Chapitre 1

Algèbres semi-simples et théorème de Wedderburn

1.1 semi-simplicité

Définition 1.1.1. Soit R un anneau (unitaire) et $0 \neq_R M$ R-module.

1. $0 \neq_R M$ est simple si les seuls sous-modules de M sont $\{0\}$ et M.
2. ${}_RM$ est semi simple si tout R-sous module N de M est un sommant direct, i.e. s'il existe ${}_RN'$ tel que $N \oplus N' = M$.

Exercices 1.1.2.
1. Montrer qu'un sous module d'un module semi simple est semi simple.
2. Montrer qu'un module quotient d'un module semi simple est semi simple.
3. Trouver tous les $\mathbb{Z}$-modules semi simples.

Lemma 1.1.3. *Tout sous module non nul d'un module semi-simple contient un sous module simple.*

Démonstration. Soit $0 \neq_R N < M$ et M semi-simple. Soit $n \in N \setminus \{0\}$ et $Rn \cong R/L$ où $L = ann_R n$ est un idéal à gauche. Soit I un idéal à gauche maximal contenant L (lemme de Zorn). Alors I/L est un sous-module maximal de R/L. L'isomorphisme $R/L \cong Rn$ applique I/L sur In qui est donc un sous module maximal de Rn. Puisque M est semi-simple $M = In \oplus P$ pour un certain sous-module P. Tout élément $x \in Rn$ s'écrit $x = \alpha n + x'$ où $\alpha \in I, x' \in P$ et $x' = x - \alpha n \in Rn \cap P$. On a donc

$$Rn = In \oplus (P \cap Rn)\,.$$

Puisque In est un sous module maximal de Rn, il est clair que $P \cap Rn$ est un module simple; c'est donc un sous module simple de N.

□

Lemma 1.1.4. *Soit $M = \sum_{i\in I} M_i$ une somme non nécessairement directe de sous modules simples. Alors il existe un sous ensemble $J \subseteq I$ tel que $M = \oplus_{j\in J} M_j$.*

Démonstration. On considère $\mathcal{F} := \{E \subseteq I \mid \sum_{i\in E} M_i \text{ est une somme directe }\}$. Bien sur pour tout $i \in I$,$\{i\} \in \mathcal{F}$. En particulier, $\mathcal{F} \neq \emptyset$. On montre que $\mathcal{F}$ est un inductif : Soit $(I_\lambda)_{\lambda\in\Lambda}$ une chaîne dans $\mathcal{F}$. Montrons que $J = \cup_{\lambda\in\Lambda} I_\lambda$ est aussi un élément de $\mathcal{F}$: si $j_0 \in J$ et $x \in M_{j_0} \cap \sum_{i\in J\setminus\{j_0\}} M_i$, alors $x = x_{i_1} + x_{i_2} + ... + x_{i_l} \in M_{j_0}$ où $i_j \in J \setminus \{j_0\}$ et $x_{i_j} \in M_{i_j}$. Il existe $\mu \in \Lambda$ tel que $\{j_0,i_1,\ldots,i_l\} \subseteq I_\mu$. Mais alors $\sum_{s\in I_\mu} M_s$ est une somme directe donc $x = 0$. On conclut que la somme $\sum_{j\in J} M_j$ est directe et donc que $J \in \mathcal{F}$. Le lemme de Zorn montre qu'il existe $K \subseteq I$ maximal tel que $\sum_{k\in K} M_k$ est directe. Montrons maintenant que pour tout $i \in I, M_i \subseteq \sum_{k\in K} M_k$; M_i étant simple on a $M_i \cap \sum_{k\in K} M_k$ est soit le module nul soit égal à M_i. Mais la première possibilité contredit la maximalité de K... On doit donc avoir $M_i \cap \sum_{k\in K} M_k = M_i$ ce qui montre que $M_i \subseteq \sum_{j\in J} M_j$. Ainsi $M = \sum_{j\in J} M_j = M_i \oplus_{j\in J} M_j$ □

Theorem 1.1.5. *Soit ${}_RM$ un R-module à gauche. Les affiramtions suivantes sont équivalentes :*

1. *M est semi-simple.*
2. *M est la somme d'une famille de sous modules simples.*
3. *M est la somme directe d'une famille de sous modules simples.*

Démonstration. 1) ⇒ 2) Soit M_1 la somme des sous modules simples de M, $M = M_1 \oplus M_2$. Si $M_2 \neq 0$, le lemme 1.1.3 montre M_2 contient un sous module simple ce qui contredit la définition de M_1.

2) ⇒ 3) c'est une conséquence imméditate du lemme 1.1.4.

3) ⇒ 1) Supposons $M = \oplus_{i\in I} M_i$, M_i simple et soit $N < M$ $(N \neq M)$. On considère $\mathcal{F} := \{J \subseteq I \mid \oplus_{j\in J} M_j \cap N = 0\}$. □

On aura besoin du résultat suivant, connu sous le nom de lemme de Schur :

Proposition 1.1.6. *Si ${}_RM$ est un R-module simple, $End_R(M)$ est un corps.*

Démonstration. Il suffit de noter que tout le noyau d'un endomorphisme non nul est un sous module propre de M, puisque M est simple on doit donc avoir un noyau nul. De même puisque l'image d'un endomorphisme non nul est un sous module non nul, on conclut que tout endomorphisme doit être surjectif. □

1.2 Théorème de Wedderburn

On a besoin de quelques résultats relatifs aux homomorphismes entre somme directes de modules. Si R est un anneau, $n \in \mathbb{N}$ et M est un R-module, on

note $M^{(n)}$ le module $M \oplus M \oplus \cdots \oplus M$ où figure n facteurs M.

Lemma 1.2.1. *Soit R un anneau et M,M_1,M_2,...,M_n des R-modules à droite.*

1. $$End_R(M^{(n)}) \cong M_n(End_R(M)) \quad .$$
2. *Si pour $i \neq j, Hom_R(M_i,M_j) = 0$, alors*
$$End_R(\bigoplus_{i=1}^{n} M_i) \cong \prod_{i=1}^{n} End_R(M_i) \quad .$$

Les isomorphismes étant des isomorphismes d'anneaux.

Voici maintenant un résultat fondamental,classique et très facile à démontrer.

Lemma 1.2.2. *(Lemme de Schur)*

Soient M_1 et M_2 des R-modules à gauche simples.

1. *Si $M := M_1 = M_2$, alors $End_R(M)$ est un corps.*
2. *Si $M_1 \ncong M_2$, alors $Hom_R(M_1,M_2) = 0$.*

Démonstration. Pour la preuve il suffit de se rappeler le fait que le noyau et l'image d'un morphisme sont des sous-modules et les seuls sous modules d'un module simple... □

Remarque Si $M_2 \overset{\phi}{\cong} M_1$, alors $Hom_R(M_1,M_2)$ est aussi un corps pour le produit défini par $f.g := f \circ \phi \circ g$...(exercice).

Theorem 1.2.3. *(théorème d'Artin Wedderburn)*

Soit R un anneau, les assertions suivantes sont équivalentes :

1. *${}_RR$ est semi-simple.*
2. *Tout R-module simple à gauche est semi-simple.*
3. *Tout idéal à gauche de R est une facteur direct de R.*
4. *$R \cong \prod_{i=1}^{s} M_{n_i}(K_i)$, où les K_i sont des corps (éventuellemnt non commutatifs) et l'isomorphisme est un isomorphise d'anneaux.*

Démonstration. □

1.3 Théorème de Maschke

Soit k un corps commutatif et G un groupe. On considère les applications de G à coefficients dans k à support fini : $kG := \{f : Glongrightarrowk \,|\, |\{x \in G|f(x) \neq 0\}| < \infty\}$. L'addition et la multipliaction étant définie via ces mêmes opérations sur k. Si $f \in kG$ on écrit généralement f sous la forme $f = \sum_{g \in supp(f)} f(g)g$, i.e. $kG = \{\sum_{finie} \alpha_x x\}$. l'addition de deux éléments

$f = \sum \alpha_x x \quad g = \sum \beta_y y$ de kG écrits sous cette forme se fait alors en sommant les coeffcients correspondant à $sup(f) \cup sup(g)$ la multiplication se fait de la manière suivante (vérifier qu'elle correspond bien à la multiplication ponctuelle des fonctions)

$$f.g = \sum_{x \in supp(f), y \in supp(g))} \alpha_x \beta_y xy = \sum_z (\sum_{(x,y)|xy=z} \alpha_x \beta_y) z$$

On vérifie que kG est une algèbre appelée algèbre du groupe G sur le corps k. Cette algèbre est intimement liée aux représentations du groupe G. Le théorème suivant montre qu'elle estt très souvent semisimple, sa structure sera donc donnée par le théorème d'Artin-Wedderburn.

Theorem 1.3.1. *(théorème de Maschke).*

Soit G ungroupe fini et k un corps commutatif. kG est semisimple si et seulement si chark ne divise pas $|G|$.

Chapitre 2

Représentations des groupes finis

2.1 Définitions et premiers exemples

Définitions 2.1.1. 1. Soit V un k-espace vectoriel de dimension finie. Une représentation linéaire d'un groupe G dans V est la donnée d'un morphisme de groupes :

$$\rho : G \longrightarrow GL(V)\,.$$

2. $dimV$ est appelé le degré de la représentation.
3. Si on fixe une base $\mathcal{B}$ de l'espace vectoriel V de dimension n, on obtient une représentation matricielle de G dans $GL_n(k)$ plus explicitement : si $\rho : G \longrightarrow GL(V)$ est une représentation de G, l'application $\mu : G \longrightarrow GL_n(k) : g \mapsto M_{\mathcal{B}}(\rho(g))$ est la représentation matricielle associée.
4. Une représentation sur un espace vectoriel est dite fidèle si l' application ρ ci-dessus est injective. On dit aussi que G agit fidèlement sur V.

Remarques 2.1.2. La donnée d'une représentation d'un groupe G correspond à la donnée d'une action du groupe G sur V : il suffit de noter $g.v = \rho(g)(v)$. On dit aussi que V est un G-module (voir plus loin pour une explication de cette dénomination). On étudiera uniquement les représentations des groupes finis. On considèrera généralement des représentations sur des $\mathbb{C}$-vectoriels de dimension finies (i.e. $k = \mathbb{C}$, dans la définition ci-dessus).

Exemples 2.1.3. 1. La représentaion triviale d'un groupe G sur un vectoriel V est celle qui correspond à l'application triviale :

$$\rho : G \longrightarrow Gl(V) : g \mapsto Id_V\,.$$

Cette représentation n'est évidemment pas fidèle.

2. La représentation régulière reg d'un groupe fini G : on considère le $\mathbb{C}$-vectoriel $V = \oplus_{g\in G}\mathbb{C}e_g$. L'ensemble $\{e_g \,|\, g \in G\}$ est une bas de V. Si

$g \in G$, la multiplication par g à gauche définit une permutation sur les éléments de G et $reg(g) \in GL_{\mathbb{C}}(V)$ est défini par $reg(g)(e_h) := e_{gh}$ pour $h \in G$. C'est une représentation fidèle de degré $|G|$.

3. La représentation du groupe $\mathcal{S}_3$ via les idométries d'un triangle équilatérale : On dessine un triangle équlatéral et on fixe un repère tel que les coordonnées des sommets A,B,C de ce triangle soient respectivement $(0,1),(-\sqrt{3}/2,-1/2),(\sqrt{3}/2,-1/2)$. On fait correspondre à la permutation (1,2) la symétrie qui fixe A, et à la permutation (1,2,3) la rotation qui applique A sur B. Puisque les permuations (1,2) et (1,2,3) engendrent $\mathcal{S}_3$ on en déduit une représentation ρ de $\mathcal{S}_3$ caractérisée par :

$$\rho((1,2)) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \rho((1,2,3)) = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}$$

Cette représentation est fidèle et de degré 2.

2.2 Représentations équivalentes, représentations irréductibles

Définition 2.2.1. a) Deux représentations $\rho : G \longrightarrow GL(V)$,$\mu : G \longrightarrow GL(W)$ d'un même groupe G sont dites équivalentes s'il existe un isomorphisme $\phi : V \longrightarrow W$ tel que :

$$\forall g \in G \ \mu(g) \circ \phi = \phi \circ \rho(g)$$

b) Une représentation $\rho : G \longrightarrow GL(v)$ est dite irréductible si les seuls sous-spaces de V qui sont stables pour toutes les actions $\rho(g)$ où $g \in G$ sont les sous espaces $\{0\}$ et V lui-même.

c) Soient $\rho : G \longrightarrow GL(V)$,$\mu : G \longrightarrow GL(W)$ deux représentations d'un même groupe G. On peut alors définir

1) la somme de ces deux représentations $\rho \oplus \mu : G \longrightarrow GL(V \oplus W)$ via $(\rho \oplus \mu)(g)(v,w) = (\rho(g)(v),\mu(g)(w))$.
2) Le produit de ces deux représentations $\rho \otimes \mu : G \longrightarrow GL(V \otimes W)$ via $(\rho \otimes \mu)(g)(v \otimes w) = \rho(g)(v) \otimes \mu(g)(w))$.

Exercices 2.2.2. Examiner la signification des définitions a) et c) ci-dessus pour les représentations matricielles associées. Préciser les degrés des représentations somme et produit.

Proposition 2.2.3. *Soient V un $\mathbb{C}$-vectoriel de dimension finie et G un groupe fini. On pose $R := \mathbb{C}G$.*

a) $\rho : G \longrightarrow GL(V)$ est une représentation si et seulement si l'application $R \times V \longrightarrow V : \sum_{g \in G} \alpha_g g \mapsto \sum_{g \in G} \alpha_g \rho(g)(v)$ muni V d'une structure de $R = \mathbb{C}G$-module.

b) Deux représentations sont équivalentes si et seulement si les $\mathbb{C}G$-modules qui leur correspond sont isomorphes.

c) Une représentation $\rho : G \longrightarrow GL(V)$ est irréductible si et seulement si ${}_{kG}V$ est simple.

d) Toute représentation est somme directe de représentations irréductibles.

e) Les R-modules simples à gauche sont isomorphes aux idéaux à gauche minimaux de R.

f) Le nombre de représentations irréductibles non équivalentes est borné par $|G|$.

g) Les représentations irréductibles d'un groupe abélien fini sont toutes de dimension 1.

h) Soient $\rho : G \longrightarrow GL(V)$ une représentation et $g \in G$ alors $\rho(g)$ est diagonalisable. Plus précisément si g est d'ordre r, il existe une base $\mathcal{B}$ de V telle que $[\rho(g)]_{\mathcal{B}} = diag(\omega_1, \ldots, \omega_n)$ où les ω_i sont des racines r^{ime} de 1.

Démonstration. a) Ceci est laissé au lecteur.
b) La relation donnée ci dessus dans la définition de l'équivalence de deux représentations est en réalité exactemlent la relation qui permet de conclure que ϕ est un morphisme de $\mathbb{C}G$-module.
c) Il suffit de constater que les kG-sous modules de V correspondent aux sous espaces vectoriels de V qui sont stables par toutes les applications $\rho(g), g \in G$.
d) Ceci est du au fait que $\mathbb{C}G$ est un anneau semisimple et donc que tout $\mathbb{C}G$-module est semisimple et et donc tout $\mathbb{C}G$-module est somme directe de $\mathbb{C}G$ modules simples.
e) Soit V un $R = \mathbb{C}G$-module simple à gauche. On a $V \cong R/M$ où M est un idéal à gauche maximal de R. Puisque R est semisimple il existe I un idéal à gauche de R tel que $R = M \oplus I$ et on a $V \cong I$. Puisque M est maximal, I est minimal.
f) Les idéaux minimaux de R se coupent trivialement et sont de dimension au moins un comme $\mathbb{C}$-vectoriel. Puisque la dimension de R en tant que $\mathbb{C}$ est égale à $|G|$, on peut conclure.
g) Si G est abélien et $\rho G \longrightarrow GL(V)$ une représentation irréductible de G. Alors V est isomorphe à un idéal à gauche minimal de $R = \mathbb{C}G$. Puisque G est abélien, R est commutatif et Le théorème d'Artin-Wedderburn montre que R est une produit de corps commutatif tous isomorphes à $\mathbb{C}$ (car $\mathbb{C}$ est algébriquement clos). Les idéaux minimaux de $R = \mathbb{C}G$ sont donc de dimension 1...
h) Soit $g \in G$. On doit montrer que $\rho(g)$ est diagonalisable. Soit H le sous groupe de G engendré par g. H est un groupe cyclique, donc commutatif et $\rho/_H$ est une représentation de H. D'après ce qui précède, ${}_{\mathbb{C}H}V$ est isomorphe en tant que $\mathbb{C}H$-module à une somme directe de modules de dimension 1. On

a donc en tant que $\mathbb{C}H$-module à gauche $V = V_1 \oplus \cdots \oplus V_l$ où les V_i sont de dimension 1. Si $\mathcal{B} = \{v_1, \ldots, v_l\}$ est une base adaptée à cette décomposition, on constate que les éléments de $\mathcal{B}$ sont des vecteurs propres de $\rho(g)$. En outre si g est d'ordre r et $\rho(g)(v_i) = \alpha_i v_i$ alors, $\alpha_i^r = 1$. □

2.3 Caractères, caractères irréductibles

Définition 2.3.1. Si $\rho : G \longrightarrow GL(V)$ est une représentation du groupe G, on appelle caractère de ρ l'application $\chi_\rho : G \longrightarrow \mathbb{C} : g \mapsto Tr(\rho(g))$, où Tr dénote la trace (On rappelle que V est un $\mathbb{C}$-vectoriel de dimension finie).

Voici quelques premières propriétés des caractères :

Proposition 2.3.2. *Soit G un groupe fini de cardinal n et $\rho : G \longrightarrow GL(V)$ une représentation de G. (dimension de ${}_{\mathbb{C}}V$ est finie) et $\chi : G \longrightarrow \mathbb{C}$ un caractère.*

1. *χ est indépendant de la base de V utilsée pour calculer les traces des $\rho(g)$, $g \in G$.*
2. *$\chi(1) = dim_{\mathbb{C}} V$.*
3. *$\chi(g)$ est une somme de racines n^{ime} de l'unité.*
4. *$\chi(g^{-1}) = \overline{\chi(g)}$ pour tout $g \in G$.*
5. *$\chi(ghg^{-1}) = \chi(h)$.*

Démonstration. Cette proposition est maintenant facile. Démontrons simplement le point 4). Soit $g \in G$, On note $\mathcal{B}$ une base de V telle que $\rho(g)$ est diagonal, soit $\rho(g) = diag(\lambda_1, \ldots, \lambda_n)$ où les λ_i sont des racines n^{ime} de l'unité. On a alors $\chi_\rho(g^{-1}) = tr(\rho(g^{-1})) = tr((\rho(g))^{-1}) = tr(diag(\lambda_1, \ldots, \lambda_n)^{-1}) = tr(diag(\lambda_1^{-1}, \ldots, \lambda_n^{-1}))$. Puisque les λ_i sont des racines de l'unité on a $\lambda_i^{-1} = \overline{\lambda_i}$ et on conclut alors facilement. □

Exercice

Si pour $i = 1,2$, $\rho_i : G \longrightarrow GL(V_i)$ sont deux représentations d'un même groupe fini G et $f : V_1 \longrightarrow V_2$ est un $\mathbb{C}$-linéaire, montrer que f est un morphisme de $\mathbb{C}G$-modules si et seulement si

$$\forall g \in G \quad f \circ \rho_1(g) = \rho_2(g) \circ f.$$

Lemma 2.3.3. *Soient $\rho_i : G \longrightarrow GL(V_i)$, $i = 1,2$ deux représentations irréductibles d'un même groupe fini G et $f : V_1 \longrightarrow V_2$ un morphisme de $\mathbb{C}G$-modules. Alors*

a) Si ρ_1 n'est pas équivalente à ρ_2 alors $f = 0$.

b) Si $V_1 = V_2$ et $\rho_1 = \rho_2$ alors f est une multiplication par un scalaire.

Démonstration. a) Ceci est clair si on se souvient que V_1 et V_2 sont des $\mathbb{C}G$-modules simples.
b) Si λ est une valeur propre de f ($\mathbb{C}$ est algébriquement clos), alors $f - \lambda id$ est un $\mathbb{C}G$-morphisme qui n'est pas injectif. On doit donc avoir $f - \lambda id = 0$ i.e. $f = \lambda id$. □

Corollary 2.3.4. *Soient $\rho_i : G \longrightarrow GL(V_i)$, $i = 1,2$ deux représentations irréductibles d'un même groupe fini G et $h : V_1 \longrightarrow V_2$ une application $\mathbb{C}$-linéraire. On pose*

$$h^\circ := |G|^{-1} \sum_{t \in G} \rho_2(t)^{-1} \circ h \circ \rho_1(t)$$

Alors

a) h° est un morphisme de $\mathbb{C}G$-modules.

b) $\rho_1 \nsim \rho_2 \Rightarrow h^\circ = 0$.

c) Si $\rho_1 = \rho_2$ et $V_1 = V_2$ alors $h^\circ = n^{-1} Tr(h) id.$, où $n = Dim V_1$.

Démonstration. □

On interprête maintenant le corollaire ci-dessus sous forme matricielle: Supposons $\rho^1(t) = r_{i_1 j_1}(t)$ et $\rho^2(t) = r_{i_2 j_2}(t)$ l'application h étant elle donnée par une matrice $(x_{i_2 j_1})$ et ${}^{h\circ}$ défini par $(x^\circ{}_{i_2 j_2} mmm)$. On a par définition de h° :

$$x^0_{i_2 j_1} = |G|^{-1} \sum_{g, j_1, j_2} r_{i_2 j_2}(g^{-1}) x_{j_2 j_1} r_{j_2 i_1}(g) \,.$$

On distingue alors deux cas comme dans les lemmes qui precedent.

A) Dans le premier cas, le membre de droite s'annule pour toute matrice $(x_{j_2 i_1})$. Ses coefficients sont donc nuls , on en déduit

$$\forall i_1, i_2, j_1, j_2 \quad \sum_{g \in G} r_{i_2 j_2}(g^{-1}) r_{j_2 i_1}(g) = 0 \,.$$

B) Dans le deuxième cas on a $h^\circ = n^{-1} Tr(h) id. = n^{-1} \sum \delta_{j_2 j_1} x_{j_2 j_1}$ et on en déduit

$$|G|^{-1} \sum_{g, j_1, j_2} r_{i_2 j_2}(g^{-1}) x_{j_2 j_1} r_{j_1 i_1}(g) = n^{-1} \sum_{j_1, j_2} \delta_{i_2 i_1} \delta_{j_2 j_1} x_{j_2 j_1} \,.$$

En égalant les coefficients des $x_{j_2 j_1}$ on obtient

$$|G|^{-1} \sum_{g} r_{i_2 j_2}(g^{-1}) r_{j_1 i_1}(g) = n^{-1} \delta_{i_2 i_1} \delta_{j_2 j_1} = \begin{cases} n^{-1} & \text{si } i_1 = i_2 \text{ et } j_1 = j_2, \\ 0 & \text{sinon.} \end{cases}$$

Définition 2.3.5. Soit G un groupe fini et ϕ,ψ deux applications de G dans $\mathbb{C}$.

a) ϕ est dite centrale si elle est constante sur chaque classe de conjugaison de G.

b) on pose

$$(\phi \,|\, \psi) = |G|^{-1} \sum_{g \in G} \phi(g)\overline{\psi(g)} \qquad < \phi,\psi > = |G|^{-1} \sum_{g \in G} \phi(g)\psi(g^{-1}) \,.$$

Bien sur les caractères sont des applications centrales.

Proposition 2.3.6. *Soient ϕ,ψ des applications de G dans $\mathbb{C}$.*

1. *$(\phi \,|\, \psi)$ définit un produit scalaire sur l'espace E des applications de G dans $\mathbb{C}$: il est linéaire en ϕ, semi-linéaire en ψ, et $(\phi \,|\, \psi) > 0$ pour tout ϕ dans E.*
2. *$< \phi,\psi > = |G|^{-1} \sum_{g \in G} \phi(g^{-1})\psi(g)$.*
3. *Si, comme ci-dessus, on désigne par $(r_{i_1 j_1}(g))$ et $(r_{i_2 j_2}(g))$ les matrices correspondant à deux représentations ρ^1 et ρ^2 on a*
   a) $< r_{i_2 j_2}, r_{j_1 i_1} > = 0 \; \forall \, i_1,i_2,j_1,j_2$ si ρ^1 et ρ^2 ne sont pas isomorphes.
   b) $< r_{i_2 j_2}, r_{j_1 i_1} > = n^{-1} \delta_{i_2 i_1} \delta_{j_2 j_1}$ si $V_1 = V_2$ et $\rho_1 = \rho_2$.
4. *Si χ est un caractère de G, $< \phi \,, \chi > = (\phi \,|\, \chi)$.*

Démonstration. Elle est laissée au lecteur. □

2.4 Relations d'orthogonalités et tables des caractères

Theorem 2.4.1. *Soient χ,ψ deux caractères irréductibles distincts.*

1. *$< \chi,\chi > = 1$.*
2. *$< \chi,\psi > = 0$.*

Démonstration. 1) Si $r_{ij}(g)$ est une représentation matricielle (de degré disons n) associée à χ, i.e. $\chi(g) = \sum_{g \in G} r_{ii}(g)$. En utilisant 2.3.6 3 b) on a alors $< \chi,\chi > = \sum_{ij} < r_{ii} r_{jj} > = \sum_{ij} n^{-1} \delta_{ij} = 1$.
2) Si $\chi(g) = \sum_{g \in G} r_{i_1 i_1}(g)$ et $\psi(g) = \sum_{g \in G} r_{i_2 i_2}(g)$. En utilisant 2.3.6 3 a), on a $< \chi,\psi > = 0$. □

Corollary 2.4.2. *Soit $V = \bigoplus_{i=1}^{n} V_i$ la décomposition d'un $\mathbb{C}G$-module en somme directe de modules simples. Si W est un $\mathbb{C}G$-module simple alors, en désignant par χ,ψ sont les caratères associés à V et W respectivement,*

$$|\{i \,|\, V_i \cong W\}| = <\chi,\psi> .$$

Ce nombre est indépendant de la décomposition choisie. Deux représentations ayant même caractère sont isomorphes.

Démonstration. $\chi = \sum \chi_i$ donc $(\chi,\psi) = (\sum \chi_i,\psi) = \sum \delta_{V_i,W}$.

Soient V_1,V_2 deux $\mathbb{C}G$-modules ($dim_{\mathbb{C}}V_1 < \infty$ et $dim_{\mathbb{C}}V_2 < \infty$) de caractères respectifs ψ_1 et ψ_2. On suppose $\psi_1 = \psi_2$ alors pour tout $\mathbb{C}G$-module irréductible W de caractère χ on a $<\psi_1,\chi> = <\psi_2,\chi>$ et donc le nombre de fois où W apprait dans la décomposition de V_1 en somme directe de modules simples est le même que le nombre de fois où W apparait dans la décomposition de V_2. On en déduit $V_1 \cong V_2$. □

On sait que tout $\mathbb{C}G$-module est somme directe de sous-modules simples. On en déduit que tout caractère est somme directe de caractère irréductibles.

Corollary 2.4.3. *Soit χ un caractère et $\chi = \sum n_i\chi_i$ la décomposition de χ en caractères irréductibles. Alors*

1. $(\chi,\chi) = \sum n_i^2$.
2. $(\chi,\chi) = 1$ *si et seulement si χ est irréductible.*

Démonstration. C'est clair. □

Soit $G = C_1 \cup C_2 \cup \cdots \cup C_r$ la décomposition d'un groupe fini G en classe de conjugaison. On pose $C_1 = \{1_G\}$ et, pour $i = 1,\ldots,r$, soit e_i l'élément de $\mathbb{C}G$ égal à la somme des éléments de la classe C_i. Avec ces notations on a

Lemma 2.4.4. *Les éléments $e_1,\ldots,e_r$ forment une base du centre de $\mathbb{C}G$ sur $\mathbb{C}$.*

Démonstration. Il est facile de constater que, pour $i = 1,\ldots,r$, l' élément e_i est central dans $\mathbb{C}G$. D'autre part si un élément $a = \sum_{g\in G} \alpha_g g$ appartient au centre, alors pour tout $h \in G, hah^{-1} = a$, on en conclut que, pour tout $h \in G, \alpha_g = \alpha_{hgh^{-1}}$. Autrement dit les coefficients de a qui correspondent à des élément d'une même classe de conjugaison sont tous égaux. On en conclut aisément que a est une combinaison linéaire des $e_1,\ldots,e_r$. □

Remarquons que l'espace des fonctions centrales de G dans $\mathbb{C}$, noté $\mathcal{C}$, est un $\mathbb{C}$-vectoriel de dimension r (r désigne comme ci-dessus le nombre de classes de conjugaison). En effet si $G = C_1 \cup C_2 \cup \cdots \cup C_r$ est la décomposition de G

en classes de conjugaison, les applications $f_1, \ldots, f_r$ définies par $f_i(g) = 0$ si $g \notin C_i$ et $f_i(g) = 1$ si $g \in C_i$ forment une base de $\mathcal{C}$ sur $\mathbb{C}$.

Proposition 2.4.5. *Le nombre de caractères irréductibles distincts du groupe G est égal au nombre de classes de conjugaison. Les caractères irréductibles forment une base othonormale de l'espace $\mathcal{C}$ des fonctions centrales, muni du produit scalaire introduit ci-dessus.*

Démonstration. Le théorème d'Artin Wedderburn montre que $\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_s}(\mathbb{C})$ et les $\mathbb{C}G$-modules simples à gauche étant isomorphes à des idéaux minimaux à gauche, on constate que le nombre de modules simples à gauche est, à isomorphisme près, égale à s. Puisque les classes d'isomorphismes de modules simples à gauche correspndent aux caractères irréductibles, on conclut que le nombre de caractères irréductibles distincts est égal à s. En outre s est aussi la dimension du centre de $\prod_{i=1}^{s} M_{n_i}(\mathbb{C})$. On conclut que $s = r$, c'est à dire que le nombre de caractères irréductibles est égal au nombre de classes e conjugaison de G. Le reste est clair. □

Soit $G = C_1 \cup \ldots C_s$ la décomposition de G en classe de conjugaison et $g_i \in C_i$ des représentants de ces classes. Soit aussi $\chi_1, \ldots, \chi_s$ les différents caractères irréductibles de G. La table des caractères de G est un tableau

G	$g_1 = 1_G$	g_2	...	g_s
χ_1	1	1	1	1
χ_2	n_2	$\chi_2(g_2)$	$\ldots$	$\chi_2(g_s)$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
χ_s	n_s	$\chi_s(g_2)$	$\ldots$	$\chi_s(g_s)$

χ_1 est le caractère de la représentation triviale. $\chi_i(1) = n_i$ est le degré du caractère (= degré d'une représentation associée). La proposition suivante indique des relations entre les lignes et entre les colonnes de ce tableau.

Proposition 2.4.6. *Avec les notations introduites ci-dessus on a*

a) $\forall l,m \in \{1, \ldots, s\} \quad \sum_{i=1}^{s} \frac{\chi_l(g_i)\overline{\chi_m(g_i)}}{|C_G(g_i)|} = \delta_{lm}$ *(Orthogonalité sur les lignes).*

b) $\forall l,m \in \{1, \ldots, s\} \quad \sum_{i=1}^{s} \chi_i(g_l)\overline{\chi_i(g_m)} = \delta_{lm}|C_G(g_l)|$ *(Orthogonalité sur les colonnes).*

Démonstration. a)

$$\begin{aligned}
\delta_{lm} &= <\chi_l,\chi_m> = |G|^{-1}\sum_{g\in G}\chi_l(g)\overline{\chi_m(g)} \\
&= |G|^{-1}\sum_{i=1}^{s}(\sum_{g\in C_i}\chi_l(g)\overline{\chi_m(g)}) \\
&= |G|^{-1}\sum_{i=1}^{s}|C_i|\chi_l(g_i)\overline{\chi_m(g_i)} \\
&= \sum_{i=1}^{s}(|C_G(g_i)|)^{-1}\chi_l(g_i)\overline{\chi_m(g_i)}
\end{aligned}$$

b) Pour $1 \leq l \leq s$ on note ψ_l la fonction caractéristique de C_l. On a donc $\psi_l(g_i) = \delta_{il}$. Puisque ψ_l est une fonction de classe, elle s'écrit comme combinaison linéaire de $\chi_1,\ldots,\chi_s$. Soit donc $\psi_l = \sum_{j=1}^{s}\lambda_j\chi_j$ et on a :

$$\begin{aligned}
\lambda_i &= <\psi_l,\chi_i> = |G|^{-1}\sum_{g\in G}\psi_l(g)\overline{\chi_i(g)} \\
&= |G|^{-1}\sum_{g\in C_l}\overline{\chi_i(g)} \qquad (\text{or } |C_l| = \frac{|G|}{|C_G(g_l)|}) \\
&= |C_G(g_l)|^{-1}\overline{\chi_i(g_l)}
\end{aligned}$$

On en déduit $\delta_{lm} = \psi_l(g_m) = \sum_{i=1}^{s}\lambda_i\chi_i(g_m) = \sum_{i=1}^{s}\frac{\chi_i(g_m)\overline{\chi_i(g_l)}}{|C_G(g_l)|}$. □

Définition 2.4.7. Soit G un groupe fini. La représentation $\rho_{reg} : G \longrightarrow GL(\mathbb{C}G) : g \mapsto L_g$ où $L_g : \mathbb{C}G \longrightarrow \mathbb{C}G : x \mapsto gx$ est appelée la représentation régulière de G.

Exercice : montrer que ρ_{reg} est effectivement une représentation de G.

Proposition 2.4.8. *1. $\chi_{reg}(1_G) = |G|$ et $\chi_{reg}(g) = 0$ si $g \neq 1_G$.*

2. La multiplicité d'une représentation irréductible π dans la représentation régulière ρ_{reg} est égale au dehré de π.

3. Les degrés $d_1,\ldots,d_s$ des différentes représentations irréductibles de G vérifient $\sum_{i=1}^{s}d_i^2 = |G|$.

Démonstration. 1) Ceci est laissé en exercice.

2) Il suffit de calculer $<\chi_{reg},\chi_\pi> = |G|^{-1}\sum_{g\in G}\chi_{reg}(g)\overline{\chi_\pi(g)}$. En utilisant le point 1) ci-dessus on on conclut $<\chi_{reg},\chi_\pi> = deg\pi$.

3) Le point 2) ci-dessus montre que $\chi_{reg} = \sum_{i=1}^{s}d_i\chi_i$ et donc $|G| = \chi_{reg}(1_G) = \sum_{i=1}^{s}(d_i^2)$. □

Exercice : Utiliser la proposition ci-dessus pour redémontrer qu'un groupe G est abélien si et seulement si les représentations irreductibles de G sont toutes de degré 1.

Définition 2.4.9. Soit A un sous anneau d'un anneau commutatif R. Un élément $x \in R$ est entier sur A s'il est racine d'un polynême unitaire à coefficients dans A. Si x est un nombre réel ou complexe qui est entier sur $\mathbb{Z}$ on dira que est un antier algébrique.

Exemples : Tout entier $d \in \mathbb{Z}$ est entier algébrique ; toute racine n^{ieme} de l'unité dans $\mathbb{C}$ est un entier algébrique.

Proposition 2.4.10. *Soit A un sous anneau d'un anneau commutatif R, et $x \in R$. Les conditions suivantes sont équivalentes :*

1. *x est entier sur A.*
2. *Le A-module $A[x]$ est finiment engendré.*
3. *x appartient à un sous anneau B tel que $A \subseteq B$ et B est finiment engendré comme A-module.*

Démonstration. $(i) \Longrightarrow (ii)$. Si x est une racine d'un polynôme unitaire à copefficients dans A de degré n, alors x^n et toutes les puissances supériures de x peuvent être exprimées omme combinaison linéaire (à coefficients dans A) des éléments $1,x,x^2,\ldots,x^{n-1}$. Donc $\{1,x,x^2,,...,x^{n-1}\}$ engendre A[x] sur A.

$(ii) \Longrightarrow (iii)$. Prendre $B = A[x]$.

$(iii) \Longrightarrow (i)$. Si $a_1,\ldots,a_n$, engendre B sur A, alors xa_i est une combinaison linéaire des a_j, soit $xa_i = \sum_{j=1}^{n} c_{ij}a_j$. Donc si $\overline{a}$ est un vecteur colonne dont les composantes sont les a_i, I est la matrice idenité de taille $n \times n$ et $C = (c_{ij}) \in M_n(A)$, alors $(xI - C)\overline{a} = 0$, et si on premultiplie par la matrice adjointe de $xI - C$, on obtient $det(xI - C)I\overline{a} = 0$, donc $det(xI - C)b = 0$ pour tout $b \in B$. En particulier pour $b = 1$ on obtient $det(XI - C) = 0$ i.e. x est une racine du polynôme $det(XI - C)$ qui unitaire à coefficients dans A. □

Corollary 2.4.11. *Soient $A \subseteq B$ des anneaux commutatifs. Les éléments de B qui sont entiers algébriques sur A forment un sous-anneau de B.*

Exercices

1) Montrer que les seuls rationnels qui sont entiers algébriques sur $\mathbb{Z}$ sont les éléments de $\mathbb{Z}$ eux-mêmes.

2) Soit $\chi : G \longrightarrow \mathbb{C}$ un caractère montrer que, pour tout $g \in G$, $\chi(g)$ est un entier algébrique.

Proposition 2.4.12. *Soit $u = \sum_g u(g)g \in Z(\mathbb{C}G)$ un élément central de $\mathbb{C}G$.*

1. *La fonction $G \longrightarrow \mathbb{C} : g \mapsto u(g)$ est centrale*
2. *Si tous les $u(g)$ sont des entiers algébriques alors l'élment u de l'anneau commutatif $Z(\mathbb{C}G)$ est entier algébrique.*

Démonstration. 1) est laissé au lecteur.

2) Soit $G = C_1 \cup \dots C_s$ la décomposition de G en classe de conjugaison et c_i des représentant des différentes classe de conjugaison. Posons, pour $i = 1, \dots, s$, $e_i = \sum_{g \in C_i} g$. Les éléments e_i forment une base du centre de $\mathbb{C}G$ sur $mathbbC$. On peut donc écrire $u = \sum_{i=1}^{s} u(c_i)e_i$. Les entiers de $Z(\mathbb{C}G)$ forment un sous anneau et les $u(c_i)$ étant entiers par hypothèse, il suffit de montrer que les e_i sont entiers. En fait $R = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_s$ est un sous-anneau du centre de $\mathbb{C}G$ qui est de type fini, tous ses éléments sont donc entiers sur $\mathbb{Z}$. □

Soit $\rho : G \longrightarrow GL(V)$ une représentation irréductible de degré n. Si $u = \sum_g u(g)g \in Z(\mathbb{Z}G)$ un élément central. On définit $\rho_u : V \longrightarrow V$ via $\rho_u = \sum_{g \in G} u(g)\chi_\rho(g) \in \mathbb{C}$. La représentation ρ étant irréductible le lemme de Schur implique que ρ_u est une homothétie de rapport

$$1/n \sum_{g \in G} u(g)\chi_\rho(g) = \frac{|G|}{n}(u, \overline{\chi_\rho}) \, .$$

Proposition 2.4.13. *Soit ρ une représentation irréductible de G de degré n et χ_ρ le carctère asoocié.*

a) L'application

$$\omega_\rho : Z(\mathbb{C}G) \longrightarrow \mathbb{C} : u \mapsto \frac{1}{n} \sum_{g \in G} u(g)\chi_\rho(g)$$

est un morphisme d'algèbres.

b) Si $u = \sum_g u(g)g \in Z(\mathbb{C}G)$ est tel que pour tout $g \in g, u(g)$ est entier algébrique alors

$$\frac{1}{n} \sum_{g \in G} u(g)\chi_\rho(g)$$

est un entier algébrique.

Démonstration. a) Ceci est laissé en exercice.

b) La proposition 2.4.12 montre que u est un entier algébrique du centre de $\mathbb{C}G$. Puisque $\frac{1}{n}\sum_{g \in G} u(g)\chi_\rho(g) = \omega_\rho(u)$ le a) ci-dessus permet de conclure que $\frac{1}{n}\sum_{g \in G} u(g)\chi_\rho(g)$ est aussi un entier algébrique. □

Theorem 2.4.14. *Les degrés des représentations irréductibles de G divisent l'ordre de G.*

Démonstration. Soit ρ une représentation irréductible de caractère χ et de degré n. $u = \sum_{g \in G} \chi(g^{-1})g$ est un élément central (car χ est une fonction centrale, on peut donc écrire u comme combinaison des c_i...) En outre les $\chi(g^{-1})$ sont entiers algébriques. Donc $1/n \sum_{g \in G} \chi(g^{-1})\chi(g) = \frac{|G|}{dimV}(\chi,\chi) = \frac{|G|}{dimV}$ (rappel :χ étant irréductible on a $(\chi,\chi) = 1$) est entier algébrique. Cet élément étant rationnel, on conclut que $\frac{|G|}{dimV} \in \mathbb{Z}$ et donc n divise $|G|$. □

2.5 Un critère de non simplicité dû à Burnside et la résolubilité des groupes d'ordre $p^a q^b$

Voici un petit lemme dont on laisse au lecteur la démonstration.

Lemma 2.5.1. *Soit $\rho : G \longrightarrow GL(V)$ une représentation de caractère χ. Alors :*

a) $\forall g \in G |\chi(g)| \leq \chi(1) = dimV$

b) $\forall g \in G$ ($|\chi(g)| = \chi(1) \Leftrightarrow \rho(g) = \lambda id_V$ pour un certain $\lambda \in \mathbb{C}$).

c) $Ker\rho = \{g \in G \,|\, \chi(g) = \chi(1)\}$.

Lemma 2.5.2. *Soit χ un caractère irréductible du groupe G et g un élément de G.*

1. *$|g^G| \frac{\chi(g)}{\chi(1)}$.*
2. *Si ($|g^G|$,$\chi(1)$) $= 1$ alors soit $\chi(g) = 0$ soit $\rho(g) = \omega id_V$ où ω est une racine de l'unité.*

Démonstration. 1) C'est une conséquence directe de la proposition 2.4.13.

2) D'après Bézout il existe l,$m \in \mathbb{Z}$ telque $l|g^G| + m\chi(1) = 1$. On en déduit que

$$\frac{\chi(g)}{\chi(1)} = l|g^G| \frac{\chi(g)}{\chi(1)} + m\chi(1)$$

est un entier algébrique. Posons $n = \chi(1)$. On a $\chi(g) = \omega_1 + cdots + \omega_n$ où ω_i sont des racines l^{ime} de l'unité. $omega_i \in W := \mathbb{Q}(e^{2i\pi/l})$. Or W est une extension galoisienne de $\mathbb{Q}$ de dimension $\varphi(l)$ On pose $H := gal(W/\mathbb{Q})$ et pour tout $\sigma \in H$on a $\sigma(\chi(g))$ est une somme de n racines l^{ime} de 1, donc $|\sigma(\chi(g))| \leq n$ et $|\sigma(\frac{\chi(g)}{\chi(1)})| \leq 1$. D'autre part $\sigma(\frac{\chi(g)}{\chi(1)})$ est un entier algébrique. Alors $N_{W/\mathbb{Q}}(\frac{\chi(g)}{\chi(1)}) = \prod_{\sigma \in H} \sigma(\frac{\chi(g)}{\chi(1)})$ est un nombre rationel de norme ≤ 1. C'est donc un élément de $\mathbb{Z}$ il est donc égal soit à 0 soit il est de norme 1. Dans le premier cas on conclut que $\chi(g) = 0$ dans le second on on obtient que $|\chi(g)| = n = \chi(1)$ et le lemme ci dessus montre que$\rho(g) = \omega id_V$ où ω est une racine de l'unité. □

Theorem 2.5.3. *Si G est un groupe simple fini alors aucune classe d conjugaison de G ne peut avoir un cardinal de la forme p^a où p est un nombre premeir et $a > 0$.*

Démonstration. Supposons que le groupe fini G soit simple et que $1 \neq g \in G$ soit tel que $|g^G| = p^a$. On sait que lea représentation régulière ρ_{reg} de G se décompose $\rho_{reg} = n_1\chi_1 + \cdots + n_s\chi_s$ où $\chi_1, \ldots, \chi_s$ sont les différents caractères irréductibles de G et $n_1, \ldots, n_s$ sont les degrés correspondants (en particulier

$n_i = \chi_i(1)$). On a donc $o = \chi_{reg}(g) = \sum_{i=1}^{s} n_i\chi_i(g)$. On peut supposer que ρ_1 est le caractère trivial et donc $\chi_1(g) = 1$, ce qui conduit à

$$1 + \sum_{i=2}^{s} n_i\chi_i(g) = 0. \tag{2.5.I}$$

Notons ρ_i des représentations irréductibles associées aux χ_i. Comme G est simple, quel que soit i, $\rho_i(g)$ ne peut être une matrice scalaire (si $\rho_i(g) = \alpha I$ alors $\rho_i^{-1}(\{\alpha^n I \,|\, n \in \mathbb{Z}\})$ est un sous groupe normal de G non réduit à $\{1_G\}$, ce qui contredit le fait que G est simple). Le lemme ci-dessus 2.5.2 montre que si p ne divise pas n_i alors $\chi_i(g) = 0$. Les seules contributions non nulles à la somme 2.5.I sont tels que p divise n_i. D'autre part, les $\chi_i(g)$ sont des entiers algébriques et la somme 2.5.I conduit donc à $1 + pb = 0$ où $b \in \mathbb{C}$ est un entier algébrique. On aurait donc $b = -\frac{1}{p}$ est un entier algébrique ce qui contredit... □

Theorem 2.5.4. *Soit p,q deux nombres premiers et a,b* $\in \mathbb{N}$. *Alors tout groupe d'ordre* $p^a q^b$ *est résoluble.*

2.6 Représentations induites, théorème de réciprocité de Frobenius

Soit $H \subseteq G$ deux groupes et ϕune fonction de classe sur H. On étend ϕ en une fonction notée $\dot{\phi}$ en posant :

$$\dot{\phi}(g) = \begin{cases} \phi(g) & \text{si } g \in H \\ 0 & \text{si } g \notin H \end{cases}$$

On définit la fonction de classe induite ϕ^G sur G via

$$\phi^G(g) = \frac{1}{H} \sum_{x \in G} \dot{\phi}(xgx^{-1}).$$

D'autre part on note la restriction d'une fonction ψ de G à H par ψ_H. Ces deux constructions sont reliées par la relation de réciprocité de Frobenius :

Theorem 2.6.1. *Soit* ϕ *une fonction de classe définie sur un sous groupe H d'un groupe G et soit* ψ *une fonction de classe sur G. Alors*

$$< \psi, \phi^G >_G = < \psi_H, \phi >_H .$$

Démonstration.

$$< \psi, \phi^G > = \frac{1}{|H||G|} \sum_{g,x} \overline{\psi}(g)\dot{\phi}(xgx^{-1}) = \frac{1}{|H||G|} \sum_{x} \sum_{g} \overline{\psi}(x^{-1}gx)\dot{\phi}(g).$$

Puisque $\overline{\psi}$ est une fonction de classe et que $\dot{\phi}$ s'annule sur $G \backslash H$, on obtient:

$$< \psi, \phi^G >= \frac{1}{|H||G|} \sum_x \sum_{h \in H} \overline{\psi}(h)\phi(h) =< \psi_H, \phi > .$$

□

Remarque 2.6.2. Si V est un $\mathbb{C}H$-module associé à ϕ, on peut montrer que le $\mathbb{C}G$-module $V^G = V \bigotimes_{\mathbb{C}H} \mathbb{C}G$ est associé à ϕ^G.

On notera g^G la classe de conjugaison de g dans G et f_g^G la fonction caractéristique de la classe de conjugaison de g.

Corollary 2.6.3. *Si χ est un caractère de G, alors*

$$< \chi, f_g^G >_G = \frac{\chi(g)}{|C_G(g)|}.$$

Démonstration. $< \chi, f_g^G >_G = \frac{1}{|G|} \sum_{x \in G} \chi(x) f_g^G(x) = \frac{1}{G} \sum_{x \in g^G} \chi(x) = \frac{|g^G|}{|G|}\chi(g) = \frac{|G|}{|C_G(g)|} \cdot \frac{1}{|G|}\chi(g) = \frac{1}{|C_G(g)|}\chi(g)$. □

2.7 Théorème de décomposition de Mackey

Chapitre 3

APPLICATIONS

3.1 un théorème d'Hurwitz sur la composition des formes quadratiques

3.2 représentation de la vibration moléculaire

Chapitre 4

ANNEXE

Rappels

1. Ordre : relation réflexive antisymétrique et transitive.
2. Ensembles partiellement ordonnés, ensembles totalement ordonnés.
3. Ensembles bien ordonnés : ensemble ordonné tel que tout sous ensemble non vide admet un plus petit élément.
4. $(E, \leq)$ un ensemble ordonné. Un sous ensemble $S \subseteq E$ est un segment inférieur de E si

$$\forall (e,s) \in E \times S,\ e \leq s \Rightarrow e \in S\,.$$

5. Borne supérieure
6. Chaîne

On énonce ici le lemme de Zorn (LZ), le principe du bon ordre (PBO) et l'axiome du choix (AC). On démontre que

$$LZ \rightarrow PBO \rightarrow AC$$

En fait ces trois enoncés sont équivalents.

AC Etant donné une famille d'ensembles non vides $\{A_i\}_{i \in I}$, il existe une fonction qui associe à chaque ensemble A_i un élément de A_i.

LZ Soit $(A, \leq)$ un ensemble non vide partiellemnt ordonné : Si toute chaîne de A admet une borne supérieure, alors A possède un élément maximal.

PBO Tout ensemble peut-être bien ordonné.

Theorem 4.0.1.

$$LZ \Rightarrow PBO \Rightarrow AC$$

Démonstration. $(LZ) \Rightarrow (PBO)$. Soit A un ensemble. On doit munir A d'un bon ordre. On considère $\mathcal{B} := \{B \subseteq A \,|\, B \text{ est bien ordonne}\}$. On munit $\mathcal{B}$ d'un ordre : pour X,$Y \in \mathcal{B}$ on pose $X \leq Y$ si $X \subseteq Y$ et X est un segment inférieur de Y. On va montrer que $(\mathcal{B}, \leq)$ satisfait les hypothèses du lemme de Zorn.

Soit $\{X_\lambda\}_{\lambda\in\Lambda}$ une chaîne dans $\mathcal{B}$. On pose $X := \bigcup_{\lambda\in\Lambda} X_\lambda$ et on munit X d'un ordre : pour x,$y \in X$ soit $\lambda \in \Lambda$ tel que x,$y \in X_\lambda$. On pose alors $x \leq y$ ssi $x \leq_\lambda y$. Cette définition a un sens : si $\mu \in \Lambda$ est aussi tel que x,$y \in X_\mu$, alors puisque $\{X_\lambda\}_{\lambda\in\Lambda}$ est une chaîne dans X, soit X_λ est un segment inférieur de X_μ soit X_μ est un segment inférieur de X_λ et on a donc aussi dans les deux cas $x \leq_\mu y$.

Montrons que $\leq$ ainsi défini sur X, est un bon ordre (ce qui montrera que $X \in \mathcal{B}$) :

Si $\emptyset \neq Y \subset X$, soit $\lambda \in \Lambda$ tel que $Y \cap X_\lambda \neq \emptyset$. Puisque X_λ est bien ordonné, $Y \cap X_\lambda$ a un plus petit élément disons y. Montrons qu'en fait y est un plus petit élément pour Y. En effet si $y' \in Y \subseteq X$, alors il existe $\mu \in \Lambda$ tel que $y' \in X_\mu$ et

-soit X_λ est un segment inférieur de X_μ dans ce cas on aura $y \in X_\lambda \subset X_\mu$ et $y \leq y'$.

-soit X_μ est un segment inférieur de X_λ et alors $y' \in X_\mu \cap Y \subseteq X_\lambda \cap Y$ et la définition de y montre que $y \leq y'$.

On conclut donc que tout sous ensemble de X a un plus petit élément c'est-à-dire que X est bien ordonné. On a donc $X \in \mathcal{B}$ et chaque X_λ est un segment initial de X. Autrement dit pour l'ordre introduit sur $\mathcal{B}$, X est une borne supérieure des X_λ. Le lemme de Zorn montre qu'il existe donc un élément maximal disons X' dans $\mathcal{B}$. On termine la démonstration en montrant que $X' = A$. Si $a \in A \setminus X'$, on ordonne $X' \cup \{a\}$ en posant $z \leq a$ pour tout $z \in X'$. Ceci fait de $X' \cup \{a\}$ un ensemble bien ordonné inclus à A et X' est alors un segment inférieur de $X' \cup \{a\}$. On a donc, dans $\mathcal{B}$, $X' \leq X' \cup \{a\}$. Ce qui contredit la maximalité de X'.

$PBO \Rightarrow AC$ Soit $\{A_i\}_{i\in I}$ une famille d'ensembles non vides. Puisque les A_i peuvent être bien ordonnés, il suffit de " choisir " dans chaque ensemble A_i le plus élément.

□

Exercice Utiliser le lemme de Zorn pour montrer que

1. Tout vectoriel sur un corps admet une base
2. Tout sous module d'un module finiment engendré est inclus dans un module maximal.