K(G)$, ce qui termine la preuve.

Corollaire : $|\bar{R}_K(G)/R_K(G)|$ est fini.

Soit maintenant m l'exposant du groupe G (ppcm des ordres de ses éléments). On a vu dans dans la théorie des groupe que m et $|G|$ ont les même facteurs premiers, et en particulier, m divise $|G|$. On a que :

Théorème : Si K contient les racines m-ièmes de l'unité, alors $R_K(G) = R_C(G)$.

Preuve : Comme $X \in R(G)$, alors d'après le corollaire du théorème de Brauer, X est combinaison linéaire entière de caractères monomiaux, i.e, $X = \sum_i n_i.Ind_{H_i}^G(f_i)$ où f_i sont des caractères de degré 1 de sous-groupes H_i de G. Or les f_i sont des racines m-ièmes de l'unité (En effet, $X_i(g^m) = X_i(1) = dim_C V_i = 1$ car monomial), donc $f_i \in R_K(H_i)$, et donc $Ind_{H_i}^G(f_i) \in R_K(G)$, et donc $X \in R_K(G)$. Voila.

On a le résultat immédiat suivant (d'après une proposition précédente):

Corollaire : Si K contient les racines m-ièmes de l'unité. Alors toute C-représentation de G est K-réalisable.

7.2 Une généralisation du théorème d'Artin

Pour finir ce livre, on va annoncer, sans démonstration (La preuve se fait de manière similaire à celle du théorème d'Artin) une généralisation du théorème d'Artin vu précédemment :

Théorème : Soit X l'ensemble des sous-groupes cycliques de G. L'application

$$\mathbb{Q} \otimes Ind : \bigoplus_{H \in X} \mathbb{Q} \otimes R(H) \to \mathbb{Q} \otimes R(G)$$

$$\sum_{H \in X} q_H \otimes f_H \mapsto \sum_{H \in X} q_H \otimes Ind_H^G(f_H)$$

est surjective.

On finit cette partie avec une citation célèbre et inspirante du philosophe Bergson:

"Pour que quelque chose change, il faut que quelque chose ne change pas" Bergson

Bibliography

Le TER se porte principalement sur ces trois livres :

{1} Le livre intitulé : Représentations linéaires des groupes finis, Jean-Pierre Serre.

{2} Le livre intitulé : Algebra, Serge Lang.

{3} Polycopie sur la théorie modulaire des représentations (Olivier Brinon): https://www.math.u-bordeaux.fr/ obrinon /enseignement/modules/modules.pdfpage25

J'ai utilisé plusieurs polycopies de cours, pour modifier, rajouter ou enrichir le contenu :

{4} Polycopie sur Les modules et produits tensoriels (David Harari):

https://webusers.imj-prg.fr/ patrick.polo/M1Galois/ATGch2.pdfpage33

{5} Cours sur la théorie algébrique des nombres (Christian Maire) : https://www.google.com/url?sa=tsource= webrct=jurl=https://members.femto-st.fr/christian-maire/sites/femto-st.fr .christian-maire/files/content /fichiers/ecoles/theoriedesnombres.pdf

Sans oublier bien sur que ce qu'on vient de traiter dans ce TER est accessible au bons élèves de L3 mathématiques ou première année de master, pour cela, nous avons les deux références ci-dessous traitant les notions importantes du licence (L3)

{6} le livre intitulé : L3-Algèbre, Jean-Pierre Marcos.

{7} Le livre intitulé : tout-en-un L3, de Jean-Pierre Ramis.