L'objectif des notes suivantes est de donner une idée de l'évolution du cours de *Master 1 Groupes finis et leurs représentations* délivré à la Sorbonne Université et d'expliquer quelques compléments ; elles seront publiées sur

`https://webusers.imj-prg.fr/~joao-pedro.dos-santos/Enseignement.html`

après chaque cours. Ces notes ne se substituent pas à la présence (virtuelle même...), où les idées essentielles seront présentées. Pour les preuves et énoncés détaillés, le lecteur devra consulter la référence [Dat] ou [Malliavin].

Programme approximatif

1) Conventions, notations, prérequis et exemples de base (les groupes cycliques $\mathbb{Z}/n$, diédral $\mathscr{D}_{2n}$, symétriques $\mathscr{S}_n$, linéaires GL_n). Action d'un groupe sur un ensemble. Actions qui préservent une structure. Stabilisateur, orbite, formule de classes.

2) Produit semi-direct.

3) Le groupe $\mathrm{GL}_n(\mathbb{K})$. Le sous-groupe des matrices triangulaires supérieures B (ou "le" Borel). Décomposition $B = U \rtimes T$. Espaces projectifs et drapeaux. Matrices de permutation, transvections et sous-groupes de racines, décomposition de Bruhat. Propriétés basiques des groupes $\mathrm{GL}_n(\mathbb{F}_q)$, $\mathrm{SL}_n(\mathbb{F}_q)$ et $\mathrm{PSL}_n(\mathbb{F}_q)$.

4) p-groupes. Théorèmes de Sylow et ses applications.

5) Groupes nilpotents. Série centrale ascendante. Exemple : U_n. Théorème de Burnside-Wielandt.

6) Représentations linéaires. Représentations de permutation. Sous-représentations, quotients, noyau, représentations simples et semi-simples. Représentations de dim 1. Exemples $\mathscr{S}_3$, $\mathscr{D}_8$, $\mathbb{Z}/n$.

7) Le produit tensoriel. La rep. $V \otimes W$. Exemples et calculs.

8) La "moyenne" et théorème de Maschke. Caractères. Formule "basique" $\dim V^G = \langle 1, \chi \rangle$ et théorème d'orthogonalité.

9) Les égalités
$$|\{\text{classes conjugaison}\}| = |\mathrm{Irr}(G)|$$
et
$$|G| = \sum_{V \in \mathrm{Irr}(G)} \dim(V)^2.$$

10) Table de caractères : plusieurs exemples.

11) Thème avancé variable.

Cours 1

(15 Janvier 2021).

1 Théorie de groupes : prérequis

Notation pour le cours. G est toujours un groupe !

Définition 1. Les définitions suivantes doivent être connues. (Elles ont été rappelées en cours.)

(1) L'ordre d'un élément g. **Notation :** $\mathrm{ord}(g)$.

(2) $H \subset G$ est sous-groupe. **Notation :** $H < G$.

(3) $H \subset G$ est sous-groupe distingué : notation $H \lhd G$.

(4) $f : G \to G'$ est un morphisme ou un isomorphisme.

(5) $\mathrm{Ker}\, f$ et $\mathrm{Im}\, f$ pour un morphisme f.

(6) Si $g \in G$, on note $\langle g \rangle$ le sous-group $\{g^n : n \in \mathbb{Z}\}$. Il est le sous-groupe engendré par g.

Les résultats suivants doivent être connus.

Théorème 2 (Théorème de Lagrange.)**.** *Soit G groupe fini. $H < G$. Alors $|H|$ divise $|G|$.*

Proposition 3 (Sur l'ordre)**.** *Soit $g \in G$.*

1) Si $\mathrm{ord}(g) = m$, alors $\langle g \rangle$ est sous-groupe d'ordre m.

2) Si $g^n = e$, alors m divise n.

3) Si $\mathrm{ord}(g) = m$, alors $\mathrm{ord}(g^n) = \dfrac{m}{\mathrm{pgcd}(m, n)}$.

Théorème 4 (Sous-groupe quotient)**.** *Soit $H \lhd G$. On introduit sur G la relation d'équivalence $g \equiv g' \mod H \iff g^{-1}g' \in H$ et on note G/H l'ensemble quotient. Alors la loi*

$$G/H \times G/H \longrightarrow G/H, \qquad gH \cdot g'H \longmapsto gg'H$$

est bien définie et induit sur G/H une structure de groupe. En plus, la projection $G \to G/H$ naturelle est un morphisme surjectif.

Théorème 5 (Théorème du noyau et de l'image)**.** *Soit $f : G \to G'$ morphisme. Alors $\mathrm{Ker}\, f \lhd G$ et $G/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$.*

Exemple 6. Soit S^1 le cercle dans $\mathbb{C}^*$; il est un sous-groupe. Soit $f : \mathbb{R} \to S^1$ le morphisme de groupes définit par $x \mapsto \cos(2\pi x) + i \sin(2\pi x)$. Alors $\mathbb{R}/\mathbb{Z}$ est isomorphe à S^1 car $\mathrm{Ker}\, f = \mathbb{Z}$ et f est surjectif.

Exemple 7. Soit $\mu_n = \{\zeta \in \mathbb{C}^* : \zeta^n = 1\}$. Alors $f : \mathbb{Z} \to \mu_n$ définie par $k \mapsto e^{2i\pi k/n}$ est un morphisme surjectif de noyau $n\mathbb{Z}$. Par conséquent, $\mathbb{Z}/n \simeq \mu_n$.

2 Exemples fondamentaux

Les exemples suivants doivent être connus.

Exemple 8. Les groupes $\mathbb{Z}/n$ avec l'addition modulaire. Le groups $\mu_n = \{z \in \mathbb{C} \,:\, z^n = 1\}$ avec la multiplication de nombres complexes. On a $\mu_n \simeq \mathbb{Z}/n$.

Exemple 9. Le groupe $\mathscr{S}_n$ des bijections $\{1, \dots, n\} \to \{1, \dots, n\}$ avec la loi de composition $\sigma \circ \tau : k \mapsto \sigma(\tau(k))$. **Révision :** Propriétés basiques de $\mathscr{S}_n$. (Détailles dans 1.2.4 de [Dat].)

Exemple 10 (Les groupes linéaires généraux)**.** Si $\mathbb{K}$ est un corps, alors $\mathrm{GL}_n(\mathbb{K})$ est un groupe avec la multiplication de matrices. Let groupes $\mathrm{GL}_n(\mathbb{F}_p)$ sont une importante source d'exemples.

Exemple 11 (Les groupes diédraux)**.** Soit $n \in \mathbb{N}\backslash 0$. On pose

$$R = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix},$$

c'est la rotation d'un angle $\dfrac{2\pi}{n}$ centrée à l'origine. Soit S la refléxion sur l'axe des x, i.e. $S(x, y) = (x, -y)$. Alors $\{I, R, \dots, R^{n-1}\} \cup \{S, RS, \dots, R^{n-1}S\}$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$, le groupe diédral $\mathscr{S}_{2n}$. (Voir l'exercice 12.) On note que chaque élément de $\mathscr{D}_{2n}$ est écrit comme R^iS^ε où $i \in \{0, \dots, n-1\}$ et $\varepsilon \in \{0, 1\}$.

Exercice 12. Soit R et S comme dans l'Exemple 11.

1) Montrer que pour chaque $k \in \mathbb{Z}$, on a $SR^kS = R^{-k}$. En déduire que $\{I, R, \dots, R^{n-1}\} \cup \{S, RS, \dots, R^{n-1}S\}$ est stable par composition.
2) Montrer que $(R^kS)^2 = I$ pour chaque $k \in \mathbb{Z}$. En déduire que $\{I, R, \dots, R^{n-1}\} \cup \{S, RS, \dots, R^{n-1}S\}$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.
3) Quel est le cardinal de $\mathscr{D}_{2n}$?
4) Montrer que $\langle R\rangle \simeq \mathbb{Z}/n$ et que $\langle R\rangle \lhd \mathscr{D}_{2n}$. Ensuite, montrer que $\mathscr{D}_{2n}/\langle R\rangle \simeq \mathbb{Z}/2$.

Remarques 13. Attention : dans [Dat], $\mathscr{D}_{2n}$ est noté D_n.

3 Actions

Définition 14. Soit X ensemble. *Action* (à gauche !) de G sur X est une fonction :

$$G \times X \longrightarrow X, \qquad (g, x) \longmapsto g * x$$

telle que

$$e * x = x, \quad \text{et} \quad (gh) * x = g * (h * x).$$

La donnée d'une action de G sur X sera notée par $G \circlearrowleft X$ et x sera appelé un G-*ensemble*. Si $G \circlearrowleft X$ et $G \circlearrowleft Y$, alors une fonction $f : X \to Y$ telle que $f(g * x) = g * f(x)$ est dite *équivariante*.

Exercice 15 (Simple mais important)**.** $G \circlearrowleft X$. Alors $T : G \to \mathrm{Bij}(X)$, définie par $T_g = g * x$ est un morphisme de groupes. Réciproquement, si $T : G \to \mathrm{Bij}(X)$ est morphisme, alors $g * x := T(g)(x)$ est action.

Remarques 16 (Vocabulaire). Souvent on dit que $T_g(x) = g * x$ est la *translation* associée à g.

Exemple 17. Le groupe S_n agit de façon évidente sur l'ensemble $\{1, \ldots, n\}$. Le groupe $\mathrm{GL}_n(\mathbb{K})$ agit de façon évidente sur $\mathbb{K}^n$. Le groupe dihédral $\mathscr{D}_{2n}$ agit sur l'ensemble de racines n-èmes de l'unité $\{1, \ldots, \zeta^{n-1}\}$, où $\zeta = e^{2i\pi/n}$.

Exemple 18. Soit $H < G$. On introduit sur G/H l'action $g*(xH) = (gx)H$; elle s'appelle l'action naturelle par translation.

Souvent l'action doit préserver une autre structure de X.

Définition 19. Soit Γ un groupe et $G \times \Gamma \to \Gamma$ une action. On dit que G agit par *homomorphismes* si $g * (\gamma\gamma') = (g * \gamma)(g * \gamma')$ pour tout $g \in G$ et $\gamma, \gamma' \in \Gamma$. Dit autrement, T_g est toujours un morphisme de groupes. Dit autrement, $T : G \to \mathrm{Bij}(X)$ prend ses valeurs dans le sous-groupe des *isomorphismes de groupes*.

Exemple 20. G agit sur lui même par $g * x = gx$. Cette action n'est pas une action par morphismes si $|G| > 1$: en effet, si $g * (xy) = g * x \cdot g * y$, alors $gxy = gxgy$ et donc $x = xg$ et $g = e$. Par contre, si on donne à $\mathbb{K}^n$ la structure évidente de groupe, alors $\mathrm{GL}_n(\mathbb{K})$ agit sur $\mathbb{K}^n$ par morphismes.

Exercice 21. L'action de $\mathscr{D}_{2n}$ sur les racines de l'unité μ_n, est-elle une action par morphismes de groupe ?

Une autre source importante de structures algébriques préservés par une action est la suivante :

Définition 22. Soit X un espace vectoriel sur corps $\mathbb{K}$ et $G \times X \to X$ une action. On dit que cette action est linéaire si T_g est toujours une application linéaire.

Exemple 23. Le groupe dihédral $\mathscr{D}_{2n}$ agit linéairement sur $\mathbb{R}^2$. En effet, $\mathscr{D}_{2n}$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.

Définition 24. $G \circlearrowleft X$. Soit $x \in X$. Le *stabilisateur* de $x \in X$ est $G_x = \{g \in G \,:\, gx = x\}$. (Parfois on écrira Stab_x, ou St_x si la notation G_x s'avère encombrante.)

L'orbite est le sous-ensemble $O(x) = \{gx \,:\, g \in G\}$. Il est clair que G_x est un sous-groupe et que $O(x)$ est stable par G (vérifiez !).

Un $x \in X$ est point fixe si $gx = x$ pour tout $g \in G$; l'ensemble des points fixes est noté X^G.

On dit que l'action est *transitive* si pour un certain $x \in X$ on a $X = O(x)$. Dans ce cas, X est appelé aussi un *espace homogène*, ou un G-ensemble *connexe*.

On dit que l'action est *libre* si pour tout $x \in X$ on a $G_x = \{e\}$.

Un *espace homogène principal*, aussi appelé un *torseur*, est un espace homogène dont l'action est libre.

Voici quelques illustrations de la définition 24.

Exemple 25. Soit X l'ensemble de racines *primitives* n-èmes de l'unité. Le groupe $(\mathbb{Z}/n)^*$ agit sur X par $\overline{k} * z = z^k$. (Le lecteur devra vérifier que cela définit bien une action.) Il n'est pas difficile de voir que cette action est libre et transitive.

Exemple 26. $\mathrm{GL}_2(\mathbb{K}) \circlearrowleft \mathbb{K}^2$ de façon standard. Alors $O(e_1) = \mathbb{K}^2 \backslash \{0\}$ et $O(0) = \{0\}$. L'action est transitive sur $\mathbb{K}^2 \backslash \{0\}$. On note que le stabilisateur de e_1 est le groupe des matrices inversibles de la forme

$$\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}, \qquad d \neq 0.$$

Cours 2

(22 Janvier 2021).

Lemme 27. *$G \circlearrowleft X$. Soit $x \in X$.*

1) La fonction $\varphi_x : gG_x \mapsto gx$ est bien définie et induit une bijection $G/G_x \to O(x)$.

2) On laisse G agir sur G/G_x par translations à gauche (voir Exemple 18), et sur $O(x)$ de façon naturelle. Alors la bijection φ_x est G–équivariante.

3) Les stabilisateurs dans une même orbite sont conjugués : $G_{gx} = gG_xg^{-1}$.

Démonstration. Évidente, mais on l'a fait pour aider à retenir les définitions.

1. Soit $gG_x = g'G_x$. Alors $g' = gs$ où $s \in G_x$. Donc, $g' * x = g * (s * x) = g * x$. Alors la fonction est bien définie. Elle est surjective par définition d'orbite. Elle est injective car $\varphi_x(gG_x) = \varphi_x(g'G_x) \iff g * x = g' * x \iff g^{-1}g' \in G_x \iff gG_x = g'G_x$.

2. $\varphi_x(h \cdot (gG_x)) = \varphi_x(hgG_x) = hg * x = h * (\varphi_x(g))$.

3. Pour le lecteur. □

Corollaire 28. *Soit X un espace homogène, c'est-à-dire, X n'a qu'une seule orbite. Alors il existe une bijection G-équivariante $\varphi : G/H \to X$.*

Démonstration. On choisit $x \in X$ et on applique le Lemme 27. □

Corollaire 29 (Formules de classe)**.** *G et X finis. $G \circlearrowleft X$.*

1. Pour chaque $x \in X$, on a

$$|O(x)| = [G : G_x].$$

2. Soit $O(x_1), \ldots, O(x_q)$ les orbites distinctes. Alors

$$|X| = \sum_{i=1}^{q} |O(x_i)| = \sum_{i=1}^{q} \frac{|G|}{|G_{x_i}|}$$

Démonstration. 1. La fonction $gG_x \mapsto gx$ induit une bijection entre G/G_x et $O(x)$. Donc $|G/G_x| = |O(x)|$. Or, $|G/G_x|$ n'est rien d'autre que $[G : G_x]$.

2. L'ensemble X est réunion disjointe des orbites $O(x_i)$. Donc $|X|$ est $\sum |O(x_i)|$. Chaque $O(x_i)$ possède $[G : G_{x_i}] = |G/G_{x_i}|$ éléments. □

Exemple 30. Soit $\mathbb{K}$ un corps et P l'ensemble des droites vectorielles de $\mathbb{K}^2$. Le groupe $\mathrm{GL}_2(\mathbb{K})$ agit transitivement sur P. Puis, le stabilisateur de la droite $\mathbb{K}\vec{e}_1$ est le sous-groupe des matrices triangulaires supérieures

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \; : \; ad \neq 0 \right\}$$

et obtient une bijection $\mathrm{GL}_2/B \to P$ en utilisant le Lemme 27.

Le cas où $\mathbb{K} = \mathbb{F}_2$ est particulièrement intéressant. On a $P = \{\mathbb{F}_2 e_1, \mathbb{F}_2 e_2, \mathbb{F}_2(e_1 + e_2)\}$ et on arrive à un homomorphisme $\rho : G \to \mathrm{Bij}(P) \simeq \mathscr{S}_3$. Clairement, ρ est injectif car chaque droite n'a que deux éléments. Puis ρ est surjectif car son image est un sous-groupe de $\mathscr{S}_3$ contenant au moins *quatre* éléments, à savoir, les images de id, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Exemple 31. Soit p un premier et G d'ordre p^n. On note Z son centre. On laisse G agir sur G par conjugaison : $g * x = gxg^{-1}$. On note $\mathrm{Cl}(x)$ l'orbite de $x \in G$; c'est la classe de conjugaison de x. Si $|G|/|G_x| > 1$, alors $|G|/|G_x| \equiv 0 \mod p$. Si $|G|/|G_x| = 1$, il suit que $\mathrm{Cl}(x) = \{x\}$ et donc $x \in Z$. La formule de classes implique :

$$|G| \equiv |Z| \mod p.$$

Par conséquent, $|Z| \equiv 0 \mod p$; en particulier $|Z| \neq 1$.

De façon plus générale, soit G encore un groupe d'ordre p et X un G-ensemble fini. Si $|O(x)| > 1$, alors $|O(x)| \equiv 0 \mod p$ et on déduit que

$$|X| \equiv |X^G| \mod p.$$

Ceci fournit un critère très simple pour l'existence de points fixes.

4 Les produits semi-directs

Les produits semi-directs sont une façon de réduire l'étude d'un groupe à l'étude d'un couple de sous-groupes.

Exemple 32. Soit A le groupe des transformations affines de $\mathbb{R} \to \mathbb{R}$, c'est-à-dire, les fonctions ayant la forme $x \mapsto \lambda \cdot x + a$, où $\lambda \in \mathbb{R}^*$ et $a \in \mathbb{R}$. Si $f(x) = \lambda \cdot x + a$ et $g(x) = \mu \cdot x + b$, alors

$$gf(x) = \lambda\mu \cdot x + \mu a + b.$$

Parmi les transformations affines, les translations $t_a : x \mapsto x + a$ et les dilatations $\delta_\lambda : x \mapsto \lambda \cdot x$ sont plus maniables. En fait, $T = \{\text{translations}\}$ et $D = \{\text{dilatations}\}$ sont des sous-groupes de A et tout $f \in A$ s'écrit comme $t_a \delta_\lambda$. (On a $T \simeq \mathbb{R}$ et $D \simeq \mathbb{R}^*$) Par contre, $(t_b \delta_\mu) \circ (t_a \delta_\lambda) \neq (t_a t_b) \circ (\delta_\mu \delta_\lambda)$! La bonne formule vient du fait que $T \lhd A$ parce que

$$\boxed{\delta_\mu t_a \delta_\mu^{-1} = t_{\mu a}}$$

et

$$\begin{aligned}(t_b\delta_\mu)\circ(t_a\delta_\lambda) &= t_b\circ\delta_\mu t_a\delta_\mu^{-1}\circ\delta_\mu\delta_\lambda\\ &= t_b t_{\mu a}\delta_\mu\delta_\lambda.\end{aligned}$$

Définition 33. Soit G un groupe, K et Q des sous-groupes avec $K\lhd G$. On dit que G est le produit semi-direct de K et Q si Chaque élément de G s'écrit de façon *unique* comme produit $k\cdot q$, où $k\in K$ et $k\in K$. On écrit [1] $G = K\rtimes Q$.

Lemme 34. *Soit G un groupe, K et Q des sous-groupes avec $K\lhd G$. Alors :*

1. *L'ensemble $KQ = \{kq\ :\ k\in K,\ q\in Q\}$ est un sous-groupe de G.*
2. *On a $G = K\rtimes Q \Leftrightarrow K\cap Q = \{e\}$ et chaque g s'écrit comme kq, avec $k\in K$ et $q\in Q$.*
3. *Si G est fini, alors $G = K\rtimes Q$ si et seulement si $K\cap Q = \{e\}$ et $|K|\cdot|Q| = |G|$.*

Démonstration. 1) Il suffit de noter que

$$kqk'q' = \underbrace{kqk'q^{-1}}_{\in K}qq' \quad \text{et} \quad (kq)^{-1} = \underbrace{q^{-1}k^{-1}q}_{\in K}q^{-1}.$$

2) "$\Rightarrow$" Soit $g\in K\cap Q$; on l'écrit comme kq où $k\in K$ et $q\in Q$. Or, $g = g\cdot e$ avec $g\in K$ et $e\in Q$. Donc $q = e$. De même, $g = e\cdot g$ avec $e\in K$ et $g\in Q$, et donc $k = e$. Ceci donne $g = e$. Réciproquement, on suppose que $K\cap Q = e$. Soit $kq = k'q'$. Il suit que $k^{-1}k' = q'^{-1}q\in K\cap Q$. Donc $q = q'$ et $k = k'$.

3) On doit montrer que chaque élément de G s'écrit comme produit kq. Or, mais la fonction $K\times Q\to G$ $(k,q)\mapsto kq$ est injective parce que $k_1q_1 = k_2q_2$ implique $k_2^{-1}k_1 = q_2q_1^{-1}$, d'où $k_1 = k_2$ et $q_1 = q_2$. ☐

Exemple 35. Soit $\mathscr{D}_{2n}$ le groupe diédral (Exemple 11). Clairement $\langle R\rangle\lhd\mathscr{D}_{2n}$, et $\mathscr{D}_{2n} = \langle R\rangle\cdot\langle S\rangle$. Puis, comme $\langle R\rangle\cap\langle S\rangle = e$, on voit que $\mathscr{D}_{2n} = \langle R\rangle\rtimes\langle S\rangle$.

Exemple 36. Soit $g\in \mathrm{GL}_2(\mathbb{C})$ et δ tel que $\delta^2 = \det g$. Alors

$$g = \left[\begin{pmatrix}1/\delta & \\ & 1/\delta\end{pmatrix}\cdot g\right]\cdot\begin{pmatrix}\delta & \\ & \delta\end{pmatrix};$$

il suit que $\mathrm{GL}_2(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})\cdot Z$, où Z sont les matrices diagonales. Par contre, GL_2 n'est pas un produit semi-direct de $\mathrm{SL}_2(\mathbb{C})$ et Z parce que $\mathrm{SL}_2(\mathbb{C})\cap Z \neq e$. Pouvez-vous trouver $Q < \mathrm{GL}_2(\mathbb{C})$ tel que $\mathrm{GL}_2(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})\rtimes Q$?

1. Dans les textes plus anciens, on trouve la notation $G = K\cdot Q$; quoique imprécise, cette notation donne la bonne idée derrière le produit semi-direct.

Soit $G = K \rtimes Q$. Pour chaque $q \in Q$, on note $c_q : G \to G$ la conjugaison par q. On a

$$c_q(gh) = c_q(g)c_q(h) \quad \text{et} \quad c_{qq'} = c_q \circ c_{q'}.$$

En particulier, Q agit sur K par des morphisms de groupe et la composition dans G s'écrit à l'aide de cette action comme dans l'exemple, à savoir :

$$\begin{aligned} kqk'q' &= kqk'q^{-1}qq' \\ &= kc_q(k')qq'. \end{aligned}$$

Ceci donne lieu au théorème suivant.

Théorème 37. *Soit K et Q des groupes. On se donne une action de $c : Q \to \mathrm{Aut}(K)$. (C'est-à-dire, Q agit par morphisme de groupes.)*

1. *En munissant $K \times Q$ de la loi*

$$(k, q) \bullet (k', q') = (k \cdot c_q(k'), qq')$$

on obtient un groupe, noté $K \rtimes_c Q$. L'identité de $K \rtimes_c Q$ est (e, e) et $(k, q)^{-1} = (c_{q^{-1}}(k^{-1}), q^{-1})$.

2. *Soit $k \in K$ et $q \in Q$. Alors*

$$(k, e) \bullet (e, q) = (k, q) \quad \text{et} \quad (e, q) \bullet (k, e) \bullet (e, q)^{-1} = (c_q(k), e).$$

3. *Soit $\overline{K} = K \times \{e\}$ et $\overline{Q} = \{e\} \times Q$. Alors $\overline{K}$ et $\overline{Q}$ sont des sous-groupes de $K \rtimes_c Q$ et les fonctions*

$$\begin{aligned} i_K &: K \longrightarrow \overline{K}, \quad k \longmapsto (k, e) \\ i_Q &: Q \longrightarrow \overline{Q}, \quad q \longmapsto (e, q) \end{aligned}$$

sont des isomomorphismes.

4. *Le sous-groupe $\overline{K}$ est distingué et $K \rtimes_c Q$ est produit semi-direct de $\overline{K}$ et $\overline{Q}$.*
5. *La projection $\pi : K \rtimes_c Q \to Q$ est un morphisme de groupes surjectif et $K \times \{e\}$ est son noyau.*

Démonstration. 1 a été faite en cours. Les autres sont des exercices faciles. □

Exemple 38. Soit $\mathscr{D}_{2n}$ le groupe dihédral (voir Exemple 11). Soit $K = \langle R \rangle$ le sous-groupe engendré par la rotation et $Q = \langle S \rangle$ le sous-groupe engendré par la réflexion S. Alors $\mathscr{D}_{2n} = \mathbb{Z}/n \rtimes \mathbb{Z}/2$ où $\mathbb{Z}/2 \to \mathrm{Aut}(\mathbb{Z}/n)$ est déterminé par l'automorphisme $c : \mathbb{Z}/n \to \mathbb{Z}/n$, $c(k) = -k$. En effet,

$$\begin{aligned} SRS^{-1} &= SRS \\ &= R^{-1}. \end{aligned}$$

De plus, on peut même construire un diédral infini : $\mathscr{D}_\infty = \mathbb{Z} \rtimes \mathbb{Z}/2$ où $\mathbb{Z}/2$ agit sur $\mathbb{Z}$ via $k \mapsto -k$.

Cours 3

(05 février 2021).

5 Quelques groupes de matrices

On fixe un corps $\mathbb{K}$ et on écrit GL_n au lieu de $\mathrm{GL}_n(\mathbb{K})$. On étudie quelques actions et sous-groupes fondamentaux de GL_n.

Définition 39. 1. On note $\mathbb{P}^{n-1}$ l'ensemble des droites de $\mathbb{K}^n$ qui passent par l'origine : c'est l'espace projectif. On note que $\mathrm{GL}_n(\mathbb{K}) \circlearrowleft \mathbb{P}^{n-1}$ de façon naturelle $g * D = g(D)$.

2. On note $\mathrm{Gr}_{k,n-1}$ l'ensemble de k-plans de $\mathbb{K}^n$ qui passent par l'origine. C'est la *grassmannienne* des k-plans. On note que $\mathrm{GL}_n(\mathbb{K}) \circlearrowleft \mathrm{Gr}_{k,n-1}$.
3. Un *drapeau* dans $\mathbb{K}^n$ est une famille de sous-espaces vectoriels $0 = F_0 \subset \cdots \subset F_m$, où les inclusions sont strictes. Un drapeau est *complet* si $\dim F_i = i$. L'ensemble des drapeaux complets est noté Drap. On note que $\mathrm{GL}_n(\mathbb{K}) \circlearrowleft \mathrm{Drap}$.

Exemple 40. Soit $C_k = \mathrm{vect}(\vec{e}_1, \dots, \vec{e}_k)$ si $k > 0$ et $C_0 = \{0\}$. Alors $C = C_0 \subset \cdots \subset C_n$ est un drapeau ; qu'on appelera le drapeau *complet canonique*.

Définition 41. On note $B_n = \{(b_{ij}) \in \mathrm{GL}_n \ : \ b_{ij} = 0 \text{ si } i > j\}$. C'est l'ensemble des matrices triangulaires supérieures.

Dans la suite on fixe n et on écrit B au lieu de B_n.

Lemme 42. *Soit C le drapeau canonique de $\mathbb{K}^n$. Alors B est le stabilisateur de C pour l'action naturelle de* GL_n *sur* Drap. *En particulier, B est un sous-groupe.*

Démonstration. On montre $B \subset \mathrm{St}(C)$. Soit $b = (b_{ij}) \in B$. Alors

$$\begin{aligned} be_j &= \sum_{i=1}^{n} b_{ij}\vec{e}_i \\ &= \sum_{i=1}^{j} b_{ij}\vec{e}_i \in C_j. \end{aligned}$$

Par conséquent, $b(C_j) \subset C_j$ et comme la dimension est la même, $b(C_j) = C_j$.

On montre $\mathrm{St}(C) \subset B$. Soit $s \in \mathrm{St}(C)$. Alors $se_j = \sum s_{ij}\vec{e}_i$ appartient à C_j. Donc, $s_{ij} = 0$ si $i > j$. □

On écrit

$$T_n = \left\{ \begin{pmatrix} t_1 & & \\ & \ddots & \\ & & t_n \end{pmatrix} \ : \ t_i \in \mathbb{K}^* \right\}, \quad \text{et} \quad U_n = \{(b_{ij}) \in B_n \ : \ b_{ii} = 1\}.$$

Comme avant, on fixe n et on écrit T et U à la place de T_n et U_n.

Un calcul simple montre que la fonction [2]

$$p : B \longrightarrow T, \quad \begin{pmatrix} b_{11} & * & * \\ & \ddots & * \\ & & b_{nn} \end{pmatrix} \longmapsto \operatorname{diag}(b_{11}, \dots, b_{nn})$$

est un morphisme entre B et T. Son noyau est U, d'où $U \lhd B$.

Proposition 43. *Le groupe B est le produit semi-direct entre U et T.*

Démonstration. On doit montrer que chaque $b = (b_{ij})$ s'écrit de façon unique comme produit ut, où $u \in U$ et $t \in T$ et pour cela on fait appel à $p : B \to T$ décrite avant. Si $b \in B$, alors $u := b(p(b))^{-1}$ est tel que $p(u) = p(b)p(b)^{-1}$, et donc $u \in U$. Puis, $b = b \cdot p(b)$. Pour montrer que la décomposition est unique, on note que $U \cap T = I$. □

Exercice 44. Montrer que $U_2 \simeq (\mathbb{K}, +)$ et que $T_2 \simeq \mathbb{K}^* \times \mathbb{K}^*$. Calculer explicitement l'action de T_2 sur U_2. Est-elle linéaire ?

On étudie maintenant quelques sous-groupes importants de GL_n.

Définition 45. Pour chaque couple $i, j \in \{1, \dots, n\}$ $1 \leqslant i \leqslant j \leqslant n$, on note E_{ij} la matrice

$$(E_{ij})_{k\ell} = \begin{cases} 1, & \text{si } (i,j) = (k,\ell), \\ 0, & \text{autrement.} \end{cases}$$

Si $i \neq j$, on écrit $X_{ij}(\lambda) = I + \lambda E_{ij}$; il s'agit d'une transvection [3].

On note que $E_{ij}(\vec{e}_k) = 0$ si $k \neq j$ et $E_{ij}(\vec{e}_j) = \vec{e}_i$.

Lemme 46. *Soit i, j, k et ℓ des entiers de $\{1, \dots, n\}$. Alors*

$$E_{ij}E_{k\ell} = \begin{cases} E_{i\ell}, & si\ j = k, \\ 0, & autrement. \end{cases}$$

Démonstration. On admet que $j \neq k$. Donc, $E_{ij}E_{k\ell}(\vec{e}_\ell) = E_{ij}(e_k) = 0$. Puis, $E_{k\ell}(\vec{e}_\lambda) = 0$ si $\lambda \neq \ell$. Ensuite, $E_{ij}E_{j\ell}(\vec{e}_\ell) = e_i$ et $E_{ij}E_{j\ell}(\vec{e}_\lambda) = 0$ si $\lambda \neq \ell$. □

Corollaire 47. *Pour chaque $i \neq j$, $X_{ij} : \mathbb{K} \to \mathrm{GL}_n(\mathbb{K})$ est un morphisme.*

Démonstration. Facile étant donnée $E_{ij}E_{ij} = 0$ car $i \neq j$. □

2. Si $c_1, \dots, c_n \in \mathbb{K}$, on note $\operatorname{diag}(c_1, \dots, c_n)$ la matrice qui a des zéros partout, sauf sur la diagonale, et l'entrée (i,i) est c_i.

3. Cette application linéaire laisse inchangé chaque vecteur de $\operatorname{vect}(\vec{e}_1, \dots, \vec{e}_{j-1}, \vec{e}_{j+1}, \dots, \vec{e}_n)$ et si $\vec{v} = \sum v_k \vec{e}_k$, alors $X_{ij}(\lambda)\vec{v} = \vec{v} + \lambda v_j \vec{e}_i$ est une translation de $\vec{v}$ dans la direction de $\vec{e}_i$.

Définition 48. Les sous-groupes $X_{ij}(\mathbb{K})$ seront appelés les sous-groupes de racines.[4]

Tous ceux ayant fait un cours d'algèbre linéaire élémentaire ont rencontré les groupes $X_{ij}(\mathbb{K})$ en faisant échelonnant des matrices. Dans la suite, on écrit $\mathscr{L}_i$ pour la i-ème ligne, et $\mathscr{C}_j$ pour la j-ème colonne.

Lemme 49. *Soit $M \in \mathrm{M}_n(\mathbb{K})$. Alors*

$$\mathscr{C}_k(MX_{ij}(\lambda)) = \begin{cases} \mathscr{C}_k(M) & \text{si } k \neq j, \\ \mathscr{C}_j(M) + \lambda\mathscr{C}_i(M), & \text{si } k = j. \end{cases}$$

De même,

$$\mathscr{L}_k(X_{ij}(\lambda) \cdot M) = \begin{cases} \mathscr{L}_k(M) & \text{si } k \neq i, \\ \mathscr{L}_i(M) + \lambda\mathscr{L}_j(M), & \text{si } k = i. \end{cases}$$

Dit autrement,

$$\begin{array}{ccc} \textit{multiplication à droite} & = & \mathscr{C}_j \to \mathscr{C}_j + \lambda\mathscr{C}_i \\ \textit{par } X_{ij}(\lambda) & & \end{array}$$

$$\begin{array}{ccc} \textit{multiplication à gauche} & = & \mathscr{L}_i \to \mathscr{L}_j + \lambda\mathscr{L}_j \\ \textit{par } X_{ij}(\lambda) & & \end{array}$$

Démonstration. La preuve est très simple, mais on la fera pour retenir les notations. Soit $M_k = M(\vec{e}_k)$ la k-ème colonne de M. La j-ème colonne de $MX_{ij}(\lambda)$ est

$$\begin{aligned} MX_{ij}(\lambda) \cdot \vec{e}_j &= M(\vec{e}_j + \lambda\vec{e}_i) \\ &= M_j + \lambda M_i \\ &= \mathscr{C}_j(M) + \lambda\mathscr{C}_i(M). \end{aligned}$$

Puis, si $k \neq j$, alors

$$MX_{ij}(\lambda)\vec{e}_k = M_k.$$

Pour la deuxième affirmation, on fait appel à la transposée. Clairement, $X_{ij}(\lambda)^t = X_{ji}(\lambda)$. On a

$$\begin{aligned} \mathscr{L}_i(X_{ij}(\lambda) \cdot M) &= \mathscr{C}_i(M^t X_{ji}(\lambda)) \\ &= \mathscr{C}_i(M^t) + \lambda\mathscr{C}_j(M^t) \\ &= \mathscr{L}_i(M) + \lambda\mathscr{L}_j(M). \end{aligned}$$

4. Cette terminologie n'est pas courante en Français, où on dit plutôt "groupe vectoriel associé à la racine."

Puis, si $k \neq i$, alors

$$\begin{aligned}\mathscr{L}_k(X_{ij}(\lambda)\cdot M) &= \mathscr{C}_k(M^t X_{ji}(\lambda))\\ &= \mathscr{C}_k(M^t)\\ &= \mathscr{L}_k(M).\end{aligned}$$

□

Corollaire 50. *Soit $\lambda \neq 0$. Si $A \in \mathrm{GL}_n$ commute avec chaque $X_{ij}(\lambda)$ pour $i \neq j$, alors A est un multiples de l'identité.*

Démonstration. Soit $i \neq j$. On sait que

$$\mathscr{L}_i(X_{ij}(\lambda)A) = \mathscr{L}_i(A) + \lambda\cdot\mathscr{L}_j(A) \quad \text{et} \quad \mathscr{C}_i(AX_{ij}(\lambda)) = \mathscr{C}_i(A).$$

Donc, $(X_{ij}(\lambda)A)_{ii} = a_{ii} + \lambda a_{ji}$ et $(AX_{ij}(\lambda))_{ii} = a_{ii}$. Puisque $\lambda \neq 0$, il suit que $a_{ji} = 0$. Comme i et j sont arbitraires, A est diagonale. Ensuite, comme

$$\mathscr{L}_i(X_{ij}(\lambda)A) = \mathscr{L}_i(A) + \lambda\cdot\mathscr{L}_j(A) \quad \text{et} \quad \mathscr{C}_j(AX_{ij}(\lambda)) = \mathscr{C}_j(A) + \lambda\mathscr{C}_i(A),$$

on déduit que $(X_{ij}(\lambda)A)_{ij} = a_{ij} + \lambda a_{jj}$ tandis que $(AX_{ij}(\lambda))_{ij} = a_{ij} + \lambda a_{ii}$. Par conséquent, $a_{ii} = a_{jj}$. □

Pour énoncer le Corollaire suivant, on se rappelle que $\mu_n(\mathbb{K}) = \{c \in \mathbb{K}^* : c^n = 1\}$.

Corollaire 51. *Le centre de GL_n, respectivement SL_n, est $\mathbb{K}^*\cdot I$, respectivement $\mu_n(\mathbb{K})\cdot I$.*

Démonstration. Soit $X \in Z(\mathrm{GL}_n)$. Alors X commute avec $X_{ij}(1)$ pour tout $i \neq j$ et donc X est un multiple de l'identité.

Si $X \in \mathrm{SL}_n$ commute avec tout élément de SL_n, alors X commute avec chaque $X_{ij}(1) \in \mathrm{SL}_n$. De ce fait, X est aussi un multiple de l'identité. Comme $\det(cI) = c^n$, on voit que $c \in \mu_n$. □

On montre maintenant comment re-construire U à partir des groupes $X_{1,2}(\mathbb{K})$, $X_{13}(\mathbb{K})$, etc. Comme la notation devient légèrement compliqué, on commence avec

Exemple 52. On écrit $X(a) = \begin{pmatrix}1 & a & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$, $Y(b) = \begin{pmatrix}1 & 0 & b\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$ et $Z(c) = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}$. Alors

$$Z(c)Y(b)X(a) = \begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}.$$

En particulier, le groupe U est engendré par $X(\mathbb{K})$, $Y(\mathbb{K})$ et $Z(\mathbb{K})$.

La généralisation est maintenant simple.

Lemme 53. *(a) Soit $i \in \{1, \dots, n-1\}$ fixé. Alors pour tout $u_{i,i+1}, \dots, u_{i,n}$ de $\mathbb{K}$, on a*

$$I + u_{i,i+1}E_{i,i+1} + \cdots + u_{i,n}E_{i,n} = \underbrace{X_{in}(u_{in}) \cdots X_{i,i+1}(u_{i,i+1})}_{n-i}.$$

(Le lecteur devra écrire cette dernière équation en terme de matrices !)

(b) Soit $u = (u_{ij}) \in U$. On pose pour chaque $i \in \{1, \dots, n-1\}$,

$$u_i = X_{in}(u_{in}) \cdots X_{i,i+1}(u_{i,i+1}).$$

Alors

$$u = u_{n-1} \cdots u_1.$$

En particulier, la fonction

$$\mathbb{K}^{n(n-1)/2} \longrightarrow U,$$

$$(u_{ij}) \longmapsto X_{n-1,n}(u_{n-1,n}) \cdots X_{12}(u_{12}) \cdots X_{1n}(u_{1n})$$

est bijective et U est engendré par les sous-groupes $\{X_{ij}(\mathbb{K})\}_{i<j}$.

Démonstration. (a) On montre par récurrence sur $k \in \{i+1, \dots, n\}$ que

$$I + u_{i,i+1}E_{i,i+1} + \cdots + u_{i,k}E_{i,k} = X_{ik}(u_{ik}) \cdots X_{i,i+1}(u_{i,i+1}).$$

Le cas $k = i+1$ n'étant que la définition de $X_{i,i+1}$, on suppose que

$$I + u_{i,i+1}E_{i,i+1} + \cdots + u_{i,k-1}E_{i,k-1} = X_{i,k-1}(u_{i,k-1}) \cdots X_{i,i+1}(u_{i,i+1}).$$

Donc, en utilisant que $E_{ik} \cdot E_{i,j} = 0$ parce que $k > i$, on a

$$\begin{aligned} X_{ik}(u_{ik}) \{X_{i,k-1}(u_{i,k-1}) \cdots X_{i,i+1}(u_{i,i+1})\} &= (I + u_{ik}E_{ik}) \cdot \{I + u_{i,i+1}E_{i,i+1} + \cdots + u_{i,k}E_{i,k-1}\} \\ &= I + u_{i,i+1}E_{i,i+1} + \cdots + u_{i,k}E_{i,k-1} + \\ &+ u_{ik}E_{ik}. \end{aligned}$$

(b) La preuve est similaire à la preuve de (a). $\square$

Exemple 54. Le groupe $U_3(\mathbb{F}_2)$ a cardinal 8 et $R = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ est un élément d'ordre 4 : en effet, $R^2 = X_{13}(1)$ et $X_{13}(1)^2 = X_{13}(2) = I$ (puisque $2 = 0$ en $\mathbb{F}_2$). Soit $S = X_{12}(1)$, qui est d'ordre 2 et n'appartient pas à $\langle R \rangle$ (justifier !). De ce fait, $\langle R \rangle \cap \langle S \rangle = I$. Comme $\langle R \rangle$ est d'indice 2, il est distingué et on déduit que $U_3(\mathbb{F}_2) = \langle R \rangle \rtimes \langle S \rangle$. Un calcul simple montre que $SRS = R^3$, d'où $U_3(\mathbb{F}_2) \simeq \mathscr{D}_8$.

Cours 4

(12 février 2021).

6 La décomposition de Bruhat de GL_n

Définition 55. Soit $\sigma \in \mathscr{S}_n$. On définit $w_\sigma : \mathbb{K}^n \to \mathbb{K}^n$ par $w_\sigma(\vec{e}_j) = \vec{e}_{\sigma(j)}$. Une transformation linéaire de la forme w_σ est dite une matrice de permutation.

Exemple 56. Soit $n = 2$. Alors $\mathscr{S}_2 = \{e, (12)\}$ et w est déterminée par $w_{(12)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Lemme 57. *La fonction $w : \mathscr{S}_n \to \mathrm{GL}_n(\mathbb{K})$ définit un morphisme injectif de groupes.*

Démonstration. On a

$$\begin{aligned} w_\tau \cdot w_\sigma(\vec{e}_j) &= w_\tau(\vec{e}_{\sigma(j)}) \\ &= e_{\tau\sigma(j)} \\ &= w_{\tau\sigma}(\vec{e}_j), \end{aligned}$$

ce qui prouve être w un morphisme. Puis, si w_σ est l'identité, on voit que $w_\sigma(\vec{e}_j) = \vec{e}_j$ et donc $\vec{e}_{\sigma j} = \vec{e}_j$; ceci implique que $\sigma j = j$, et $\sigma = \mathrm{id}$. □

Définition 58. Le sous-groupe $W := w(\mathscr{S}_n) \leqslant \mathrm{GL}_n(\mathbb{K})$ est le **groupe de Weyl** (de $\mathrm{GL}_n(\mathbb{K})$).

Théorème 59. *Pour $w \in W$, on note BwB le sous-ensemble des matrices ayant la forme $b_1 w b_2$, avec b_1 et b_2 dans B. Alors on a la décomposition de Bruhat*[5]

$$\mathrm{GL}_n(\mathbb{K}) = \bigsqcup_{w \in W} BwB.$$

La preuve de *l'existence* de la décomposition de Bruhat fait intervenir l'action de $\mathrm{GL}_n(\mathbb{K})$ sur les drapeaux. On commence par comprendre quelle est la relation entre les drapeaux et les bases ordonnées.

Définition 60. Soit $F = \{0 = F_0 \subset \cdots \subset F_n\}$ un drapeau complet. Une base ordonnée $\boldsymbol{f} = [\vec{f}_1, \ldots, \vec{f}_n]$ est adaptée à F si $\vec{f}_j \in F_j$ pour chaque j. Soit $f \in \mathrm{GL}_n(\mathbb{K})$ et soit $\vec{f}_j = f \cdot \vec{e}_j$. On dira que f est adaptée à F si $[\vec{f}_1, \ldots, \vec{f}_n]$ est adaptée à F.

Lemme 61. *Soient F un drapeau complet et $f \in \mathrm{GL}_n(\mathbb{K})$. On désigne par $\boldsymbol{f}$ la base ordonnée $[\vec{f}_1, \ldots, \vec{f}_n]$, où $\vec{f}_j = f\vec{e}_j$.*

5. Le symbole $\bigsqcup$ signifie “réunion disjointe.”

*1) La base **f** est adaptée à F $\Leftrightarrow$ $\vec{f_j} \in F_j \backslash F_{j-1}$ pour chaque $j = 1, \ldots, n$.*

2) La matrice f est adaptée à F $\Leftrightarrow$ $fC = F$. (Ici, C est le drapeau canonique.)

Démonstration. 1) ($\Rightarrow$) Par définition $f_j \in F_j$. Si $f_j \in F_{j-1}$, alors $\{f_1, \ldots, f_j\}$ est contenu dans F_{j-1}, qui a dimension $j-1$ et $\{f_1, \ldots, f_j\}$ ne peut pas être libre.

($\Leftarrow$) Direct de la définition.

2) ($\Rightarrow$) On a $fC_j \subset F_j$ et comme $\dim fC_j = \dim F_j$, l'égalité est immédiate. ($\Leftarrow$) Si $fC_j \subset F_j$, alors $fe_j \in F_j$. $\square$

Maintenant la décomposition de Bruhat prend une forme plus maniable.

Théorème 62. *Soient F et G deux drapeaux complets. Alors il existe*

1. *une permutation $\sigma \in \mathscr{S}_n$ et*
2. *une base ordonnée $\boldsymbol{f} = [\vec{f_1}, \ldots, \vec{f_n}]$ adaptée à F*

telles que $[\vec{f}_{\sigma 1}, \ldots, \vec{f}_{\sigma n}]$ soit adaptée à G.

<u>L'existence</u> de la décomposition de Bruhat. Soit $g \in \mathrm{GL}_n(\mathbb{K})$ et $G = gC$ le drapeau associé. Soit $\boldsymbol{f} = [\vec{f_1}, \ldots, \vec{f_n}]$ une base ordonnée associée à C et $\sigma \in \mathscr{S}_n$ tels que $[\vec{f}_{\sigma 1}, \ldots, \vec{f}_{\sigma n}]$ soit associée à G (dont l'existence suit du Théorème 62). Soit f la matrice dont la j-ème colonne est $\vec{f_j}$. Il suit que la j-ème colonne de fw_σ est $\vec{f}_{\sigma j}$ et la base ordonnée $[\vec{f}_{\sigma 1}, \ldots, \vec{f}_{\sigma n}]$ est simplement la base associée à fw_σ. Le Lemme 61 montre que $fw_\sigma C = gC$. Par conséquent, $w_\sigma^{-1} f^{-1} g \in \mathrm{St}(C) = B$ et donc $g \in fw_\sigma B$. Or, mais $f \in B$ car $fC = C$. Ceci prouve l'existence de la décomposition. $\square$

Preuve du Théorème 62. On *fixe* $i \in \{1, \ldots, n\}$ et on construit un $\tau_{F,G}(i) \in \{1, \ldots, n\}$.

Il existe un *unique* $j \in \{1, \ldots, n\}$ tel que

$$F_{i-1} + G_{j-1} \neq F_i + G_{j-1} \quad \text{et} \quad F_{i-1} + G_j = F_i + G_j. \tag{*}$$

On arrive à une fonction $\tau_{F,G} : \{1, \ldots, n\} \to \{1, \ldots, n\}$. On affirme que $\tau_{G,F} \circ \tau_{F,G} = \mathrm{id}$. Soit ainsi $\tau_{F,G}(i) = j$, on veut montrer que $\tau_{G,F}(j) = i$, qui se traduit par

$$F_{i-1} + G_{j-1} \neq F_{i-1} + G_j \quad \text{et} \quad F_i + G_{j-1} = F_i + G_j. \tag{**}$$

On considère

$$\begin{tikzcd}
& F_i + G_j \arrow[dl, equal] \arrow[dr, dash] & \\
F_{i-1} + G_j \arrow[dr, dash, "\text{codim} \leqslant 1"'] & & F_i + G_{j-1} \arrow[dl, dash, "\text{codim } 1"] \\
& F_{i-1} + G_{j-1}. &
\end{tikzcd}$$

Il suit que $F_i+G_{j-1} = F_i+G_j$ et que $F_{i-1}+G_{j-1} \neq F_{i-1}+G_j$, et l'affirmation est prouvée.

On construit maintenant la base $\boldsymbol{f}$. Pour simplifier la notation, on écrit τ au lieu de $\tau_{F,G}$. Le fait que

$$\begin{aligned}\dim F_i \cap G_{\tau i} &= \dim F_i + \dim G_{\tau i} - \dim(F_i + G_{\tau i})\\ &= 1 + \dim F_{i-1} + \dim G_{\tau i} - \dim(F_{i-1} + G_{\tau i})\\ &= 1 + \dim(F_{i-1} \cap G_{\tau i}),\end{aligned}$$

donne l'existence d'un

$$\vec{f_i} \in F_i \cap G_{\tau i} \smallsetminus F_{i-1};$$

il suit que $[\vec{f_1}, \ldots, \vec{f_n}]$ est une base ordonnée adaptée à F. Puis, si $\sigma = \tau^{-1}$, alors $f_{\sigma i} \in G_i$. De ce fait, $[\vec{f}_{\sigma 1}, \ldots, \vec{f}_{\sigma n}]$ est base ordonnée adaptée à G. □

Corollaire 63. GL_n *est engendré par les groupes* $\{X_{ij}(\mathbb{K}) \,:\, i \neq j\}$ *et* T_n.

Démonstration. Voici les grandes lignes de la preuve : Soit $G < \mathrm{GL}_n$ un sous-groupe contenant T_n et les groupes de racines. Donc G contient B_n. On doit vérifier maintenant que $W < G$. Il suffit de montrer que $w_{(ij)} \in G$ pour chaque couple $i \neq j$. Or,

$$\begin{aligned}X_{ji}(1)X_{ij}(-1)X_{ji}(1)(\vec{e}_i) &= \vec{e}_j\\ X_{ji}(1)X_{ij}(-1)X_{ji}(1)(\vec{e}_j) &= -\vec{e}_i\\ X_{ji}(1)X_{ij}(-1)X_{ji}(1)(\vec{e}_k) &= \vec{e}_k.\end{aligned}$$

Donc,

$$\begin{aligned}w_{(ij)}X_{ji}(1)X_{ij}(-1)X_{ji}(1)(\vec{e}_i) &= \vec{e}_i\\ w_{(ij)}X_{ji}(1)X_{ij}(-1)X_{ji}(1)(\vec{e}_j) &= -\vec{e}_j\\ w_{(ij)}X_{ji}(1)X_{ij}(-1)X_{ji}(1)(\vec{e}_k) &= \vec{e}_k.\end{aligned}$$

Ceci signifie que $w_{(ij)}X_{ji}(1)X_{ij}(-1)X_{ji}(1)$ est diagonale. □

On montre maintenant que la décomposition de Bruhat est unique, c'est-à-dire, que la réunion dans le Théorème 59 est en effet unique. Tout dépend du calcul suivant :

Exercice 64. Soit $A \in \mathrm{Mat}_n(\mathbb{K})$ et $\sigma \in S_n$. Alors

$$\mathscr{C}_j(A \cdot w_\sigma) = \mathscr{C}_{\sigma(j)}A, \quad \text{et} \quad \mathscr{L}_i(w_\sigma^{-1} \cdot A) = \mathscr{L}_{\sigma(i)}A.$$

Lemme 65. *Soit v et w dans W et β dans B. Si $w^{-1}\beta v$ appartient à B alors $v = w$. En particulier, si $BvB \cap BwB \neq \varnothing$, alors $v = w$.*

Démonstration. Or, un calcul direct montre que

$$(w^{-1}X)_{ij} = x_{w(i),j}, \quad \text{et} \quad (Xv)_{ij} = x_{i,v(j)}.$$

Donc,

$$(w^{-1}\beta v)_{ij} = \beta_{w(i),v(j)}.$$

Par conséquent, $\beta_{w(i),v(i)}$ n'est jamais nul car $(w^{-1}\beta v)_{ii} \neq 0$. Comme $\beta \in B$, il suit que $w(i) \leqslant v(i)$ pour chaque i. En faisant l'argument avec l'inverse de $w^{-1}\beta v$, qui est $v^{-1}\beta^{-1}w$, on voit que $v(i) \leqslant w(i)$, et donc $v = w$.

Pour démontrer la dernière affirmation, on suppose que $b_1 v b_2 = c_1 w c_2$, où b_1, b_2, c_1 et c_2 appartiennent à B. Donc, $w^{-1}(c_1^{-1}b_1)v = c_2 b_2^{-1}$ et la première partie de la preuve montre que $w = v$. □

Quelques propriété des groupes $\mathrm{GL}_n(\mathbb{F}_q)$, $\mathrm{SL}_n(\mathbb{F}_q)$, etc

On fixe un corps fini $\mathbb{F}_q$ avec q éléments.

Lemme 66. *Les égalités suivantes sont vraies :*

1. $|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) = q^{\frac{n(n-1)}{2}}(q-1)\cdots(q^n-1)$.
2. $|U(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}}$ *et* $T(\mathbb{F}_q) = (q-1)^n$.
3. $|B(\mathbb{F}_q)| = (q-1)^n q^{\frac{n(n-1)}{2}}$.

Démonstration. 1. La formule est évidemment vraie pour $n = 1$. On fait une récurrence. On laisse $\mathrm{GL}_n(\mathbb{F}_q) \circlearrowleft \mathbb{F}_q^n$. Soit

$$H = \left\{ \begin{pmatrix} 1 & a_1 & \cdots & a_{n-1} \\ 0 & & & \\ \vdots & & \mathrm{GL}_{n-1} & \\ 0 & & & \end{pmatrix} \right\}$$

le stabilisateur de e_1. On a $q^n - 1 = |\mathbb{F}_q^n \backslash \{0\}| = [\mathrm{GL}_n(\mathbb{F}_q) : H]$. Clairement,

$$\begin{aligned} |H| &= |\mathrm{GL}_{n-1}| \cdot q^{n-1} \\ &= q^{n-1} \cdot \underbrace{(q^{n-1} - 1) \cdots (q^{n-1} - q^{n-2})}_{n-1} \\ &= (q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}). \end{aligned}$$

Donc $|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n - 1) \cdot |H|$ donne la formule souhaitée. Puis,

$$\begin{aligned} (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) &= (q^n - 1)q(q^{n-1} - 1)q^2(q^{n-2} - 1) \cdots q^{n-1}(q - 1) \\ &= q^{(n-1)n/2}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1). \end{aligned}$$

2. Faciles.
3. Suit du fait que en tant qu'ensembles, $B = U \times T$. □

Remarques 67. Le calcul de $|\mathrm{GL}_n(\mathbb{F}_q)|$ se fait également de la façon suivante. Pour choisir la première colonne X_1 d'une matrice $X \in \mathrm{GL}_n(\mathbb{F}_q)$, on a $|\mathbb{F}_q^n \backslash \{0\}| = q^n - 1$ choix. La deuxième colonne, X_2, appartient à $\mathbb{F}_q^n \backslash \mathbb{F}_q X_1$, qui est un ensemble de $q^n - q$ éléments. La troisième doit appartenir à $\mathbb{F}_q^n \backslash \mathbb{F}_q X_1 + \mathbb{F}_q X_2$, qui a $q^n - q^2$ éléments, etc. Donc, $|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$.

Corollaire 68. [6] $|\mathrm{SL}_n(\mathbb{F}_q)| = q^{n(n-1)/2}(q^2 - 1) \cdots (q^n - 1)$.

Démonstration. On considère le morphisme $\det : \mathrm{GL}_n(\mathbb{F}_q) \to \mathbb{F}_q^*$. Il est surjectiv. Donc, $|\mathrm{GL}_n(\mathbb{F}_q)|/|\mathrm{SL}_n(\mathbb{F}_q)| = q - 1$. □

7 p-groupes et Théorèmes de Sylow

On peut utiliser la théorie des groupes linéaires pour prouver élégamment les théorèmes de Sylow.

Définition 69. On dit que G est un p-groupe si $|G|$ est une puissance de p. On dit qu'un $P < G$ est un p-sous-groupe de Sylow, ou p-Sylow, si p divise $|G|$, si P est un p-groupe, et si $|G|/|P|$ est premier à p.

Exemple 70. D'après le Lemme 66, $U_n(\mathbb{F}_p) < \mathrm{GL}_n(\mathbb{F}_p)$ est un p-Sylow. En fait, si $q = p^e$, alors $U_n(\mathbb{F}_q)$ est un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_q)$.

6. Cet exemple n'a pas été traité en cours.

Cours 5

(19 Février 2021).

On suppose que

$$\boxed{G \text{ a cardinal } p^r m \text{ où } m \not\equiv 0 \mod p.}$$

Lemme 71. *Soit X un G-ensemble fini. Si $|X|$ est premier à p, alors il existe une orbite dont le cardinal est premier à p.*

Démonstration. Soient $X_1, \ldots, X_m$ les orbites distinctes. On suppose que $|X_i| \equiv 0 \mod p$ pour tout i. Alors $|X| = \sum_i |X_i| \equiv 0 \mod p$, absurde. $\square$

Corollaire 72. *On suppose que G est sous-groupe d'un groupe fini $\overline{G}$. Si $\overline{P} < \overline{G}$ est un p-Sylow, alors pour un certain $\overline{g} \in \overline{G}$, $\overline{g}\,\overline{P}\,\overline{g}^{-1} \cap G$ est p-Sylow.*

Démonstration. G agit sur $\overline{G}/\overline{P}$ par translation : $g * \overline{g}\overline{P} = g\overline{g}\overline{P}$. Clairement, $\mathrm{St}(\overline{g}\overline{P}) = \overline{g}\,\overline{P}\,\overline{g}^{-1} \cap G$. Si $G * (\overline{g}\overline{P})$ est une orbite dont le cardinal, qui est $|G|/|\mathrm{St}(\overline{g}\overline{P})|$, est premier à p, alors $\overline{g}\,\overline{P}\,\overline{g}^{-1} \cap G$ est un p-Sylow. $\square$

On continue la discussion sur les sous-groupes de Sylow. On suppose que

$$\boxed{G \text{ a cardinal } p^r m \text{ où } m \not\equiv 0 \mod p.}$$

Théorème 73 (Les théorèmes de Sylow). *Les affirmations suivantes sont vraies.*

i) Le groupe G possède un p-Sylow.

ii) Deux p-Sylows sont toujours conjugués.

iii) Si $H < G$ est un p-groupe, alors H est contenu dans un p-Sylow.

iv) Si n_p note le nombre de p-Sylows de G, alors $n_p | m$

v) Si n_p est comme avant, alors $n_p \equiv 1 \mod p$.

Démonstration. (i) Tout groupe est sous-groupe d'un $\mathscr{S}_n$, et $\mathscr{S}_n$ est isomorphe au sous-groupe de Weyl de $\mathrm{GL}_n(\mathbb{F}_p)$. On applique ainsi le Corollaire 72 avec $\overline{G} = \mathrm{GL}_n(\mathbb{F}_p)$ et $\overline{P} = U_n(\mathbb{F}_p)$.
(ii) Soient P et Q des p-Sylows. Par le Corollaire 72, il existe ainsi un $g \in G$ tel que $gPg^{-1} \cap Q$ est un p-Sylow de Q, donc $gPg^{-1} = Q$.
(iii) Même argument que pour (ii).
(iv) Soit X l'ensemble des p-Sylows de G sur lequel G agit par conjugaison. D'après (ii), si $P \in X$, alors $X = G * P$ et $\mathrm{St}_P = N_G(P)$, le normalisateur de P. Donc,

$$|X| = [G : N_G(P)] = \frac{[G : P]}{[N_G(P) : P]} = \frac{m}{[N_G(P) : P]},$$

et $|X|$ divise m.
(v) On conserve les notations de l'item précédent. Soit $P \in X$ un p-Sylow ; on laisse P agir sur X. Clairement $O(P) = \{P\}$. Ensuite, soit $P' \neq P$. On sait que $|O(P')|$ est diviseur de $|P|$, soit $|O(P')| \equiv 0 \mod p$, soit $|O(P') = 1$. Si $|O(P')| = 1$ alors $P \subset N_G(P')$. Comme P' est l'unique p-Sylow de $N_G(P')$, ceci montre que $P = P'$, une contradiction. Donc $|O(P')| \equiv 0 \mod p$. La conclusion suit de la formule $|X| = |O(P)| + \sum_{P' \neq P} |O(P')| = 1 + \text{multiple } p$. □

8 Groupes nilpotents

Comme d'habitude, G note un groupe.

Définition 74 (Groupe des commutateurs)**.**
1. Si h et k appartiennent à G, on écrit $[h,k] = hkh^{-1}k^{-1}$. (Attention : Dans [Dat] on trouve la notation $[h,k] = h^{-1}k^{-1}hk$.)
2. Si H et K sont des sous-groupes de G, note $[H,K]$ le sous-groupe de G engendré par l'ensemble $\{[h,k] \,:\, h \in H,\, k \in K\}$.

Définition 75 (La série centrale descendente)**.** On pose $C^0G = G$ et $C^{k+1}G = [G, C^kG]$. On dit que G est nilpotent si $C^kG = e$ pour un certain k. Le plus petit k tel que $C^kG = e$ est appelé la classe de nilpotence de G. (Assez souvent dans la littérature on trouve une définition décalée $C^1 = G$.)

Exemple 76. Classe de nilpotence 0 $\Leftrightarrow$ trivial. Classe 1 $\Leftrightarrow$ abélien.

Exemple 77. Étudions la nilpotence des groupes $\mathscr{D}_{2n}$. On a $[R^i, R^j] = I$,

$$\begin{aligned}[R^iS, R^j] &= R^iSR^jSR^{-i}R^{-j} \\ &= R^iR^{-j}R^{-i-j} \\ &= R^{-2j},\end{aligned}$$

et

$$\begin{aligned}[R^iS, R^jS] &= R^iSR^jSSR^{-i}SR^{-j} \\ &= R^{i-j}R^{i-j} \\ &= R^{2(i-j)}.\end{aligned}$$

D'où, $[R^j, R^iS] = R^{2j}$, et on déduit $C^1(\mathscr{D}_{2n}) = \langle R^2 \rangle$. De même, $[R^iS, R^{2j}] = R^{-4j}$ et $[R^i, R^{2j}] = I$ montre que $C^2(\mathscr{D}_{2n}) = \langle R^4 \rangle$, et en général on a $C^k(\mathscr{D}_{2n}) = \langle R^{2^k} \rangle$. Or,

$$\begin{aligned}|\langle R^{2^k} \rangle| &= \mathrm{ord}(R^{2^k}) \\ &= \frac{n}{\mathrm{pgcd}(n, 2^k)}.\end{aligned}$$

Il suit que si n n'est pas une puissance de 2, alors $\mathrm{pgcd}(n, 2^k) \neq n$ et $\mathscr{D}_{2n}$ n'est pas nilpotent. Par contre, si $n = 2^k$, alors $\mathscr{D}_{2n}$ est nilpotent.

Exemple 78. Une autre classe importante d'exemples de groupes nilpotents sont les groupes $U_n(\mathbb{K})$; la vérification de ce fait est l'objet des lignes suivantes. Pour simplifier la notation, on écrira $U = U_n(\mathbb{K})$.

Soit N le sous-espace vectoriel de $\mathrm{M}_n(\mathbb{K})$ définit par

$$N = \{x \in \mathrm{M}_n(\mathbb{K}) \,:\, x_{ij} = 0 \text{ si } j - i \leqslant 0\}.$$

Dit autrement, N est l'ensemble des matrices triangulaires supérieures dont la diagonal est nulle et de ce fait, pour chaque $u \in U$, l'on a $u - I \in N$. Or, en écrivant

$$C_j = \begin{cases} \mathrm{vect}\{\vec{e}_1, \dots, \vec{e}_j\} & \text{si } j > 0 \\ \{0\} & \text{si } j \leqslant 0, \end{cases}$$

on déduit que

$$N = \{x \in \mathrm{M}_n(\mathbb{K}) \,:\, \forall j,\ xC_j \subset C_{j-1}\}$$

De façon analogue, on introduit, pour chaque $p \geqslant 0$, le sous-espace

$$N^p = \{x \in \mathrm{M}_n(\mathbb{K}) \,:\, xC_j \subset C_{j-1-p}\}$$

Par exemple, si $n = 4$ alors

$$N^1 = \left\{ \begin{pmatrix} 0 & 0 & a & b \\ 0 & 0 & 0 & c \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \,:\, a, b, c \in \mathbb{K} \right\}, \quad N^2 = \left\{ \begin{pmatrix} 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \,:\, b \in \mathbb{K} \right\}.$$

En particulier, $N^0 = N$ et $N^{n-1} = 0$. De plus, les affirmations suivantes sont vraies (et leur démonstration est simple) :

(1) Pour chaque p et q, on a $N^p \cdot N^q \subset N^{p+q+1}$.

(2) Si $x \in N^0 = N$, alors $(I - x)^{-1} = I + x + \cdots x^n$.

(3) Si $u \in U$ et $x \in N^p$, alors xu et ux appartiennent à N^p.

Ces informations permettent maintenant de montrer que U est nilpotent de classe $\leqslant n - 1$. On écrit

$$U^p = I + N^p$$

de tel forme que $U^0 = U$. Pour $x \in N^p$ et $y \in N^q$, l'on a

$$\begin{aligned}
[I + x, I + y] &= (I + \underbrace{x + y + xy}_{u})(I + \underbrace{x + y + yx}_{v})^{-1} \\
&= (I + u)(I - v + v^2 - \cdots) \\
&= I - v + v^2 - \cdots + u(I - v + v^2 - \cdots) \\
&= I - v \cdot (I - v + v^2 - \cdots) + u \cdot (I - v + v^2 - \cdots) \\
&= I + (u - v) \cdot (I - v + v^2 - \cdots) \\
&= I + (xy - yx) \cdot (I - v + v^2 - \cdots) \\
&= I + \text{élément de } N^{p+q+1}.
\end{aligned}$$

Il suit que

$$[U^p, U^q] \subset U^{p+q+1}.$$

En particulier,

$$\begin{aligned}
C^1U &= [U^0, U^0] \subset U^1, \\
C^2U &= [C^1U^0, U^0] \subset U^2 \\
&\vdots \subset \vdots \\
C^pU &\subset U^p,
\end{aligned}$$

et $C^{n-1}U \subset U^{n-1} = \{I\}$.

En fait, la classe de nilpotence de U est exactement $n-1$, ce que se voit par l'argument suivant. Si $n = 2$, alors $U \simeq \mathbb{K}$ et la classe de nilpotence est 1, puisque U est abélien. On suppose ainsi $n \geqslant 3$. Un calcul direct montre que

$$[X_{ij}(\lambda)\,,\, X_{jk}(\mu)] = X_{ik}(\lambda\mu) \quad \text{pourvu que } i, j \text{ et } k \text{ soient distincts.}$$

D'où

$$\begin{aligned}
[X_{12}(1)\,,\, X_{23}(1)] &= X_{13}(1) \in C^1U \\
[X_{13}(1)\,,\, X_{34}(1)] &= X_{14}(1) \in C^2U \\
&\vdots = \vdots \\
[X_{1,n-1}(1)\,,\, X_{n-1,n}(1)] &= X_{1n}(1) \in C^{n-2}U
\end{aligned}$$

et $C^{n-2}U \neq \{I\}$.

Voici quelques propriétés structurelles des nilpotents.

Lemme 79. *1) G nilpotent $\Rightarrow Z(G) \neq 1$.*

2) Un sous-groupe ou un quotient d'un nilpotent est nilpotent.

3) Soit $\pi : G \to Q$ *un morphisme surjectif tel que* $\mathrm{Ker}(\pi)$ *est contenu dans* $Z(G)$. *Si* Q *est nilpotent de classe* $\leqslant s$, *alors* G *est nilpotent de classe* $\leqslant 1 + s$.

Démonstration. 1) Soit n la classe de nilpotence : $[C^n, G] = 1$. Alors $C^{n-1}G \neq 1$ et $C^{n-1}G$ est dans le centre.

2) Simple.

3) On voit facilement que $\pi(C^n G) = C^n Q$. Comme $C^s Q = \{e\}$, on voit que $C^s G \subset \mathrm{Ker}(\pi) \subset Z(G)$ et $[C^s G, G] = \{e\}$. □

Corollaire 80. *Soit* P *un* p*-groupe. Alors* P *est nilpotent.*

Démonstration. Si $|P| = p$, alors P est abelian $\Rightarrow$ nilpotent. On suppose que groupe d'ordre $\leqslant p^n$ est nilpotent. Soit P d'ordre p^{n+1} ; son centre, notons-le Z, n'est pas trivial (voir Exemple 31) et G/Z est un p-groupe d'ordre $\leqslant p^n$. Soit $\pi : P \to P/Z$ la projection. Comme Z est nilpotent, on déduit que P est nilpotent par le lemme. □

Corollaire 81. *Soient* $p_1, \ldots, p_r$ *des nombres premiers distincts et, pour chaque* i, *soit* P_i *un* p_i*-groupe. Alors* $P_1 \times \cdots \times P_r$ *est nilpotent.*

Lors du prochain cours, on vera que tous les groupes nilpotents finis sont de la forme décrite au corollaire précédent.

Cours 6

(5 mars 2021).

On étudie les groupes nilpotent finis. On aura besoin de la

Définition 82. Un sous-groupe H de G est *maximal* si $H \neq G$ et si de plus le seul sous-groupe H' de G contenant strictement H est G lui même.

On note que si G est fini, alors tout sous-groupe propre H est contenu dans un maximal. En effet, on considère l'ensemble fini $\mathscr{F}$ des sous-groupes propres de G qui contiennent H et on choisit un élément dont le cardinal est maximal. Par contre, ceci est faux si l'hypothèse de finitude est abandonnée.

Théorème 83 (Burnside–Wielandt)**.** *Soit G fini. Les affirmations suivantes sont équivalentes.*

1. *G est nilpotent.*
2. *Si H est un sous-groupe propre , alors H est un sous-groupe propre de $N_G(H)$. (Les normalisateurs grandissent.)*
3. *Soit $M < G$ maximal. Alors $M \lhd G$. (Les maximaux sont distingués.)*
4. *Soit $P < G$ un Sylow. Alors $P \lhd G$. (Les Sylows sont distingués.)*
5. *G est un produit de p-groupes.*

La preuve aura besoin du

Lemme 84 (L'argument de Frattini)**.** *Soient G fini, $D \lhd G$ et $P < D$ un Sylow de D. Alors, dans la notation du Lemme 34, l'on a $DN_G(P) = G$. (Attention : pas forcément un produit semi-direct !)*

Démonstration. Soit $g \in G$. Alors gPg^{-1} est un Sylow de D (Corollaire 72). Donc $dPd^{-1} = gPg^{-1}$ pour un certain $d \in D$. Il suit que $d^{-1}g \in N_G(P) \Rightarrow g \in DN_G(P)$. □

Démonstration. 1. ⇒ 2. Soit $H \lneqq G$. Soit $n \in \mathbb{N}$ tel que $C^{n+1}G < H$ mais C^nG n'est pas contenu dans H. Comme $[C^nG, H] \leqq [C^nG, G] \leqq C^{n+1}G$, on voit que $[C^nG, H] \leqq H$. Donc, si $c \in C^nG$ et $h \in H$, on a $chc^{-1}h^{-1} \in H$ et donc $chc^{-1} \in H$, c'est à dire, $C^nG \leqq N_G(H)$.

2. ⇒ 3. Trivial.

3. ⇒ 4. On suppose l'existence d'un Sylow P qui n'est pas distingué. Dans ce cas, $N_G(P) \neq G$. Soit ainsi $M \lneqq G$ maximal contenant $N_G(P)$. Par hypothèse $M \lhd G$. L'argument de Frattini (Lemme 84) montre que $MN_G(P) = G$. Par conséquent, $M = G$, ce qui est contradictoire.

4. $\Rightarrow$ 5. On e que si H et K sont des sous-groupes distingués tels que $H \cap K = e$, alors $[H, K] = e$; il suffit de remarquer que pour $h \in H$ et $k \in K$ on a $[h, k] = \underbrace{hkh^{-1}}_{\in K} k^{-1} = h \underbrace{kh^{-1}k}_{\in H}$; d'où $[h, k] = e$. Ceci étant, si P est un p-Sylow et Q un q-Sylow avec $p \neq q$, il suit que $[P, Q] = e$. Soit $|G| = p_1^{e_1} \cdots p_r^{e_r}$ avec p_i premier. Soient P_i un p_i-Sylow associé. Alors

$$\phi : P_1 \times \cdots \times P_r \longrightarrow G, \quad (x_1, \ldots, x_r) \mapsto x_1 \cdots x_r$$

est un morphisme car $[P_i, P_j] = e$. Il est un morphisme *injectif* : si $x_1 \cdots x_r = e$ et si $q_i = |G|/p_i^{e_i}$, alors

$$(x_1 \cdots x_r)^{q_1} = x_1^{q_1} \cdots x_r^{q_1} = x_1^{q_1} = e.$$

Or, mais $\operatorname{ord}(x_1^{q_1}) = \operatorname{ord}(x_1)$, et donc $x_1 = e$. Par récurrence on voit que $x_i = e$ pour tout i.

5.$\Rightarrow$1. Facile. □

9 Représentations linéaires

G est un groupe. On fixe un corps de base $\mathbb{K}$.

Définition 85. Une représentation linéaire [7] est la donnée d'un espace vectoriel V et d'un action linéaire $G \times V \to V$; dit autrement, $g * (\lambda v + w) = \lambda \cdot g * v + g * w$.

Il est clair qu'une représentation linéaire sur V est la même chose qu'un morphisme de groupes $\varrho : G \to \mathrm{GL}(V)$. Dans la suite, si nécessaire, on dira que (V, ϱ) est une représentation de G.

Exemple 86.

1. La *representation* triviale est la rep. de G sur l'espace $\mathbb{K}$ donnée par $g * c = c$. Elle sera notée $\mathbb{1}$.
2. Si $G \leqq \mathrm{GL}_n$, alors le morphisme $\mathrm{id} : G \to \mathrm{GL}_n$ définit la rep. “standard”.
3. Soient V et W des représentations de G. Alors l'espace vectoriel $V \oplus W$ avec l'action $g(v, w) = (gv, gw)$ est une rep. linéaire dite la rep. *somme directe.*
4. Soient V et W des représentations de G et soit $H = \mathrm{Hom}_{\mathbb{K}}(V, W)$. Alors pour chaque $\phi : V \to W$ et chaque $g \in G$ on pose

$$g\phi : v \mapsto g\phi(g^{-1}v).$$

On vérifie facilement qu'il s'agit d'une représentation de G.

7. Bientôt “linéaire” sera omis !

5. Si dans le cas précédent $W = \mathbb{1}$, alors $\mathrm{Hom}_{\mathbb{K}}(V, W) = V^*$ est appelée la *représentation duale* (ou contragrédiente !) de V.
6. Soit X un ensemble. On note $F(X, \mathbb{K})$ l'espace vectoriel des fonctions $\phi : X \to \mathbb{K}$. Si $G \circlearrowleft X$, alors $F(X, \mathbb{K})$ admet une représentation définie par

$$g\phi(x) = \phi(g^{-1}x).$$

   Cette rep. est dite la *représentation de permutation* associée à X.
7. Si G agit sur lui même par translations à gauche, la représentation $F(G, \mathbb{K})$ construite avant est appelée la représentation régulière (à gauche).

Définition 87. 1. Soient V et W des représentation de G. Une application linéaire G-equivariante $\phi : V \to W$ est dite un morphisme de représentations.

2. Soit V une rep. de G. Un sous-espace $W \subset V$ est dit une sous-représentation quand $g(W) \subset W$ pour tout $g \in G$. (On dit aussi : W est *invariant* par G, V est *stable* par G.)

Exemple 88. Soit $G = \mathbb{Z}$. Si V est un espace vectoriel, alors une représentation de G sur V est la donnée d'un $A \in \mathrm{GL}(V)$: en effet,

$$\rho(k) = A^k$$

définie un morphisme $\mathbb{Z} \to \mathrm{GL}(V)$.

Exemple 89. Soit $n \in \mathbb{N} \backslash 0$. Alors pour chaque racine $n$ème de l'unité ζ, on obtient une représentation de $\mathbb{Z}/n$ sur $\mathbb{C}$ par

$$\rho(k \mod n) = \zeta^k.$$

(Ici, ζ^k est vue comme application linéaire de $\mathbb{C}$ dans $\mathbb{C}$ par multiplication.) En fait, une représentation de $\mathbb{Z}/n$ sur $\mathbb{K}^r$ est déterminée par une matrice A d'ordre n.

Exemple 90. Soit V une représentation de G. Alors $V^G = \{v \in V : gv = v\}$ est l'ensemble des vecteurs invariants ; clairement V^G est une sous-représentations.

Si W_i sont des sous-reps de V alors $\sum W_i$ est également une sous-rep. de G.

Exercice 91. Soit $\phi : V \to W$ un morphisme de reps. de G. Alors $\mathrm{Ker}(\phi)$ est une sous-rep. de V et $\mathrm{Im}(\phi)$ est une sous-rep. de W.

Définition 92. Soit V une rep. de G. On dira que V est *simple*, ou *irréductible*, si $V \neq \{0\}$ et les seules sous-représentations de V sont $\{0\}$ et V elle même. On dira que V est *semi-simple* si V peut-être engendré par des sous-représentations simples. [8]

Exemple 93. Toute représentation de dimension un est simple.

Exemple 94. Soit $n > 2$ et $\sigma : \mathscr{D}_{2n} \to \mathrm{GL}_2(\mathbb{R})$ la rep. standard. On affirme que σ est simple. En effet, si $L \subset \mathbb{R}^2$ est une sous-représentation, différente de $\{0\}$ ou $\mathbb{R}^2$, alors L est une droite et $S(L) = L$. Donc L est l'axe des x ou des y. Mais R ne preserve pas l'axe des x, car R n'est pas la rotation de π.

Exercice 95. Soit $n > 2$. On considère la représentation tautologique de $\tau : \mathscr{D}_{2n} \to \mathrm{GL}_2(\mathbb{C})$; c'est-à-dire, τ est la composition

$$\mathscr{D}_{2n} \xrightarrow{\sigma} \mathrm{GL}_2(\mathbb{R}) \xrightarrow{\text{incl.}} \mathrm{GL}_2(\mathbb{C}).$$

Montrer que τ est simple.

Exemple 96 (Représentations simples d'un abélien)**.** Soit G abélien et (V, ϱ) une représentation complexe *simple* de dimension finie. Soit $g \in G$ et soit λ un valeur propre de g. Alors l'espace propre $E(\lambda, g) = \{v \in V \ : \ gv = \lambda v\}$ est stable par G : si $h \in G$ et $v \in E(\lambda, g)$ alors

$$\begin{aligned} g(hv) &= hg(v) \\ &= h(\lambda v) \\ &= \lambda h(v). \end{aligned}$$

Comme V est simple, $E(\lambda, g) = V$ et $g = \lambda I$. Comme g est arbitraire, on voit que pour chaque $h \in G$, on a $hv = \lambda_h \cdot v$ pour un certain $\lambda_h \in \mathbb{C}^*$. Or, il est clair que dans ce cas, la simplicité force $\dim V = 1$.

8. Dans les notes de cours précédentes, il avait une *erreur* dans la définition de semi-simplicité, comme m'a averti Shunan Sun, qui est vivement remercié. J'ai fait confusion entre "V est engendré par les sous-représentations simples" et "V est réunion des représentations simples". Il est assez facile de voir que si S et T sont des reps simples non-isomorphes de G, alors pour chaque couple $s \in S \backslash \{0\}$ et $t \in T \backslash \{0\}$, l'élément $s + t \in S \oplus T$ n'appartient pas à une sous-rep simple ! En effet, soit $X \subset S \oplus T$ sous-rep simple contenant $s + t$. On considère les projections $\pi_S : X \to S$ et $\pi_T : X \to T$, qui sont non-nulles. Par Schur, $X \simeq S$ et $X \simeq T$!

Cours 7

(12 mars 2021).

Voici quelques remarques qui n'ont pas été traités à la fin du dernier cours.

Exemple 97. Soit $G = \mathbb{Z}/4$ et soit $\varrho : G \to \mathrm{GL}_2(\mathbb{R})$ la rep. définie par

$$\varrho(1) = R_{\pi/2} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Elle est simple, mais de dimension 2, donc dans l'exemple 96 il faut en effet prendre des reps complexes.

Remarques 98 (Mise en garde). Soit V une rep. de G. Soit $v \in V$ non-nul. Alors

$$\langle Gv \rangle := \mathrm{Vect}\{gv \ : \ g \in G\}$$

est clairement une sous-rep. Même si $\langle Gv \rangle$ semble être simple, il n'est pas forcément comme montre l'exemple 99.

Exemple 99. Soit $G = \mathbb{Z}$, on considère la rep. en $\mathbb{C}^2$ définie par

$$k \longmapsto \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}.$$

Alors V n'est pas semi-simple. En effet, $\mathbb{C}e_1$ est une sous-rep. Puis, on voit que si W est une sous-rep. contenant e_2, alors $1 * e_2 - e_2 = e_1$ implique que $e_1 \in W$ et donc e_2 n'est pas contenu dans une sous-rep. simple.

On fera maintenant un brève étude de la semi-simplicité suivant [Lang]. Avant de commencer, le lecteur doit se certifier d'être capable de faire l'exercice suivant :

Exercice 100. Soit V une rep de G et soient S et W des sous-reps de V. On suppose que S est *simple*. Montrer que $W \cap S = 0$ ou $S \subset W$.

Pour développer la théorie de la semisimplicité, on aura besoin des rappels suivants :

Définition 101 (Rappel)**.** Soit V un espace vectoriel et $\{W_i\}_{i \in I}$ une famille de sous-espaces. On définit $\sum_i W_i$ comme étant le sous-espace vectoriel de V engendré par la famille $\{W_i\}$: un élément $v \in V$ appartient à V si et seulement si il existe un sous-ensemble fini $I_0 \subset I$ et, pour chaque $i \in I_0$, un élément $w_i \in W_i$ tel que $v = \sum_{i \in I_0} v_i$.

On dira que la somme $\sum W_i$ est *directe*, si pour chaque sous-ensemble fini $I_0 \subset I$ et chaque famille $\{w_i \in W_i \ : \ i \in I_0\}$, l'équation $\sum_{i \in I_0} w_i = 0$ force $w_i = 0$. Si la somme est directe, alors on écrit $\bigoplus W_i$ au lieu de $\sum W_i$.

On note que $\sum_{i\in I} W_i$ est directe si et seulement si, pour chaque $i \in I$, on a

$$W_i \cap \sum_{i\in I\setminus\{i\}} W_i = 0.$$

Avec cette définition, on a la réformation suivante de la définition de semi-simplicité. Soit V une rep. de G. On note $\{S_i : i \in I\}$ le sous-ensemble des sous-représentations simples et non-nulles de V. Alors V est semi-simple si et seulement si $V = \sum_i V_i$. En fait, on a :

Théorème 102. *Soit V une rep. de G et $\{S_i : i \in I\}$ la famille des sous-reps simples de V. Les conditions suivantes sont équivalentes.*

1. *V est semi-simple.*
2. *Pour un certain sous-ensemble $M \subset I$, on a $V = \bigoplus_{m\in M} S_m$. (Dit autrement, $V = \sum_{m\in M} S_m$ et la somme est directe.)*
3. *Si $W \subset V$ est une sous-représentation, il existe une autre sous-rep. $C \subset V$ telle que $V = W \oplus C$.*

Démonstration. On fera la preuve que dans le cas $\dim V < \infty$. Si $J \subset I$, on écrit $S_J = \sum_{j\in J} S_j$.

1. $\Rightarrow$ 2. Soit $\mathscr{D}$ le sous-ensemble de parties de I formé par $D \subset I$ tel que la somme $\sum_{d\in D} S_d$ est directe. (Clairement chaque $\{i\} \in \mathscr{D}$.) Pour chaque $D \in \mathscr{D}$, la dimension $\dim S_D$ est bornée par $\dim V$, et on choisit $M \in \mathscr{D}$ tel que $\dim S_M$ soit maximale. On montre que $V = S_M$. Pour cela, on doit montrer que pour chaque $i \in I$, le sous-espace S_i est contenu dans S_M. Soit, par absurde, $i \in I$ tel que S_i n'est pas contenue dans S_M. Clairment $i \notin M$. Comme $S_i \cap S_M \neq S_i$, la simplicité de S_i entraine $S_i \cap S_M = 0$. Or, dans ce cas, la somme $S_i + S_M$ est directe et $\dim S_i + S_M > S_M$. Contradiction.

2. $\Rightarrow$ 3. On suppose $W \neq V$ (autrement il n'y a rien à prouver). Soit

$$\mathscr{D} = \{D \subset M : \text{la somme } W + S_D \text{ est directe}\}.$$

On note que si S_i n'est pas contenu dans W, alors $\{i\} \in \mathscr{D}$. Donc $\mathscr{D} \neq \varnothing$. Soit $N \in \mathscr{D}$ tel que $\dim S_N$ est maximale. Par construction, $W + S_N$ est directe.
Affirmation. $V = W + S_N$.

On doit montrer que $S_m \subset W + S_N$ pour chaque $m \in M$. Soit ainsi $m \in M$. Si $S_m \subset S_N$ il n'y a rien à faire. Donc, on suppose $S_m + S_N \neq S_N$ (en particulier $m \notin N$). Dans ce cas, $N \cup \{m\}$ ne peut pas appartenir à $\mathscr{D}$ et la somme $W + (S_m + S_N)$ n'est pas directe. Il existe ainsi $w \in W$, $s_m \in S_m$, un sous-ensemble fini N_0 de N et une famille $\{s_n : n \in N_0\}$ ayant les deux propriétés suivantes :

— Au moins un éléments de $\{w, s_m\} \cup \{s_n : n \in N_0\}$ est non-nul et

— $w + s_m + \sum_{n \in N_0} s_n = 0$.

Si $s_m = 0$, alors le fait que $W + S_N$ soit directe montre que $w = s_n = 0$, une contradiction. Donc $s_m \neq 0$. Par conséquent, $S_m \cap (W + S_N) \neq 0$ et on déduit $S_m \subset W + S_N$.

3. $\Rightarrow$ 1. On montre d'abord que chaque sous-rep non-nulle $W \subset V$ contient une sous-rep simple non-nulle : en effet, on considère l'ensemble

$$\{\dim X \,:\, X \subset W \text{ est une sous-représentation non-nulle}\}.$$

Si $\dim X$ est minimale, alors X est simple. On considère la sous-rep. S_I de V. Par définition, $S_I \oplus C = V$ pour une certaine sous-rep C de V. Or, si $C \neq 0$, il existe un $i \in I$ tel que $S_i \subset C$, et donc la somme n'est pas directe. $\square$

Remarques 103. Il est intéressant de voir que $M \neq I$ dans (2). En effet, si $G = e$ et $V = \mathbb{C}^2$, alors chaque droite vectorielle de V est une sous-rep. et clairement V n'est pas la somme directe de toutes ses droites vectorielles.

Remarques 104. Soit V une rep et $\{S_i\}_{i \in I}$ l'ensemble des sous-reps *simples* de V. La somme $\sum S_i$ est une rep *semi-simple* de V connue comme la socle (notation $\mathrm{soc}(V)$) de V.

Remarques 105. La propriété (3) décrite dans le Théorème 102 a eu une importance dans la célèbre théorie des invariants. (Beaucoup étudié au XIX et au XX et responsable pour pas mal de résultats d'Algèbre moderne.) Si $G < \mathrm{GL}_n(\mathbb{C})$ est un sous-groupe, on peut considérer l'action de G sur les polynômes $\mathbb{C}[\boldsymbol{x}] = \mathbb{C}[x_1, \ldots, x_n]$ définie par

$$gP(x_1, \ldots, x_n) = P\left(\sum_{i=1}^n g_{i1} x_i, \ldots, \sum_{i=1}^n g_{in} x_i\right)$$

et se demander quelle est la nature de l'anneau $\mathbb{C}[\boldsymbol{x}]^G = \{P \in \mathbb{C}[\boldsymbol{x}] \,:\, gP = P\}$. L'existence des compléments permet de construire une fonction $\mathbb{C}[\boldsymbol{x}] \to \mathbb{C}[\boldsymbol{x}]^G$.

Exercice 106. Soit $A \in \mathrm{GL}_n(\mathbb{C})$ et $\varrho : \mathbb{Z} \to \mathrm{GL}_n(\mathbb{C})$ la rep. de $\mathbb{Z}$ naturelement déduite : $\varrho(k) = A^k$. Montrer que ϱ est semi-simple si et seulement si A est diagonalisable.

Lemme 107. *Soit V rep. semi-simple de G. Soit $i : U \to V$ une sous-rep. Alors U est semi-simple. Soit $\pi : V \to Q$ une rep. quotient. Alors Q est semi-simple.*

Démonstration. Soit $U' \subset U$ une sous-rep et soit $C \subset V$ un complément G-invariant de U. Si $u \in U$, alors on écrit $u = u' + c$ avec $u' \in U'$ et $c \in C$. Dans ce cas, $u - u' = c \in C \cap U$ et $U = U' \oplus (U \cap C)$.

Ensuite, soit $S \subset V$ une rep simple. Alors $\pi(S)$ est soit nulle, soit simple (vérifiez). Comme $\pi\left(\sum_i S_i\right) = \sum \pi(S_i)$, on voit que Q est semi-simple. $\square$

Le Théorème 102 dit qu'une représentation semi-simple est isomorphe à une somme directe de représentations simples. Rien, à priori, assure que cette décomposition est bien déterminée. On travaillera maintenant pour comprendre cette situation en prouvant le théorème suivant qui conduira à la définition 111 plus bas.

Théorème 108. *Soient $S_1, \ldots, S_m$ des représentations simples de dimension finie non-isomorphes deux-à-deux et $a_1, \ldots, a_m$ des entiers strictement positifs. Soient $T_1, \ldots, T_n$ des représentations simples de dimension finie non-isomorphes deux-à-deux et $b_1, \ldots, b_n$ des entiers strictement positifs. Soit*

$$\varphi : \bigoplus_{i=1}^{m} S_i^{a_i} \xrightarrow{\sim} \bigoplus_{j=1}^{n} T_j^{b_j}$$

un isomorphisme entre représentations. Alors

1) Les entiers m et n coincident.

2) Il existe $\sigma \in \mathscr{S}_n$ telle que $S_i \simeq T_{\sigma(i)}$, et

3) $a_i = b_{\sigma(i)}$.

La preuve aura besoin du Lemme de Schur et de son Corollaire.

Lemme 109 (Lemme de Schur)**.** *Soient S et T reps. simples.*

1. Si $\varphi : S \to T$ est morphisme de G-reps non-nul, alors φ est iso.

2. Si $\mathbb{K}$ est algébriquement clos, alors chaque morphism $u : S \to S$ est un scalaire $u(s) = \lambda s$.

Démonstration. (1) On regarde $\mathrm{Ker}(\varphi)$ et $\mathrm{Im}(\varphi)$ et on employe la définition de simplicité.

(2) Soit λ une valeur propre de φ. Alors $\varphi - \lambda \mathrm{I} : S \to S$ est un morphisme de représentations. Comme $\varphi - \lambda\mathrm{I}$ n'est pas iso. (car le noyau est non-nul) on voit que $\varphi = \lambda \mathrm{I}$. □

Corollaire 110. *Soient S et T simples. Si $\varphi : S^a \to T^b$ est un morphisme non-nul, alors $S \simeq T$.*

Démonstration. Soit $p_i : T^b \to T$ la i-ème projection et $u_j : S \to S^a$ la j-ème inclusion. Alors $p_i \varphi u_j$ est un iso. ou est nulle. Si elle est nulle pour tout i et j alors φ est nulle. Pour un certain couple i, j il suit que $p_j \varphi u_i \neq 0$ et on conclut par le Lemme de Schur. □

Démonstration du Théorème 108. Pour chaque $i \in \{1, \ldots, m\}$ et chaque $j \in \{1, \ldots, n\}$, soit $u_i : S_i^{a_i} \to \bigoplus_k S_k^{a_k}$ l'inclusion et $p_j : \bigoplus T_k^{b_k} \to T_j^{b_j}$ la projection. Alors $p_j \varphi u_i : S_i^{a_i} \to T_j^{b_j}$ est morphisme de représentations.

Soit $i \in \{1,\ldots,m\}$ fixé. Si $j \in \{1,\ldots,n\}$ est tel que $p_j\varphi u_i \neq 0$ alors $S_i \simeq T_j$ (Corollaire 110). Si $p_j\varphi u_i = 0$ pour *tout* $j \in \{1,\ldots,n\}$, on voit que $\varphi u_i = 0$, ce qui est impossible car φ est injective. Il existe ainsi un $j \in \{1,\ldots,n\}$ tel que

$$p_j\varphi u_i \neq 0$$

et donc $T_j \simeq S_i$. En plus, j est l'unique $k \in \{1,\ldots,n\}$ tel que $p_k\varphi u_i \neq 0$ comme garantit le Corollaire 110 et le fait que les $T_1,\ldots,T_n$ sont non-isomorphes deux-à-deux.

On obtient alors une fonction

$$\sigma : \{1,\ldots,m\} \longrightarrow \{1,\ldots,n\}$$

avec les propriétés suivantes :

a) $p_{\sigma(i)}\varphi u_i \neq 0$,

b) $S_i \simeq T_{\sigma(i)}$ et

c) $p_j\varphi u_i = 0$ si $j \neq \sigma(i)$.

Par (b), on déduit $\dim S_i = \dim T_{\sigma(i)}$. Par (c), on déduit que $\varphi(S_i^{a_i}) \subset T_{\sigma(i)}^{b_{\sigma(i)}}$: ceci montre que $a_i \leqslant b_{\sigma(i)}$ et que σ est surjective car

$$\varphi\left(\bigoplus_{i=1}^m S_i^{a_i}\right) \subset \bigoplus_{i=1}^m T_{\sigma i}^{b_{\sigma(i)}}.$$

Puis, si $\sigma(i) = \sigma(i')$ alors (b) prouve que $S_i \simeq S_{i'}$ et donc $i = i'$ par hypothèse : σ est injective. Pour terminer, l'inégalité $a_i \leqslant b_{\sigma(i)}$ est une égalité car autrement $\sum_{i=1}^m a_i \dim S_i < \sum_{i=1}^m b_{\sigma i} \dim T_{\sigma(i)}$. □

Une [9] conclusion importante de ce résultat est la suivante. Soient V une rep. semi-simple (dimension finie) de G et X une rep simple de G. On écrit $V \simeq \bigoplus_{i=1}^m S_i^{a_i}$, où chaque S_i est simple, chaque a_i es strictement positif, et S_i n'est pas isomorphe à $S_{i'}$ si $i \neq i'$. On définit

$$(V : X) := \begin{cases} a_i, & \text{si } S_i \simeq X \\ 0, & \text{si } X \text{ n'est pas isomorphe à un des } S_i. \end{cases}$$

Par le théorème, le naturel $(V : X)$ est indépendant du isomorphisme $S \simeq \bigoplus_{i=1}^m S_i^{a_i}$ choisi.

Définition 111. Soit V une rep. semi-simple de dimension finie de G et X une représentation simple. L'entier $(V : X)$ est dit la *multiplicité* de X dans V et un isomorphisme $V \simeq \bigoplus_{i=1}^r S_i^{a_i}$, où $\{S_i\}_{i=1}^r$ sont simples et deux-à-deux non isomorphes, est appelé une décomposition *isotypique* de V.

9. Cette partie va être traitée dans la prochaine séance.

Cours 8

(19 Mars 2021).

Le principal cas où toutes les représentations sont semi-simples est :

Théorème 112 (Maschke)**.** *Soit V une représentation de dimension finie du groupe fini G. On suppose que l'entier $|G|$ est inversible dans le corps $\mathbb{K}$. Alors V est semi-simple.*

On donnera deux preuves. La première, très simple, suppose $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Démonstration. On fera le cas $\mathbb{K} = \mathbb{C}$. $\varphi : V \times V \to \mathbb{C}$ une forme hermitienne définie positive. Par exemple, on peut choisir une base $\{v_1, \ldots, v_n\}$ et décréter $\varphi(v_k, v_\ell) = 0$ si $k \neq \ell$ et 1 si $k = \ell$.

Alors

$$\psi(v, w) = \frac{1}{|G|} \sum_{g \in G} \varphi(gv, gw)$$

est une forme bilinéaire, symétrique et *invariante*, i.e. $\psi(gv, gw) = \psi(v, w)$. En plus, ψ est définie positive aussi car

$$\psi(v, v) = \frac{1}{|G|} \sum_{g \in G} \varphi(gv, gv).$$

Si U est sous-rep., alors $U^{\perp_\psi}$ est sous-rep. également (si $\psi(v, u) = 0$ pour tout $u \in U$, alors $\psi(gv, u) = \psi(v, g^{-1}u) = 0$. Or, comme $U^\perp \oplus U = V$, la preuve est terminée. □

L'autre preuve est aussi très utile. On employe :

Théorème 113 (L'opérateur de moyenne)**.** *Soit V une représentation de dimension finie de G. On suppose que $|G|$ est inversible dans $\mathbb{K}$. Alors la fonction*

$$M : V \longrightarrow V, \qquad v \longmapsto \frac{1}{|G|} \sum_{g \in G} g(v)$$

est telle que

(1) $M(V) \subset V^G$,

(2) pour chaque $v \in V^G$, $M(v) = v$, et

(3) M est équivariante.

Dit autrement, $M : V \to V^G$ est un projecteur équivariant.

Démonstration. (1) Soit $v \in V$ et $h \in G$. On a

$$\begin{aligned} h\left(M(v)\right) &= \frac{1}{|G|} \cdot h\left(\sum_{g \in G} g(v)\right) \\ &= \frac{1}{|G|} \sum_g hg(v) \\ &= \frac{1}{|G|} \sum_{g'} g'(v) \\ &= M(v). \end{aligned}$$

On déduit $M(v) \in V^G$.

(2) Si $v \in V^G$, alors $M(v) = \dfrac{1}{|G|} \displaystyle\sum_g g(v) = \dfrac{1}{|G|} \sum_g v = \dfrac{1}{|G|} \cdot |G| v$.

(3) On a

$$\begin{aligned} M(hv) &= \frac{1}{|G|} \sum_g gh(v) \\ &= \frac{1}{|G|} \sum_{g'} g'(v) \\ &= M(v) \\ &= hM(v). \end{aligned}$$

□

Remarques 114. L'idée de "faire la moyenne" est très utile. Dans la théorie des groupes de Lie, on remplace $\frac{1}{|G|} \sum_{g \in G}$ par une "intégrale invariante" $\int_G$. Voir §VIII du Chap. V de [Chevalley]. Cette idée a été aussi employée pour étudier les groupes de Lie qui ne sont pas compacts mais qui "possèdent un sous-groupe compact suffisamment grand." Voir par exemple la Section 4.11 du livre [Varadarajan].

Avant de donner notre deuxième preuve du Thm. de Maschke, on propose au lecteur de prendre le temps et de faire le

Exercice 115. Soient V et W des reps de G. Rappeler que $H = \mathrm{Hom}(V, W)$ est naturellement une rep de G et prouver que H^G est exactement le sous-espace des morphismes G-équivariants $\mathrm{Hom}_G(V, W)$.

Deuxième preuve du théorème de Maschke. Soit $U \subset V$ invariant. Soit $p : V \to U$ un *projecteur arbitraire*, c'est-à-dire, $p(u) = u$ pour tout u. On interprète p comme un élément de $H = \mathrm{Hom}(V, U)$. Soit Mp sa moyenne ; il s'agit d'un élément de $\mathrm{Hom}_{\mathbb{K}}(V, U)^G =$

$\mathrm{Hom}_G(V, U)$. Pour $u \in U$, on a $gu \in U$, et donc $p(gu) = gu$, qui montre que

$$\begin{aligned} Mp(u) &= \frac{1}{|G|} \sum_{g \in G} gp(u) \\ &= \frac{1}{|G|} \sum_{g \in G} gp(g^{-1}u) \\ &= \frac{1}{|G|} \sum_{g \in G} u \\ &= u. \end{aligned}$$

Par conséquent, $Mp : V \to U$ est un projecteur G-équivariant. Soit $U' = \mathrm{Ker}(Mp)$. Alors si $v \in V$, on a

$$v = \underbrace{v - Mp(v)}_{\in U'} + \underbrace{Mp(v)}_{\in U}.$$

Donc, $V = U + U'$. Puis, si $u \in U \cap U'$ alors $u = Mp(u) = 0$ et donc la somme est directe. □

Reps de dimension 1

Définition 116. Le groupe quotient $G/[G, G]$ est appelé l'abélianisé de G et est notée G^{ab}. (Le lecteur doit se rappeler que $[G, G] \lhd G$.)

Exercice 117. Soit A un groupe abélien. Alors chaque morphisme $\varrho : G \to A$ s'écrit de façon unique comme $\overline{\varrho}\pi$ où $\overline{\varrho} : G^{\mathrm{ab}} \to A$ est un morphisme et $\pi : G \to G^{\mathrm{ab}}$ est le morphisme quotient. Dit autrement,

$$\mathrm{Hom}(G^{\mathrm{ab}}, A) \longrightarrow \mathrm{Hom}(G, A), \quad \varphi \longmapsto \varphi\pi$$

est bijective.

Une représentation de dimension un de G est dite un *caractère*. Soit (L, χ) une telle représentation. Si $\ell \in L \backslash 0$ alors on peut écrire $\chi(g)\ell = \chi_g \cdot \ell$. Si ℓ' est un autre vecteur non nul, alors on voit facilement que $\chi(g)\ell' = \chi_g \ell'$ (pas de faute de frappe : c'est le même χ_g). Ceci étant, on a une bijection

$$\left\{ \begin{array}{c} \text{classes d'isomorphismes} \\ \text{de caractères de } G \end{array} \right\} \longrightarrow \mathrm{Hom}(G, \mathbb{K}^*).$$

En particulier, l'ensemble des caractères (à isomorphisme près) est un groupe avec la multiplication

$$\theta_1 * \theta_2(g) = \theta_1(g)\theta_2(g).$$

Ce groupe sera noté $\mathbb{X}(G)$. D'après l'exercice 117, le morphisme évident de groupes

$$\mathbb{X}(G^{\mathrm{ab}}) \longrightarrow \mathbb{X}(G), \quad \theta \longmapsto \theta \circ \pi$$

est un isomorphisme.

Exemple 118. On sait que $[\mathscr{D}_{2n}, \mathscr{D}_{2n}] = \langle R^2 \rangle$ (Exemple 77). Il suit que

$$\#[\mathscr{D}_{2n}, \mathscr{D}_{2n}] = \begin{cases} n, & \text{si } n \equiv 1 \mod 2, \\ n/2 & \text{si } n \equiv 0 \mod 2. \end{cases}$$

Si n est impair, alors $\mathscr{D}_{2n}^{\mathrm{ab}} \simeq \mathbb{Z}/2$. Si n est pair, alors $\mathscr{D}_{2n}^{\mathrm{ab}}$ est un groupe abélien d'ordre 4. Comme il est engendré par (les classes de) R et S, on voit que dans $\mathscr{D}_{2n}^{\mathrm{ab}}$ il n'existe aucun élément d'ordre 4, et ceci signifie que

$$\mathbb{Z}/2 \times \mathbb{Z}/2 \longrightarrow \mathscr{D}_{2n}^{\mathrm{ab}}, \quad (i,j) \longmapsto R^i S^j$$

est un isomorphisme. Ceci étant, autre le caractère trivial, on a 3 caractères de $\mathscr{D}_{2n}$. Le premier $\theta_1 : \mathscr{D}_{2n} \to \mathbb{K}^*$ satisfait $\theta_1(R) = -1$ et $\theta(S) = 1$, le deuxième $\theta_2(R) = 1$ et $\theta_2(S) = -1$, et le troisième est leur "produit" $\theta_1\theta_2$.

Représentations de permutation

Soit X un G-ensemble fini. On étudie davantage $F(X, \mathbb{K})$. Soit $\delta_x : X \to \mathbb{K}$ la fonction de "Dirac" associée au point $x \in X$: $\delta_x = 0$ sauf sur x, où δ_x vaut 1. Clairement, $\{\delta_x\}_{x \in X}$ est une base de $F(X, \mathbb{K})$ et on souhaite déterminer la matrice de $g \in G$ associée à cette base. On a

$$\begin{aligned} g\delta_x(y) &= \delta_x(g^{-1}y) \\ &= \begin{cases} 1 & \text{if } gx = y, \\ 0 & \text{autrement.} \end{cases} \\ &= \delta_{gx}(y). \end{aligned}$$

Donc

$$\boxed{g\delta_x = \delta_{gx}}.$$

En écrivant

$$g\delta_y = \sum_{x \in X} g_{xy} \cdot \delta_x,$$

on déduit que

$$g_{xy} = \begin{cases} 1 & \text{si } gy = x, \\ 0 & \text{autrement.} \end{cases}$$

On remarque que $F(X, \mathbb{K})$ possède toujours une sous-représentation isomorphe à $\mathbb{1}$ définie par $\mathbb{K}1$ (les fonctions constantes). Il est aussi possible de voir la rep $\mathbb{1}$ comme *quotient* de $F(X, \mathbb{K})$ via

$$\Sigma : F(X, \mathbb{K}) \longrightarrow \mathbb{1}, \quad \varphi \longmapsto \sum_{x \in X} \varphi(x).$$

Le noyau de Σ est une sous-rep de $F(X, \mathbb{K})$ et sera noté $I(X, \mathbb{K})$. Voici quelques propriétés de $I(X, \mathbb{K})$.

Lemme 119. *Si $|X|$ est inversible dans le corps $\mathbb{K}$ (c'est-à-dire, si la caractéristique de $\mathbb{K}$ ne divise pas $|X|$) alors la rep $F(X, \mathbb{K})$ s'écrit comme somme directe des sous-reps $I(X, \mathbb{K})$ et $\mathbb{K}1$.*

Démonstration. Il suit facilement que $\mathbb{1} \cap I(X, \mathbb{K}) = 0$ car $\Sigma(c1) = c \cdot |X|$. □

Tout comme $F(X, \mathbb{K})$ vient avec une base canonique $\{\delta_x\}$, $I(X, \mathbb{K})$ peut être muni d'une base qui dépend du choix d'un point de base $x_0 \in X_0$, ou d'un ordre dans X.

Lemme 120. *Soit $x_0 \in X$. Alors $\{\delta_x - \delta_{x_0} : x \neq x_0\}$ est une base de $I(X, \mathbb{K})$. Si X est en bijection avec $\{1, \ldots, n\}$, alors $\delta_2 - \delta_1, \ldots, \delta_n - \delta_{n-1}$ est aussi une base.*

Démonstration. Soit $\varphi \in I(X)$. Alors $\varphi(x_0) = -\sum_{x \neq x_0} \varphi(x)$. Donc, comme $\varphi = \varphi(x_0)\delta_{x_0} + \sum_{x \neq x_0} \varphi(x)\delta_x$ on a $\varphi = \sum_{x \neq x_0} \varphi(x)(\delta_x - \delta_{x_0})$.

Pour prouver la deuxième affirmation, on note que $\delta_i - \delta_1 = (\delta_i - \delta_{i-1}) + (\delta_{i-1} - \delta_{i-2}) + \cdots + (\delta_2 - \delta_1)$. □

Mais il ne faut pas croire que ses bases doivent toujours être préférées :

Exemple 121. Soit $G = \mathscr{D}_8$; il agit sur $X = \{e_1, e_2, -e_2, -e_2\}$ (quatre côtés d'un carré). On souhaite déterminer la décomposition isotypique de $F(X) = F(X, \mathbb{C})$. En numérotant les sommets de façon anti-horaire, on trouve une base $\varepsilon_1 = \delta_{e_1}$, $\varepsilon_2 = \delta_{e_2}$, $\varepsilon_3 = \delta_{-e_1}$ et $\varepsilon_4 = \delta_{-e_2}$. On jette $\mathbb{C}1$ et on se concentre sur $I = I(X, \mathbb{K})$, qui a dimension 3. On aura besoin ainsi de trouver des sous-espaces invariants, et la géométrie nous suggère de travailler avec des arêtes du carré. En écrivant $\varepsilon_{ij} = \varepsilon_i - \varepsilon_j$, on munit I de la base ordonnée $\{\varepsilon_{13}, \varepsilon_{24}, \varepsilon_{12}\}$. (Le lecteur doit vérifier que $\varepsilon_{13}, \varepsilon_{24}$ et ε_{12} est une base de I.) Par ce choix, $V = \mathrm{vect}(\varepsilon_{13}, \varepsilon_{24})$ est clairement une sous-rep. En fait, par rapport à la base $\{\varepsilon_{13}, \varepsilon_{24}, \varepsilon_{12}\}$, on voit que

$$R \longmapsto \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad \text{et} \quad S \longmapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Ainsi, V est la rep standard définie par

$$R \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad S \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Quel est son complémentaire ? On choisit $p : I \to V$ la projection orthogonale à ε_{12} et on fait la moyenne

$$Mp : I \longrightarrow V, \quad Mp(v) = \frac{1}{8}\sum_{i=0}^{3} R^i p R^{-i}(v) + R^i S p R^i S(v).$$

Or, on sait que $Mp : I \to V$ est un projecteur et dont pour le calculer explicitement il nous manque $Mp(\varepsilon_{12})$. À l'aide des équations

$$\begin{aligned} p(\varepsilon_{12}) &= 0 \\ p(\varepsilon_{13}) &= \varepsilon_{13} \\ p(\varepsilon_{14}) &= \varepsilon_{24}, \end{aligned}$$

on trouve

$$Mp(\varepsilon_{12}) = \frac{1}{2}(\varepsilon_{13} - \varepsilon_{24}).$$

Le noyau de Mp est ainsi engendré par $v = 2\varepsilon_{12} - \varepsilon_{13} + \varepsilon_{24}$ et $Rv = -v$ tandis que $Sv = v$. Donc, le complémentaire de V est le caractère θ_1 de l'exemple 118.

Cours 9

(26 mars 2021).

On termine en regardant l'une des reps de permutation les plus utiles : la rep. régulière à gauche. (Voir l'exemple 86.)

En fait, pour donner une preuve plus claire, on fera appel à la rep. régulière *à droite.* On suppose G fini ; si $\varphi : G \to \mathbb{K}$ est une fonction, alors on définit

$$\varrho_{\mathrm{d}}(g)(\varphi) : G \longrightarrow \mathbb{K} \quad \text{par} \quad x \longmapsto \varphi(xg).$$

Clairement, ceci est la rep de permutation où on laisse G agir sur G non par translations à gauche, mais par translations à droite :

$$g \star x = xg^{-1}.$$

La représentation ainsi déduite est *la représentation régulière à droite.* On va la noter par $F_{\mathrm{d}}(G, \mathbb{K})$ et on reserve le symbole $F(G, \mathbb{K})$ pour la rep. régulière à gauche (voir exemple 86). Rien de vraiment nouveau a été crée car :

Lemme 122. *La fonction*

$$\sigma : F(G, \mathbb{K}) \longrightarrow F_{\mathrm{d}}(G, \mathbb{K}), \qquad \varphi \longmapsto (x \mapsto \varphi(x^{-1}))$$

définit un isomorphisme entre la rep. régulière à gauche et la rep. régulière à droite.

Démonstration. Soient $x, g \in G$ et $\varphi \in F(G, \mathbb{K})$. Alors

$$\begin{aligned}[][\sigma(g\varphi)](x) &= [g\varphi](x^{-1}) \\ &= \varphi(g^{-1}x^{-1}) \\ &= \varphi((xg)^{-1}).\end{aligned}$$

Puis,

$$\begin{aligned}[][\varrho_{\mathrm{d}}(g)(\varphi)](x) &= \varphi(xg) \\ &= [\sigma\varphi]((xg)^{-1}).\end{aligned}$$

□

Finalement on peut montrer que la rep. régulière (droite ou gauche !) "contient toutes les reps".

Proposition 123. *Soit V une rep de G de dimension finie. Soit $F_{\mathrm{d}}(G, V)$ l'espace des fonctions $G \to V$ muni de l'action*

$$\varrho_{\mathrm{d}}\varphi : x \longmapsto \varphi(xg).$$

1) Avec la définition précédente, G agit linéairement sur $F_{\mathrm{d}}(G, V)$.

2) Si $\dim V = n$, alors il existe un isomorphisme de reps $F_{\mathrm{d}}(G, V) \simeq F_{\mathrm{d}}(G, \mathbb{K})^n$.

3) Si $\dim V = n$, alors il existe un isomorphisme de reps $F(G, V) \simeq F(G, \mathbb{K})^n$.

4) La fonction

$$\mathrm{orb} : V \longrightarrow F_{\mathrm{d}}(G, V), \quad v \longmapsto \mathrm{orb}_v : g \mapsto gv,$$

est linéaire injective et équivariante.

Démonstration. (1) Facile.

(2) On choisit une base de V.

(3) On utilise que $F_{\mathrm{d}}(G, \mathbb{K}) \simeq F(G, \mathbb{K})$.

(4) Linéaire : Facile. Injectivité : $\mathrm{orb}_v = 0$ implique que $v = \mathrm{orb}_v(e) = 0$. Équivariance : On veut montrer que $g\,\mathrm{orb}_v = \mathrm{orb}_{gv}$. Soit ainsi $x \in G$. On a

$$\begin{aligned} (g(\mathrm{orb}_v))\,(x) &= \mathrm{orb}_v(xg) \\ &= xg \cdot v \\ &= x(gv) \\ &= \mathrm{orb}_{gv}(x). \end{aligned}$$

□

Corollaire 124. *Soit G fini tel que $|G|$ est inversible dans $\mathbb{K}$. Soit S une rep. simple de dimension finie et soit*

$$F_{\mathrm{d}}(G, \mathbb{K}) \simeq S_1^{a_1} \oplus \cdots \oplus S_m^{a_m}$$

une décomposition isotypique. Alors $S \simeq S_i$ pour un certain i. En particulier, il n'existe que un nombre fini de classes d'isomorphisme de représentations simples de G.

Démonstration. Si $\dim S = s$, alors on a une fonction équivariante et injective :

$$\mathrm{orb} : S \longrightarrow F_{\mathrm{d}}(G)^n.$$

Clairement, une décomposition isotypique de $F_{\mathrm{d}}(G)$ est $S_1^{na_1} \oplus \cdots \oplus S_m^{na_m}$. Alors $S \simeq S_i$ pour un certain i par le Corollaire 110. □

Le produit tensoriel

Une façon très importante de construire des nouvelles représentations est le concept de produit tensoriel. La construction d'un produit tensoriel n'appartient pas vraiment à un cours de théorie des représentations, mais il s'agit d'une partie de l'algèbre linéaire qui demande plus de maturité pour être comprise par l'étudiant.

Soient[10] M, N et P des espaces vectoriels (sur le corps $\mathbb{K}$). On veut construire un $\mathbb{K}$-espace $M \otimes_{\mathbb{K}} N$ ayant la propriété que les applications $\mathbb{K}$-bilinéaires sont simplement les applications linéaires $M \otimes_{\mathbb{K}} N \to P$.

La construction emploie la notion d'espace libre sur un ensemble. Soit X un ensemble arbitraire. On note $\mathbb{K}^{(X)}$ le $\mathbb{K}$-espace des fonctions $X \to \mathbb{K}$ qui sont nulles *sauf pour un nombre fini d'éléments de* X. Une base de $\mathbb{K}^{(X)}$ est $\{\delta_x\}_{x \in X}$, où δ_x est la "fonction de Dirac" définie par $\delta_x(y) = 0$ si $y \neq x$ et $\delta_x(x) = 1$.

Proposition 125. *Soient M et N des $\mathbb{K}$-espaces vectoriels.*

(1) Il existe un $\mathbb{K}$-espace $M \otimes_{\mathbb{K}} N$ et une application bilinéaire

$$\bullet \otimes \bullet : M \oplus N \longrightarrow M \otimes_{\mathbb{K}} N, \qquad (x, y) \longmapsto x \otimes y$$

tels que :

(T1) *Si $\beta : M \oplus N \to P$ est bilinéaire, alors il existe une application* linéaire

$$\beta^* : M \otimes_{\mathbb{K}} N \longrightarrow P$$

telle que pour tout $x \in M$ et $y \in N$ on l'a

$$\boxed{\beta^*(x \otimes y) = \beta(x, y).}$$

Dit autrement, le diagramme suivant est commutatif :

$$\begin{tikzcd}
 & M \otimes N \arrow[d, dashed, "\beta^*"] \\
M \oplus N \arrow[ur, "\otimes"] \arrow[r, "\beta"'] & P
\end{tikzcd}$$

(T2) *Si $\beta^\dagger : M \otimes N \to P$ satisfait aussi $\beta^\dagger(x \otimes y) = \beta(x, y)$, alors $\beta^* = \beta^\dagger$.*

(G) *Si $\{x_i\}$ est une base de M et $\{y_j\}$ est une de N, alors $\{x_i \otimes y_j\}$ est une base de $M \otimes N$.*

(2) Si $\boxtimes : M \times N \to M \boxtimes N$ jouit de (T1) et (T2) alors il existe un unique *isomorphisme $u : M \otimes N \to M \boxtimes N$ tel que $u(x \otimes y) = u(x) \boxtimes u(y)$.*

Démonstration. (1) Dans $\mathbb{K}^{(M \times N)}$, on considère le sous-espace vectoriel R engendré par les ensembles suivants :

$$A_1 = \{\delta_{(x+x',y)} - \delta_{(x,y)} - \delta_{(x',y)} \ : \ x, x' \in M, \ y \in N\}.$$
$$A_2 = \{\delta_{(x,y+y')} - \delta_{(x,y)} - \delta_{(x,y+y')} \ : \ x \in M, \ y, y' \in N\}$$
$$L_1 = \{\delta_{(\lambda x,y)} - \lambda\delta_{(x,y)} \ : \ x \in M, \ y \in N, \ \lambda \in \mathbb{K}\}$$
$$L_2 = \{\delta_{(x,\mu y)} - \mu\delta_{(x,y)} \ : \ x \in M, \ y \in N, \ \mu \in \mathbb{K}\}$$

10. Cette partie est presque *copiée* du livre "Commutative Algebra" de M. Atiyah et I. G. Macdonald.

Dit autrement,

$$\begin{aligned}
\delta_{(x+x',y)} &\equiv \delta_{(x,y)} + \delta_{(x',y)} \mod R,\\
\delta_{(x,y+y')} &\equiv \delta_{(x,y)} + \delta_{(x,y')} \mod R,\\
\delta_{(\lambda x,y)} &\equiv \lambda\delta_{(x,y)} \mod R,\\
\delta_{(x,\mu y)} &\equiv \mu\delta_{(x,y)} \mod R.
\end{aligned}$$

On pose

$$\boxed{M \otimes_{\mathbb{K}} N = \mathbb{K}^{(M\times N)}/R}$$

ainsi que

$$\boxed{x \otimes y = \text{classe de } \delta_{(x,y)} \text{ modulo } R.}$$

On note que $\mathbb{K}^{(M\times N)}$ est *engendré librement* par $\{\delta_{(x,y)}\}_{(x,y)\in M\times N}$; donc $M \otimes_{\mathbb{K}} N$ est engendré par $x \otimes y$. En plus, pour tout x, x' de M, y, y' de N et λ, μ de $\mathbb{K}$, on a

$$\begin{aligned}
(x+x') \otimes y &= x \otimes y + x' \otimes y,\\
x \otimes (y+y') &= x \otimes y + x \otimes y',\\
(\lambda x) \otimes y &= \lambda \cdot (x \otimes y)\\
x \otimes (\mu y) &= \mu \cdot (x \otimes y),
\end{aligned}$$

et $\otimes$ est bilinéaire.
(T1) Soit $\beta : M \times N \to P$ bilinéaire. On définit une application *linéaire*

$$\beta^\circ : \mathbb{K}^{(M\times N)} \longrightarrow P$$

par $\beta^\circ(\delta_{(x,y)}) = \beta(x,y)$. Ceci est clairement possible car $\mathbb{K}^{(M\times N)}$ est libre de base $\{\delta_{(x,y)} : (x,y) \in \mathbb{K}^{(M\times N)}\}$. Or,

$$\begin{aligned}
\beta^\circ(\delta_{(x+x',y)} - \delta_{(x,y)} - \delta_{(x',y)}) &= \beta(x+x',y) - \beta(x,y) - \beta(x,y)\\
&= 0\\
\beta^\circ(\delta_{(x,y+y')} - \delta_{x,y} - \delta_{(x,y+y')}) &= \beta(x,y+y') - \beta(x,y) - \beta(x,y')\\
&= 0\\
&\text{etc.}
\end{aligned}$$

Donc $\beta^\circ(R) = 0$ et on arrive à la définition de $\beta^* : \mathbb{K}^{(M\times N)}/R \to P$. Comme la classe de $\delta_{(x,y)}$ en $\mathbb{K}^{(M\times N)}/R$ est $x \otimes y$, on voit en plus que

$$\beta^*(x \otimes y) = \beta(x,y).$$

(T2) Comme $M \otimes N$ est engendré par l'image de $\otimes : M \times N \to M \otimes N$, on déduit que $\beta^* : M \otimes N \to P$ est unique.

(G) On laisse au lecteur la preuve du fait que $\{x_i \otimes y_j\}$ est une famille génératrice et on montre qu'elle est libre. Soit ainsi

$$\sum_{\substack{i \in I' \\ j \in J'}} \lambda_{ij} \cdot (x_i \otimes y_j) = 0,$$

où I' et J' sont finis et λ_{ij} n'est jamais nul. Soient $k \in I'$ et $\ell \in J'$. On construit une application bilinéaire $\beta : M \times N \to \mathbb{K}$ telle que $\beta(x_i, y_j) = 0$ si $(i,j) \neq (k,\ell)$ et $\beta(x_k, y_\ell) = 1$, c'est-à-dire,

$$\beta\left(\sum_i a_i x_i\,,\, \sum_j b_j y_j\right) = a_k b_\ell.$$

(Ou encore, si $\{\phi_i\}$, resp. $\{\psi_j\}$, est la base duale à $\{x_i\}$, resp. à $\{y_j\}$, alors $\beta(x,y) = \phi_k(x) \cdot \psi_\ell(y)$.) Soit ainsi β^* comme dans **(T1)**. On a :

$$\begin{aligned}
0 &= \beta^*\left(\sum_{\substack{i \in I' \\ j \in J'}} \lambda_{ij} \cdot (x_i \otimes y_j)\right) \\
&= \sum \lambda_{ij} \beta^*(x_i \otimes y_j) \\
&= \sum \lambda_{ij} \beta(x_i, y_j) \\
&= \lambda_{k\ell}.
\end{aligned}$$

Une contradiction.

(2) Soit maintenant $\boxtimes : M \times N \to M \boxtimes N$ une autre fonction bilinéaire jouissant de (T1) et (T2). Ceci étant, il existe des fonctions linéaires $v : M \boxtimes N \to M \otimes N$ et $u : M \otimes N \to M \boxtimes N$ telles que

$$v(x \boxtimes y) = x \otimes y \quad \text{et} \quad u(x \otimes y) = x \boxtimes y.$$

(En plus, u et v sont uniques à avoir cette propriété.) Donc,

$$uv(x \boxtimes y) = x \boxtimes y \quad \text{et} \quad vu(x \otimes y) = x \otimes y.$$

Or, on sait déjà que la fonction $\mathrm{id} : M \boxtimes N \to M \otimes N$ est telle que $\mathrm{id}(x \boxtimes y) = x \boxtimes y$, et par unicité, il faut que $uv = \mathrm{id}$. De même, $vu = \mathrm{id}$.

□

Remarques 126. Souvent, l'étudiant se dit : alors $M \otimes N = M \oplus N$! Déjà, ceci est faux car si les dimensions sont finies, alors $\dim M \otimes N = \dim(M) \times \dim(N)$.

Exemple 127. Soient X et Y des ensembles finis. Si $\varphi : X \to \mathbb{K}$ et $\psi : Y \to \mathbb{K}$ sont des fonctions, on construit la fonction produit $X \times Y \to \mathbb{K}$ par $p(\varphi, \psi)(x,y) = \varphi(x)\psi(y)$.

Clairement : $p : F(X) \times F(Y) \longrightarrow F(X \times Y)$ est bilinéaire et obtient, via la propriété **T1** une application linéaire

$$p^* : F(X) \otimes F(Y) \longrightarrow F(X \times Y)$$

telle que $p^*(\varphi \otimes \psi) = p(\varphi, \psi)$. Or, $p^*(\delta_x \otimes \delta_y) = p(\delta_x, \delta_y)$ et $p(\delta_x, \delta_y)$ est simplement $\delta_{(x,y)}$. Donc, p^* est isomorphisme puisque l'image d'une base correspond à une base. (Un résultat similaire peut être donné pour des ensembles infinis : mais il faut remplacer $F(X, \mathbb{K})$ par $F_0(X, \mathbb{K})$, le sous espace des fonctions avec support fini.)

Exercice 128. Soit $C^0(\mathbb{R})$, resp. $C^0(\mathbb{R}^2)$, l'espace vectoriel des fonctions continues $\mathbb{R} \to \mathbb{R}$, resp. de $\mathbb{R}^2 \to \mathbb{R}$. On considère l'application bilinéaire évidente $m : C^0(\mathbb{R}) \times C^0(\mathbb{R}) \to C^0(\mathbb{R}^2)$ définie par $m(\varphi, \psi)(x, y) = \varphi(x)\psi(y)$. L'application $m^* : C^0(\mathbb{R}) \otimes_{\mathbb{R}} C^0(\mathbb{R}) \to C^0(\mathbb{R}^2)$ est-elle un isomorphisme ?

Soient U et V des reps d'un groupe G. On considère alors $\beta_g : U \times V \to U \otimes V$ définie par $\beta_g(u, v) = gu \otimes gv$; il s'agit d'une application bilinéaire $U \times V \to U \otimes V$ et ainsi est de la forme

$$\beta_g^*(u \otimes v) = \beta_g(u, v)$$

pour une certaine $\beta_g : U \otimes V \to U \otimes V$ *linéaire*. On montre que $\beta_{gh}^* = \beta_g^* \circ \beta_h^*$. Pour chaque $u \in U$ et $v \in V$, on a

$$\begin{aligned} \beta_{gh}(u, v) &= gh(u) \otimes gh(v) \\ &= \beta_g(hu, hv) \\ &= \beta_g^*(hu \otimes hv) \\ &= \beta_g^*(\beta_h^*(u \otimes v)) \\ &= \beta_g^* \circ \beta_h^*(u \otimes v). \end{aligned}$$

Donc, $\beta_g^* \circ \beta_h^*$ satisfait la propriété **(T1)** caractérisant β_{gh}^*, d'où, par **(T2)**, on a

$$\beta_{gh}^* = \beta_g^* \circ \beta_h^*.$$

Ceci montre que $g \mapsto \beta_g^*$ définit un morphisme de groupes $G \to \mathrm{GL}(U \otimes V)$.

Définition 129. La représentation de G sur $U \otimes V$ construite ainsi est appelée la rep. produit tensoriel. Si $\varrho : G \to \mathrm{GL}(U)$ et $\sigma : G \to \mathrm{GL}(V)$ sont les morphismes correspondants, on trouvera utile d'écrire aussi $\varrho \otimes \sigma$ pour parler de la rep. produit tensoriel.

Le produit tensoriel permet de donner une nouvelle interprétation à la structure de groupe de l'ensemble $\mathbb{X}(G)$ (voir p. 35).

Exemple 130. Si (L, θ) et (L', θ') sont des caractères de G, alors $L \otimes L'$ est aussi un caractère car $\dim L \otimes L' = 1 \cdot 1$. Puis, $\ell \in L$ et $\ell' \in L'$ sont des bases telles que $\theta(g)\ell = \theta_g \ell$ et $\theta(g)\ell' = \theta'_g \ell'$, alors $(\theta \otimes \theta')(g)\ell \otimes \ell' = \theta_g \ell \otimes \theta'_g \ell'$, et ce dernier est $\theta_g \theta'_g \cdot (\ell \otimes \ell')$ car $- \otimes - : L \times L' \to L \otimes L'$ est bilinéaire. Ceci montre que la structure de groupe sur $\mathbb{X}(G)$ construite précédemment à l'aide de d'une bijection $\mathbb{X}(G) \to \mathrm{Hom}(G, \mathbb{K}^*)$ est intrinsèque.

Cours 10

(02 avril 2021).

Une propriété importante du produit tensoriel qui sera employée dans la suite est la suivante. Soient U et V des espaces vectoriels. Pour chaque couple[11] $(\check{u}, v) \in \check{U} \times V$, on obtient une application linéaire

$$c_{\check{u},v} : U \to V, \quad u \mapsto \check{u}(u)v.$$

Clairement, $c : \check{U} \times V \to \mathrm{Hom}(U, V)$ est bilinéaire. Soit $c^* : \check{U} \otimes V \to \mathrm{Hom}(U, V)$ ainsi définie.

Lemme 131. *Si U ou V sont de dimension finie, alors $c : \check{U} \otimes V \to \mathrm{Hom}(U, V)$ est un isomorphisme.*

Éléments de preuve. Soient $\{u_i \,:\, i \in I\}$ et $\{v_j \,:\, j \in J\}$ des bases de U et V. Soit $\{\check{u}_i\}$ la base duale : $\check{u}_i(u_{i'}) = 0$ si $i' \neq i$ et 1 autrement. Soit $c_{ij} : U \to V$ définie par $c_{\check{u}_i, v_j}$. On montre que $\{c_{ij}\}$ est une base de $\mathrm{Hom}(U, V)$. □

Caractères (de Frobenius)

On ne parlera maintenant que des représentations complexes de dimension finie d'un groupe fini G. L'idée fondamentale de Frobenius est la suivante : Soit $\varrho : G \to \mathrm{GL}(V)$ une rep. Étudier toutes les matrices $\{\varrho(g) \,:\, g \in G\}$ est très compliqué et on peut tirer beaucoup d'information en passant à l'étude des nombres complexes $\mathrm{Tr}(\varrho(g))$.

Définition 132. Soit (V, ϱ) une rep de G. On défini son caractère (de Frobenius) χ_V comme étant la fonction $g \mapsto \mathrm{Tr}(\varrho(g))$.

Si V est une rep, on note que χ_V satisfait

$$\chi_V(xgx^{-1}) = \chi_V(g)$$

pour tout $g, x \in G$. De plus on note que pour $g \in G$, l'automorphisme $g_V : V \to V$ satisfait $g_V^n = \mathrm{id}$ pour un certain n et par conséquent le polynôme minimal divise $\lambda^n - 1 = \prod_{k=0}^{n}(\lambda - e^{2\pi i k/n})$. Ceci implique que g_V *est diagonalisable et que ses valeurs propres sont des racines de l'unité.*

Lemme 133. *Soit V et W des représentations de G. Alors*

(1) $\chi_{V \oplus W} = \chi_V + \chi_W$.

11. Pour éviter des confusions, on écrira $\check{U}$ pour le dual de U.

(2) $\chi_{V\otimes W} = \chi_V \cdot \chi_W$.

(3) $\chi_{V^*} = \overline{\chi}_V$.

Démonstration. On fixe $g \in G$ et on note $\lambda_1, \ldots, \lambda_m$ et $\mu_1, \ldots, \mu_n$ les valeurs propres de g_V et g_W. Alors les valeurs propres de $g_{V\oplus W}$ sont $\{\lambda_j, \mu_k\}$. Donc, $\lambda_1 + \cdots + \lambda_m + \mu_1 + \cdots + \mu_n = \chi_V(g) + \chi_W(g)$. De même, les valeurs propres de $g_{V\otimes W}$ sont $\{\lambda_j\mu_k : 1 \leqslant j \leqslant m, 1 \leqslant k \leqslant n\}$, et donc leur somme est $\sum_{j,k} \lambda_j\mu_k$. Or, ceci n'est rien d'autre que $(\sum_j \lambda_j)(\sum_k \mu_k) = \chi_V(g)\chi_W(g)$. Finalement, les valeurs propres de g_{V^*} sont $\{\lambda_j^{-1}\}$, et comme chaque λ_j est une racine de l'unité, on a $\lambda_j^{-1} = \overline{\lambda}_j$. □

Soit (L, θ) une rep. de dimension 1. Alors il est clair que la fonction θ_g définie à la page 35 est le caractère de L. Par contre, si $\dim V \geqslant 2$, le lien entre χ_V, son caractère, n'a pas un lien explicite avec un morphisme $G \to \mathbb{C}^*$.

Définition 134. Soit $\varphi, \psi \in F(G, \mathbb{C})$. On écrit

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g\in G} \varphi(g)\overline{\psi(g)}.$$

Le lecteur n'aura aucune difficulté à vérifier :

Exercice 135. La fonction $\langle -, - \rangle$ est un produit hermitien positif défini sur $F(G, \mathbb{C})$.

Théorème 136 (Orthogonalité)**.** *Soient S et T simples. Alors*

$$\langle \chi_S, \chi_T \rangle = \begin{cases} 1, & \text{si } S \simeq T, \\ 0 & \text{sinon.} \end{cases}$$

C'est une conséquence du

Lemme 137. *Soit V une rep de G. Alors $\langle \chi_V, 1_G \rangle = \dim V^G$.*

Démonstration. Soit M la moyenne :

$$M = \frac{1}{|G|} \sum_{g\in G} g_V \,:\, V \longrightarrow V.$$

On se rappelle que M est un projecteur sur V^G. Donc, $\dim V^G = \mathrm{Tr}(M)$ (cela suit de la décomposition $V = V^G \oplus \mathrm{Ker}(M)$ et du fait que pour calculer la trace, toutes les bases sont bonnes). Mais

$$\begin{aligned} \mathrm{Tr}(M) &= \frac{1}{|G|} \sum_{g\in G} \mathrm{Tr}(g_V) \\ &= \frac{1}{|G|} \sum_{g\in G} \chi_V(g) \\ &= \langle \chi_V, 1_G \rangle. \end{aligned}$$

□

Preuve de l'orthogonalité. Soit $H = \mathrm{Hom}(S,T)$. On sait que H^G est simplement le sous-espace des morphismes équivariants. Ensuite, le Lemme de Schur garantit que

$$\dim H^G = \begin{cases} 1 & \text{si } S \simeq T, \\ 0 & \text{autrement.} \end{cases}$$

D'après le Lemme 137, on sait que $\dim H^G = \langle \chi_H, 1_G \rangle$. Or, mais en tant que reps, on a $H \simeq S^* \otimes T$ (voir le Lemme 131), d'où

$$\begin{aligned} \langle \chi_H, 1_G \rangle &= \langle \chi_{S^* \otimes T}, 1_G \rangle \\ &= \frac{1}{|G|} \sum_g \chi_{S^* \otimes T}(g) \\ &= \frac{1}{|G|} \sum_g \overline{\chi_S(g)} \chi_T(g) \\ &= \langle \chi_T, \chi_S \rangle. \end{aligned}$$

□

Pour la suite, soient

$$\boxed{\begin{array}{c} S_1, \ldots, S_r \text{ des reps simples, non-isomorphes deux-à-deux} \\ \text{telles que chaque rep simple soit isomorphe à une de ces dernières.} \end{array}}$$

(Il en a que un nombre fini. Pourquoi ?) On écrira χ_i au lieu de χ_{S_i}.

Théorème 138 (Calcul de la multiplicité)**.** *Soit V une rep de G. Alors la multiplicité de S_i en V se calcule de ainsi :*

$$(V : S_i) = \langle \chi_V, \chi_i \rangle.$$

Démonstration. On pose $V \simeq S_1^{m_1} \oplus \cdots \oplus S_r^{m_r}$. Alors $\chi_V = \sum m_i \chi_i$ et donc, l'orthogonalité donne $m_i = \langle \chi_V, \chi_i \rangle$. □

Le résultat suivant—qui est complètement spectaculaire !—suit sans effort :

Corollaire 139. *Soient V et W des reps. Si $\chi_V = \chi_W$, alors $V \simeq W$.*

Démonstration. On a $V \simeq S_1^{m_1} \oplus \cdots S_r^{m_r}$ et $W \simeq S_1^{n_1} \oplus \cdots S_r^{n_r}$ avec m_j, n_j des entiers positifs. Donc $\sum_j m_j \chi_j = \chi_V = \chi_W = \sum_j n_j \chi_j$. Par orthogonalité, $m_j = n_j$. □

Corollaire 140. *Soit V une rep. Alors V est simple si et seulement si $\|\chi_V\|^2 = \langle \chi_V, \chi_V \rangle = 1$.*

Démonstration. Si V est simple, alors le resultat est partie de la relation d'orthogonalité. On suppose $\|\chi_V\|^2 = 1$. Si $V \simeq \bigoplus_i S_i^{m_i}$, alors $\chi_V = \sum_i m_i \chi_i$. Donc, $1 = \|\chi_V\|^2 = \sum m_i^2$. Il suit que pour un certain j, on a $m_j = 1$ et $m_i = 0$ si $i \neq j$. Dit autrement, $V \simeq S_j$. □

On étudie les caractères des reps de permutation.

Théorème 141 (Le caractère des reps de permutation)**.** *Soit X un G-ensemble fini ; on écrira χ_X au lieu de $\chi_{F(X,\mathbb{C})}$.*

1. *Pour $g \in G$, $\chi_X(g) = |\mathrm{Fix}(g)|$.*
2. *Le nombre d'orbites de G est égal la multiplicité de $\mathbb{1}$ dans $F(X, \mathbb{C})$. Ce dernier est aussi $\langle \chi_X, 1_G \rangle$.*
3. *On a la formule de Burnside :*

$$\#orbites = \frac{1}{|G|} \sum_g |\mathrm{Fix}(g)|.$$

Démonstration. 1) Pour $g \in G$, on écrit

$$g(\delta_y) = \sum_{x \in X} g_{xy} \delta_x.$$

Or, mais $g(\delta_y) = \delta_{gy}$. On voit que

$$g_{xy} = \begin{cases} 1 & \text{si } gy = x, \\ 0 & \text{autrement.} \end{cases}$$

Donc, $g_{xx} = 1$ si $gx = x$ et $g_{xx} = 0$ sinon. La formule en découle.

2) On suppose que G agit transitivement sur X. Soit $\varphi : X \to \mathbb{C}$ une fonctions G-invariante, c'est-à-dire, $g\varphi = \varphi$ pour tout $g \in G$. Alors, $\varphi(g^{-1}x) = \varphi(x)$; par conséquent, φ est constante. On en déduit $\dim F(X)^G = 1$. En général, soient $X_1, \ldots, X_q$ les orbites. On voit facilement que

$$R : F(X) \longrightarrow F(X_1) \times \cdots \times F(X_q)$$

$$\varphi \longmapsto (\varphi|_{X_1}, \ldots, \varphi|_{X_q})$$

est un isomorphisme d'espaces vectoriels. De plus, R est clairement G-équivariante. Il suit que $\dim F(X)^G = q$, car $\dim F(X_i)^G = 1$. Finalement, la multiplicité de $\mathbb{1}$ n'est rien d'autre que $\dim F(X)^G$.

3) On a

$$\begin{aligned} \#\text{orbites} &= \langle \chi_X, 1 \rangle \\ &= \frac{1}{|G|} \sum_g \chi_X(g) \\ &= \frac{1}{|G|} \sum_g \mathrm{Fix}(g). \end{aligned}$$

$\square$

On écrit χ_{reg} pour le caractère de la rep. régulière (à gauche).

Corollaire 142. *Les affirmations suivantes sont vraies :*

1) Soit V une rep. Alors $\dim V = \langle \chi_{\text{reg}}, \chi_V \rangle$.

2) Si

$$F(G, \mathbb{C}) \simeq S_1^{m_1} \oplus \cdots \oplus S_r^{m_r},$$

alors $m_i = \dim S_i$.

3) On a

$$\boxed{\sum_{i=1}^{r} (\dim S_i)^2 = |G|.}$$

Démonstration. 1) Par le Théorème 141, on a

$$\chi_{\text{reg}}(g) = \begin{cases} 0 & \text{si } g \neq e, \\ |G| & \text{si } g = e. \end{cases}$$

Il suit que $\langle \chi_{\text{reg}}, \chi_V \rangle = \overline{\chi_V(e)} = \dim V$.

2) On sait que la multiplicité de S_i dans $F(G, \mathbb{C})$ est $\langle \chi_{\text{reg}}, \chi_i \rangle$. Grâce à (1), le produit interne $\langle \chi_{\text{reg}}, \chi_i \rangle$ vaut $\dim S_i$.

3) On fait la somme des dimensions. $\square$

Cours 11

(09 avril 2021).

Le nombre de représentations simples et les classes de conjugaison

On rappelle les notations et conventions pour cette partie : G est fini et une rep. de G est toujours une rep sur un $\mathbb{C}$-espace vectoriel de dimension finie. De plus, on fixe des reps simples

$$S_1, \dots, S_r$$

telles que chaque rep. simple soit isomorphe à *seulement une* parmi $\{S_i\}$. On écrira χ_i au lieu de χ_{S_i}.

On souhaite étudier le nombre r. Pour cela, on introduit :

Définition 143. Une fonction $\varphi : G \to \mathbb{C}$ est *centrale* si $\varphi(ghg^{-1}) = \varphi(h)$ pour tout h et g. Le sous-espace vectoriel de $F(G, \mathbb{C})$ formé par les fonctions centrales sera noté $F^{\text{cent}}(G, \mathbb{C})$.

Remarques 144. On montre facilement que $\varphi : G \to \mathbb{C}$ est centrale si et seulement si

$$\boxed{\varphi(gh) = \varphi(hg)}$$

pour tout $g, h \in G$.

Les caractères sont l'exemple le plus évident de fonctions centrales. Notre objectif maintenant c'est de montrer qu'ils sont essentiellement les seuls.

Théorème 145. *Les fonctions $\{\chi_i\}_{i=1}^r$ forment une base de $F^{\text{cent}}(G, \mathbb{C})$.*

La preuve fait appel à :

Lemme 146. *Soit $\varphi \in F^{\text{cent}}(G)$. Pour chaque rep. V, on considère la moyenne pondérée :*

$$M_\varphi^V : V \longrightarrow V, \quad v \longmapsto \frac{1}{|G|} \sum_g \varphi(g) \cdot g(v).$$

Alors

(1) M_φ^V est equivariante.

(2) Si $U \subset V$ est G-invariant, alors pour tout $u \in U$ on a $M_\varphi^U(u) = M_\varphi^V(u)$.

(3) Si V est simple, alors

$$\boxed{M_\varphi^V = \frac{\langle \varphi, \overline{\chi}_V \rangle}{\dim V} \operatorname{id}_V.}$$

Démonstration. La preuve de (2) est simple ; on se concentrera sur (1) et (3).
(1) On a

$$\begin{aligned} M_\varphi^V(hv) &= \frac{1}{|G|}\sum_g \varphi(g)\cdot gh(v) \\ &\overset{g'=gh}{=} \frac{1}{|G|}\sum_{g'} \varphi(g'h^{-1})\cdot g'v \\ &= \frac{1}{|G|}\sum_{g'} \varphi(h^{-1}g')\cdot g'v \\ &\overset{g=h^{-1}g'}{=} \frac{1}{|G|}\sum_{g} \varphi(g)\cdot hgv \\ &= h\left(M_\varphi^V(v)\right). \end{aligned}$$

(3) Si V est simple, alors le Lemme de Schur dit que $M_\varphi^V = \lambda\mathrm{id}$. Comme

$$\begin{aligned} \operatorname{Tr} M_\varphi^V &= \frac{1}{|G|}\sum_g \varphi(g)\cdot\chi_V(g) \\ &= \langle\varphi,\overline{\chi}_V\rangle, \end{aligned}$$

on déduit $\lambda\dim V = \langle\varphi,\overline{\chi}_V\rangle$. $\square$

Démonstration du Théorème 145. On montre qu'une fonction centrale qui est orthogonale à chaque χ_i est nulle. Soit ainsi $\varphi\in F^{\mathrm{cent}}$ telle que $\langle\varphi,\chi_i\rangle = 0$ pour tout i.

D'après le Lemme 146-(3),

$$M_{\overline{\varphi}}^{S_i} = \frac{\langle\overline{\varphi},\overline{\chi}_i\rangle}{\dim V}\,\mathrm{id}_{S_i}$$

et par conséquent $M_{\overline{\varphi}}^{S_i} = 0$.

Soit V une rep arbitraire et $S\subset V$ une sous-rep simple. Donc,

$$\begin{aligned} 0 &= M_{\overline{\varphi}}^S(\varphi)(v) \\ &= M_{\overline{\varphi}}^V(v) \end{aligned}$$

pour tout $v\in S$. Comme V est engendré par ses sous-représentations simples, on déduit que *pour chaque rep.* V l'endomorphisme $M_{\overline{\varphi}}^V$ est nul.

On applique ce résultat à la rep régulière :

$$\begin{aligned} 0 &= M_{\overline{\varphi}}^{F(G)}(\delta_e) \\ &= \frac{1}{|G|}\sum_g \overline{\varphi}(g)\delta_g, \end{aligned}$$

et on déduit que $\overline{\varphi}(g) = 0$ pour chaque g puisque $\{\delta_g\}_{g\in G}$ est une famille libre. $\square$

Dans la suite, $\mathrm{Cl}(G)$ note l'ensemble des classes de conjugaison de G.

Corollaire 147.

$$\boxed{r = |\mathrm{Cl}(G)|.}$$

Démonstration. Soit C une classe de conjugaison et δ_C sa fonction caractéristique : $\delta_C(g) = 1$ si $g \in C$ et $\delta_C(g) = 0$ sinon. Il est clair que $\{\delta_C : C \in \mathrm{Cl}(G)\}$ est une base de $F^{\mathrm{cent}}(G, \mathbb{C})$ et le Théorème 145 nous donne le résultat. $\square$

La méthode pour prouver le Lemme 146 a une conséquence importante qu'on isole ici. (Il s'agit d'une amplification du Théorème 113.)

Proposition 148. *Soit V une rep. et $V = S_1^{m_1} \oplus \cdots \oplus S_r^{m_r}$. Soit $i \in \{1, \ldots, r\}$. Alors*

$$(\dim S_i) \cdot M^V_{\overline{\chi}_i} : V \longrightarrow V$$

est le projecteur sur $S_i^{m_i}$ orthogonal à $\bigoplus_{j \neq i} S_j^{m_j}$.

Démonstration. Si $v \in S_j$ alors le Lemme 146 montre que

$$\begin{aligned} M^V_{\overline{\chi}_i}(v) &= M^{S_j}_{\overline{\chi}_i}(v) \\ &= \frac{\langle \overline{\chi}_i, \overline{\chi}_j \rangle}{\dim S_j} v \\ &= \frac{\overline{\langle \chi_i, \chi_j \rangle}}{\dim S_j} v. \end{aligned}$$

Donc, si $i \neq j$, on voit que $M^V_{\overline{\chi}_i}(v) = 0$. Ensuite, si $v \in S_i$, alors

$$M^V_{\overline{\chi}_i}(v) = \frac{1}{\dim S_i} v.$$

Le résultat suit. $\square$

Tables de caractères

Les notations sont comme avant. En plus, on pose

$$\boxed{\mathrm{Cl}(G) = \{C_1, \ldots, C_r\}.}$$

On note que si $C \in \mathrm{Cl}(G)$ et V est une rep, alors $\chi_V(g) = \chi_V(g')$ pour n'importe quel couple g, g' de C. Ceci étant, on écrit $\chi_V(C)$ pour la valeur de χ_V sur un élément quelconque de C.

La matrice suivante est la *table de caractères* de G.

	C_1	$\cdots$	C_r
χ_1	$\chi_1(C_1)$	$\cdots$	$\chi_1(C_r)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
χ_r	$\cdots$		$\chi_r(C_r)$

En utilisant les relations d'orthogonalité, on arrive à

Lemme 149 (Orthogonalité des colonnes)**.** *Pour chaque couple $i, j \in \{1, \ldots, r\}$, on écrit $\chi_{ij} = \chi_i(C_j)$. Alors*

$$\sum_{k=1}^{r} \chi_{ki}\overline{\chi_{kj}} = \begin{cases} 0, & si\ i \neq j, \\ |G|/|C_i|, & si\ i = j \end{cases}$$

Dit autrement, si $X = (\chi_{ij})$, alors

$$X^t \cdot \overline{X} = \operatorname{diag}\left(\frac{|G|}{|C_1|}, \ldots, \frac{|G|}{|C_r|}\right).$$

Démonstration. D'après les relations d'orthogonalité, on sait que

$$\sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \begin{cases} 0, & \text{si } i \neq j, \\ |G|, & \text{si } i = j \end{cases}$$

Or,

$$\begin{aligned} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} &= \sum_{k=1}^{r} \sum_{g \in C_k} \chi_i(g)\overline{\chi_j(g)} \\ &= \sum_{k=1}^{r} |C_k| \cdot \chi_{ik}\overline{\chi_{jk}}. \end{aligned}$$

Soient ainsi $D = \operatorname{diag}(|C_1|, \ldots, |C_r|)$ et $X = (\chi_{ij})$. On voit que $XD\overline{X}^t = |G| \cdot \mathrm{Id}$. Par conséquent, $X^{-1} = (D/|G|) \cdot \overline{X}^t$. Donc, $(D/|G|) \cdot \overline{X}^t \cdot X = \mathrm{Id}$, d'où $\overline{X}^t \cdot X = |G| \cdot D^{-1}$. Ce qui est la formule souhaitée après conjugaison. $\square$

Exemple 150. Soit $G = \mathscr{S}_3$. Soient $C_1 = \{e\}$, $C_2 = \{(12), (13), (23)\}$ et $C_3 = \{(123), (132)\}$ les classes de conjugaison. Soit $S_1 = \mathbb{1}$. Soit $\varepsilon : \mathscr{S}_3 \to \mathbb{C}^*$ la signature vue comme morphisme de groupes : ceci nous donne une rep. simple S_2 dimension 1. Nous avons encore une autre rep simple S_3 telle que $6 = 1^2 + 1^2 + (\dim S_3)^2$. Par conséquent, $\dim S_3 = 2$; en particulier $\chi_3(e) = 2$. Voici la table à présent :

	C_1	C_2	C_3
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	α	β

En utilisant l'orthogonalité des colonnes, on voit que $\alpha = 0$ et $\beta = -1$. On note ici que malgré le fait que χ_3 soit numériquement déterminée, on n'a pas beaucoup d'information à propos de S_3.

Exemple 151. Soit $G = \mathscr{D}_{10}$. On pose $C_1 = \{e\}$. Puis, on note que $\{S, RS, \ldots, R^4 S\}$ forme une seule classe de conjugaison car $R^i S \cdot S \cdot S R^{-i} = R^{2i} S$ et chaque R^j est de la forme R^{2i} car $\langle R \rangle \simeq \mathbb{Z}/5$. On note cette classe C_2. Ensuite, $R^i \cdot R^j \cdot R^{-i} = R^j$ et $R^i S \cdot R^j \cdot S R^{-i} = R^{-j}$. On conclut que R^i et R^{-i} sont dans la même classe. Soient

$$C_3 = \{R, R^4\}, C_4 = \{R^2, R^3\}.$$

Donc, G possède 4 classes de conjugaison et par conséquent 4 reps simples. Soit χ_1 le caractère trivial. Puis, d'après l'Exemple 118, $[\mathscr{D}_{10}, \mathscr{D}_{10}] = \langle R^2 \rangle = \langle R \rangle$ et $\mathscr{D}_{10}^{\mathrm{ab}} \simeq \mathbb{Z}/2$. On obtient ainsi une rep non-triviale de dimension 1 : on note χ_2 son caractère. Comme $10 = 1 + 1 + (\dim S_3)^2 + (\dim S_4)^2$, on voit que $\dim S_3 = \dim S_4 = 2$. Or, on connait déjà une rep simple de dimension 2, qui est la standard. Elle est donnée par

$$R \longmapsto \begin{pmatrix} \cos\frac{2\pi}{5} & -\sin\frac{2\pi}{5} \\ \sin\frac{2\pi}{5} & \cos\frac{2\pi}{5} \end{pmatrix}, \qquad S \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

On note χ_3 son caractère. Donc,

	C_1	C_2	C_3	C_4
χ_1	1	1	1	1
χ_2	1	-1	1	1
χ_3	2	0	$2\cos\frac{2\pi}{5}$	$2\cos\frac{4\pi}{5}$
χ_4	2	α	β	γ

On utilise l'orthogonalité des colonnes pour conclure que $\alpha = 0$, $\beta = -1 - 2\cos\frac{2\pi}{5}$ et $\gamma = -1 - \cos\frac{4\pi}{5}$. (En utilisant les racines de l'unité on voit que $\beta = 2\cos\frac{4\pi}{5}$ et $\gamma = 2\cos\frac{2\pi}{5}$.)

Exemple 152. On note que la connaissance d'un caractère ne conduit pas immédiatement à une description de la rep y attachée. En effet, d'après l'Exemple 150, on connait les caractères de $\mathscr{S}_3$, mais on n'a pas beaucoup plus d'informations sur la rep S_3 dont le caractères est χ_3. Dans ce cas précis, voici comment la construire.

Le groupe $\mathscr{S}_3$ agit sur $X = \{1, 2, 3\}$ et on obtient ainsi une rep de G dans $F(X)$; soit $I(X) = \{\varphi : G \to \mathbb{C} : \sum_{x \in X} \varphi(x) = 0\}$. Clairement $I(X) \subset F(X)$ est invariant et de dimension deux. Une base de $I(X)$ est $u := \delta_1 - \delta_2$ et $v = \delta_2 - \delta_3$. Dans cette base, on a

$$(12) \longmapsto \begin{pmatrix} -1 & 1 \\ & 1 \end{pmatrix}$$

$$(123) \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

Si C_1, C_2 et C_3 sont comme dans l'Exemple 150, alors

$$\chi_{I(X)}(C_1, C_2, C_3) = (2, 0, -1).$$

D'après la table de caractères, Exemple 150, $I(X)$ est la seule rep. simple de dimension > 1.

Les cours suivants on été proposés comme complément dans les années précédents.

Cours 11 (moitié) et cours 12

(5 et 12 Avril 2019).

Induction

[12] Comme avant, G note un groupe fini. Toutes représentations sont complexes et de dimension finie.

Si W est un $\mathbb{C}$-espace, on obtient par oubli de structure une structure de $\mathbb{R}$-espace sur W : elle s'appelle la *restriction de scalaires*. Cette idée a déjà apparu dans l'étude des représentations : des reps d'un groupe donnent lieu à des reps d'un sous-groupe naturellement.

Par contre, si V est un $\mathbb{R}$-espace, il n'est pas en général possible de lui donner une structure de $\mathbb{C}$-espace. Or, si iV note un autre copie de V, alors $W = V \oplus iV$ vient avec une structure de $\mathbb{C}$-espace : $(a+ib)\cdot(\boldsymbol{v}+i\boldsymbol{w}) = a\boldsymbol{v} - b\boldsymbol{w} + i(a\boldsymbol{w}+b\boldsymbol{v})$. En plus, il est clair que si $V = \mathbb{R}^n$, alors $V \oplus iV$ n'est rien d'autre que $\mathbb{C}^n$. Cette idée apparaît également en théorie des représentations. [13]

Dorénavant, H note un sous-groupe de G et on écrit $G/H = \{tH_1, \ldots, t_nH\}$. Soit W une rep. de H.

Lemme 153. *On note $F(G,W)$ l'espace des fonctions $G \to W$.*

1. *La fonction*

$$H \times F(G,W) \longrightarrow F(G,W), \qquad (h,\varphi) \longmapsto (\ x \mapsto h(\varphi(xh)\ ).$$

   est une rep de H.

2. *La fonction*

$$G \times F(G,W) \longrightarrow F(G,W), \qquad (g,\varphi) \longmapsto (\ x \mapsto \varphi(g^{-1}x)\ ).$$

   est une rep de G.

3. *Le sous-espace $F(G,W)^H$ est invariant par l'action de G induite dans l'item (2).*

Les vérifications sont triviales (une fois qu'on sait comment fixer les choses). En plus, on note que

$$F(G,W)^H = \left\{ \varphi : G \to W \ : \ \begin{array}{c} \text{pour tout } g \in G \text{ et } h \in H, \\ \text{on a } \varphi(gh) = h^{-1}\varphi(g) \end{array} \right\}.$$

12. Dans cette partie j'ai suivi les notations et conventions du livre “Representations of algebraic groups” de Jantzen. Elles diffèrent des conventions de [Dat].

13. En fait, elle apparaît *beaucoup* en mathématiques et son nom technique est “adjonction catégorique.”

Il suit ainsi que

$$\mathrm{Ind}(W) \longrightarrow W^n, \qquad \varphi \longmapsto (\varphi(t_1), \ldots, \varphi(t_n))$$

est une application injective et $\dim \mathrm{Ind}(W) \leqslant n \dim W$.

Définition 154. La représentation $F(G,W)^H$ est dite la rep. induite et sera notée par $\mathrm{Ind}_H^G(W)$.

Exemple 155. Si $W = \mathbb{1}$, alors $\mathrm{Ind} = F(G/H, \mathbb{C})$. En effet, une fonction $\varphi : G \to W$ appartient à $\mathrm{Ind}(W)$ si et seulement si $\varphi(gh) = \varphi(g)$, et donc $\mathrm{Ind}(W)$ est le sous-espace des fonctions constantes sur les classes gH, qui est $F(G/H, \mathbb{C})$. On note que $\dim \mathrm{Ind}(W) = n$.

Exemple 156. Soit $G = D_{2n}$ et $H = \langle R \rangle$. Comme $H \simeq \mathbb{Z}/n$, on obtient une rep. de H en $\mathbb{C}$ en posant $R(1) = \omega$, avec $\omega = e^{2\pi i/n}$. On note que la fonction $\delta : G \to \mathbb{C}$ définie par

$$\delta(R^k) = \omega^{-k}, \quad \text{et} \quad \delta(R^k S) = 0$$

appartient à $\mathrm{Ind}(\mathbb{C})$. (C'est la fonction "fonction indicatrice" de la classe H.) Soit $\delta' := S(\delta)$. Il suit que

$$\delta'(R^k) = 0 \quad \text{et} \quad \delta'(R^k S) = \omega^k;$$

en particulier, $\delta' \notin \mathbb{C}\delta$. Il suit que $\{\delta, \delta'\}$ est une base de $\mathrm{Ind}(\mathbb{C})$. On a

$$R(\delta)(R^k) = \delta(R^{-1+k}) = \omega^{1-k} \quad \text{et} \quad R(\delta)(R^k S) = \delta(R^{-1+k} S) = 0,$$

d'où $R(\delta) = \omega\delta$. Puis,

$$R(\delta')(R^k) = \delta'(R^{k-1}) = 0 \quad \text{et} \quad R(\delta')(R^k S) = \delta'(R^{k-1} S) = \delta(R^{1-k}) = \omega^{k-1},$$

d'où $R(\delta') = \omega^{-1}\delta'$. Dit autrement, a matrice de R dans la base $\{\delta, \delta'\}$ est

$$\begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}.$$

De façon analogue, la matrice de S dans la base $\{\delta, \delta'\}$ est

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Par conséquent, $\mathrm{Ind}(\mathbb{C})$ est isomorphe à la rep. standard de G (Exercice).

Le dernier exemple montre que la clé pour bien comprendre l'induite est d'employer "la fonction caractéristique" de H et ses images par les éléments $t_1, \ldots, t_n$. Voici cette idée en généralité :

Lemma. 1. Pour chaque $w \in W$, on définit $\delta_w : G \to W$ par

$$\delta_w(g) = \begin{cases} g^{-1}w, & \text{si } g \in H, \\ 0, & \text{si } g \notin H. \end{cases}$$

Alors $\delta_w \in \mathrm{Ind}_H^G(W)$ et l'application

$$\delta : W \longrightarrow \mathrm{Ind}_H^G(W)$$

est H-équivariante. (δ_w est l'unique fonction de $\mathrm{Ind}(W)$ qui vaut w sur e et 0 sur le complémentaire $G - H$.)

2. Pour chaque $\varphi \in \mathrm{Ind}(W)$ on a

$$\varphi(g) = \sum_{j=1}^{n} \delta_{\varphi(t_j)}(t_j^{-1}g).$$

3. Soit t_jW l'image de $\delta(W)$ par $t_j : \mathrm{Ind}(W) \to \mathrm{Ind}(W)$. Alors

$$\boxed{\mathrm{Ind}(W) = \bigoplus_{j=1}^{n} t_jW.}$$

En particulier,

$$\dim \mathrm{Ind}(W) = [G : H] \cdot \dim W$$

On démontre

Lemme 157. *1. Pour chaque $w \in W$, on définit $\delta_w : G \to W$ par*

$$\delta_w(g) = \begin{cases} g^{-1}w, & \textit{si } g \in H, \\ 0, & \textit{si } g \notin H. \end{cases}$$

Alors $\delta_w \in \mathrm{Ind}_H^G(W)$ et l'application

$$\delta : W \longrightarrow \mathrm{Ind}_H^G(W)$$

est H-équivariante et injective. (δ_w est l'unique fonction de $\mathrm{Ind}(W)$ qui vaut w sur e et 0 sur le complémentaire $G - H$.)

2. Pour chaque $\varphi \in \mathrm{Ind}(W)$ on a

$$\varphi(g) = \sum_{j=1}^{n} \delta_{\varphi(t_j)}(t_j^{-1}g).$$

3. Soit t_jW l'image de $\delta(W)$ par $t_j : \mathrm{Ind}(W) \to \mathrm{Ind}(W)$. Alors

$$\boxed{\mathrm{Ind}(W) = \bigoplus_{j=1}^{n} t_j W.}$$

En particulier,

$$\dim \mathrm{Ind}(W) = [G:H] \cdot \dim W$$

Démonstration. 1. Soit $g \in H$. Alors, pour tout $h \in H$ on a

$$\begin{aligned}\delta_w(gh) &= h^{-1}g^{-1}(w) \\ &= h^{-1}(\delta_w(g)).\end{aligned}$$

Si $g \notin H$ alors $gh \notin H$ et donc $\delta_w(gh) = 0 = h(\delta_w(g))$.

Il est clair que δ est linéaire et on montre l'équivariance. Soit $h \in H$. Alors

$$\begin{aligned}\delta_{hw}(g) &= \begin{cases} g^{-1}h(w), & \text{si } g \in H \\ 0, & \text{si } g \notin H \end{cases} \\ &= \begin{cases} \delta_w(h^{-1}g), & \text{si } g \in H \\ 0, & \text{si } g \notin H \end{cases} \\ &= \begin{cases} h(\delta_w)(g), & \text{si } g \in H \\ 0, & \text{si } g \notin H. \end{cases}\end{aligned}$$

2. Soit $g = t_k h$. Alors

$$\begin{aligned}\varphi(g) &= h^{-1}(\varphi(t_k)) \\ &= h^{-1}(\delta_{\varphi(t_k)}(e)) \\ &= \delta_{\varphi(t_k)}(h) \\ &= \delta_{\varphi(t_k)}(t_k^{-1}g).\end{aligned}$$

Si $j \neq k$, alors

$$\begin{aligned}\delta_{\varphi(t_j)}(t_j^{-1}g) &= \delta_{\varphi(t_j)}(t_j^{-1}t_k h) \\ &= 0,\end{aligned}$$

parce que $t_j^{-1}t_k h \notin H$. D'où la formule. L'injectivité est conséquence de $\delta_w(e) = w$.
3. La formule précédente s'écrit comme $\varphi = \sum_{i=1}^{q} t_i(\delta_{\varphi(t_i)})$. $\square$

Exercice 158. Montrer que l'évaluation

$$\varepsilon : \mathrm{Ind}_H^G(W) \longrightarrow W, \qquad \varphi \mapsto \varphi(e).$$

est H-équivariante.

Proposition 159 (Réciprocité de Frobenius)**.** *L'évaluation*

$$\varepsilon : \mathrm{Ind}_H^G(W) \longrightarrow W, \qquad \varphi \mapsto \varphi(e).$$

est H-équivariante.

Si V est une rep. de G, alors

$$E : \mathrm{Hom}_G(V, \mathrm{Ind}_H^G(W)) \longrightarrow \mathrm{Hom}_H(V, W), \qquad \Phi \longmapsto \varepsilon \circ \Phi$$

est bijective.

La preuve est triviale et difficile à suivre !

Démonstration. On note que

$$E(\Phi) : v \mapsto [\Phi(v)]\,(e).$$

Soit $\Psi \in \mathrm{Hom}_H(V, W)$. On introduit

$$D(\Psi) : V \longrightarrow F(G, W),$$

par

$$[D(\Psi)(v)]\,(g) = \Psi(g^{-1}v).$$

Affirmation : La fonction $D(\Psi)(v) : G \to W$ appartient à $\mathrm{Ind}(W)$.

En effet,

$$\begin{aligned}
[D(\Psi)(v)]\,(gh) &= \Psi(h^{-1}g^{-1}v) \\
&= h^{-1}\left\{\Psi(g^{-1}v)\right\} \\
&= h^{-1}\left\{[D(\Psi)(v)]\,(g)\right\}.
\end{aligned}$$

Affirmation : Si $v, v' \in V$ et $\lambda \in \mathbb{C}$, alors

$$D(\Psi)(\lambda v + v') = \lambda D(\Psi)(v) + D(\Psi)(v').$$

Donc, $D(\Psi) : V \to \mathrm{Ind}_H^G(W)$ est linéaire.

La vérification ne pose aucun problème.

Affirmation : La fonction $D(\Psi) : V \to \mathrm{Ind}(W)$ est G-équivariante.

Si $g \in G$ alors

$$D(\Psi)(gv)(x) = D(\Psi)(x^{-1}gv).$$

Puis,

$$\begin{aligned}
(gD(\Psi)(v))(x) &= \Psi(v)(g^{-1}x) \\
&= \Psi(x^{-1}gv).
\end{aligned}$$

Affirmation : $D(E(\Phi)) = \Phi$ pour chaque $\Phi \in \mathrm{Hom}_G(V, \mathrm{Ind}(W))$. Soit $v \in V$. On a

$$\begin{aligned}[D(E(\Phi))](v) : g \mapsto [E(\Phi)](g^{-1}v) \\ &= [\Phi(g^{-1}v)](e) \\ &= [g^{-1}(\Phi(v))](e) \\ &= [\Phi(v)](g).\end{aligned}$$

Affirmation : Pour chaque $\Psi \in \mathrm{Hom}_H(V, W)$ on a $E(D(\Psi)) = \Psi$.

On a

$$\begin{aligned}E(D(\Psi)) : v &\mapsto (D(\Psi)(v))(e) \\ &= \Psi(ev).\end{aligned}$$

□

Corollaire 160. *Soit V une rep de G et W une rep de H. Alors*

$$\boxed{\langle \chi_V, \chi_{\mathrm{Ind}(W)} \rangle_G = \langle \chi_{\mathrm{res}(V)}, \chi_W \rangle_H.}$$

Démonstration. Suit directement du Théorème et du fait que $\dim \mathrm{Hom}_G(X, Y) = \langle \chi_X, \chi_Y \rangle$ (Exercice !). □

On étudie maintenant les caractères induits.

Théorème 161. *On a*

$$\chi_{\mathrm{Ind}(W)}(g) = \sum_{\substack{i \in \{1,\ldots,n\} \\ g \in t_i H t_i^{-1}}} \chi_W(\underbrace{t_i^{-1} g t_i}_{\in H})$$

On aura besoin du Lemme suivant dont la preuve est laissée au lecteur.

Lemme 162. *Soit $V = V_1 \oplus \cdots \oplus V_n$ un espace vectoriel ; on note $u_i : V_i \to V$ l'injection et $p_j : V \to V_j$ la projection. Si $A : V \to V$ est une application linéaire, alors*

$$\begin{aligned}\mathrm{Tr}(A) &= \sum_{i=1}^{n} \mathrm{Tr}(p_i A u_i) \\ &= \sum_{\substack{i \in \{1,\ldots,n\} \\ A(V_i) \subset V_i}} \mathrm{Tr}(p_i A u_i)\end{aligned}$$

Démonstration du Théorème 161. Soit $g \in G$. Si $i \in \{1, \ldots, n\}$ est fixé, il existe un unique j tel que $gt_i \in t_j H$. Soit ainsi $gt_i = t_j h$. On a

$$\begin{aligned}g(t_i(\delta_w)) &= t_j h(\delta_w) \\ &= t_j(\delta_{h(w)}) \\ &\in t_j(W).\end{aligned}$$

Il suit que $g(t_iW) \subset W_i$ si et seulement si $gt_iH = t_iH$, i.e. si et seulement si $g \in t_iHt_i^{-1}$. Donc,

$$\mathrm{Tr}\ g_{\mathrm{Ind}(W)} = \sum_{\substack{i\in\{1,\ldots,n\}\\ g\in t_iHt_i^{-1}}} \mathrm{Tr}\left(g : t_i(W) \longrightarrow t_i(W)\right).$$

Or, mais si $g = t_iht_i^{-1}$ avec $h \in H$, alors

$$\begin{aligned} g(t_i(\delta_w)) &= t_ih(\delta_w) \\ &= t_i(\delta_{h(w)}). \end{aligned}$$

Par conséquent,

$$\begin{tikzcd} t_i(W) \arrow[r, "g"] & t_i(W) \\ W \arrow[u, "t_i"] \arrow[r, "h"'] & W \arrow[u, "t_i"'] \end{tikzcd}$$

on voit que

$$\mathrm{Tr}\ \ (g : t_i(W) \longrightarrow t_i(W)) = \mathrm{Tr}\ h : W \longrightarrow W.$$

Donc,

$$\mathrm{Tr}\ \ (g : t_i(W) \longrightarrow t_i(W)) = \chi_W(h).$$

$\square$

Exemple 163. Soit $G = D_{10}$ et $H = \langle R\rangle$. Si ω est une racine 5-ème de l'unité ; on obtient une rep de H en $\mathbb{C}$ via $R^k(1) \mapsto \omega^k$; clairement son caractère, notons le ζ, est la fonction $R^k \mapsto \omega^k$. On note V l'induite.

Prenons $\{e, S\}$ comme "système transversal" et utilisons les classes

$$\begin{aligned} C_1 &= \{e\}, \\ C_2 &= \{S, RS, \ldots, R^4S\}, \\ C_3 &= \{R, R^4\} \\ C_4 &= \{R^2, R^3\}, \end{aligned}$$

déterminées par l'Exemple 151 pour calculer explicitement χ_V. Soit $g \in G$. Alors $g \in G$. Si $g \notin H$, alors $g \notin SHS$ et donc $\chi_V(g) = 0$. Si $g \in H$, alors

$$\chi_V(g) = \zeta(g) + \zeta(SgS).$$

Donc,

$$\begin{aligned} \chi_V(C_1, \ldots, C_4) &= (2, 0, \omega + \omega^4, \omega^2 + \omega^3) \\ &= (2, 0, \omega + \overline{\omega}, \omega^2 + \overline{\omega}^2). \end{aligned}$$

Ceci nous montre que si $\omega = e^{2\pi i/5}$, alors V est la rep S_3 déterminée dans l'Exemple 151, et que si $\omega = e^{4\pi i/5}$, alors V est S_4.

Une autre façon d'écrie la formule dans le Théorème 161 est la suivante. Si $\zeta \in F^{\mathrm{cent}}(H,\mathbb{C})$ on note $\zeta^0 : G \to \mathbb{C}$ son extension par zéro, à savoir

$$\zeta^0(g) = \begin{cases} \zeta(g) & \text{si } g \in H \\ 0 & \text{si } g \notin H. \end{cases}$$

On définit

$$\mathrm{Ind}_H^G(\zeta)(g) = \frac{1}{|H|} \sum_{x\in G} \zeta^0(x^{-1}gx).$$

Clairement, $\zeta^0(hgh^{-1}) = \zeta^0(g)$ si $h \in H$, et donc

$$\begin{aligned} \mathrm{Ind}(\zeta)(g) &= \frac{1}{|H|} \sum_{i=1}^{n} \sum_{x\in t_iH} \zeta^0(x^{-1}gx) \\ &= \frac{1}{|H|} \sum_{i=1}^{n} \sum_{h\in H} \zeta^0((t_ih)^{-1}g(t_ih)) \\ &= \frac{1}{|H|} \sum_{i=1}^{n} \sum_{h\in H} \zeta^0(t_i^{-1}gt_i) \\ &= \sum_{i=1}^{n} \zeta^0(t_i^{-1}gt_i) \\ &= \sum_{\substack{i\in\{1,\dots,n\} \\ t_i^{-1}gt_i\in H}} \zeta(t_i^{-1}gt_i). \end{aligned}$$

Remarques 164. Soit $g \in G$; on note par $\sigma_g : S_n \to S_n$ la permutation définie par $gt_iH = t_{\sigma_g(i)}H$. On fixe i, et on écrit $gt_i = t_jh$. Donc,

$$g(t_i\delta_w) = t_j\delta_{hw}.$$

Puis, on note que

$$g\delta_w(x) = \begin{cases} 0, & x \notin gH, \\ x^{-1}g(v) & x \in gH. \end{cases}$$

Exercice 165. On suppose que $\varrho : H \to \mathrm{GL}_r$ est injective. Montrer que $\mathrm{Ind}(\varrho) : G \to \mathrm{GL}_{nr}$ est aussi injective.

Cours 12

(3 avril 2020).

G est fini ; toutes les reps sont complexes et de dimension finie. On désigne par Cl_G l'ensemble des classes de conjugaison de G. On souhaite montrer :

Théorème 166. *Soit S une rep simple de G. Alors* $\dim S$ *divise* $|G|$.

Notre preuve aura besoin du concepte de *entier algébrique*. Voici une brève digression.

Digression sur les entiers algébriques.

Un $\theta \in \mathbb{C}$ est dit un *nombre algébrique* s'il est solution d'un équation polynomiale $\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_0 = 0$ où $a_j \in \mathbb{Q}$. Le complexe θ est dit un *entier algébrique* s'il est solution d'une équation polynomiale comme avant où, de plus, chaque a_j est entier. L'ensemble des nombres algébriques est normalement noté $\overline{\mathbb{Q}}$. Celui des entiers algébriques est noté $\overline{\mathbb{Z}}$.

Exemple 167. Chaque rationnel est un nombre algébrique. Chaque entier est un entier algébrique. Les racines $\sqrt{2}$, $\sqrt{3}$, etc sont des entiers algébriques. Les racines de l'unité $\zeta = e^{2\pi ik/n}$ sont toutes des entiers algébriques car $\zeta^n - 1 = 0$. En particulier, pour chaque représentation $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ de G et chaque $g \in G$, les valeurs propres de $\rho(g)$ sont des entiers algébriques.

Donner des exemples de nombres complexes qui ne sont pas des *nombres algébriques* est assez difficile (π en est un). De l'autre côté, il est très simple de donner des exemples de complexes qui ne sont pas des *entiers algébriques*.

Lemme 168. *Soit $\theta \in \mathbb{Q} \cap \overline{\mathbb{Z}}$. Alors θ est un nombre entier.*

Démonstration. On suppose que θ n'est pas entier : $\theta = r/s$ avec $s > 1$ et $\mathrm{pgcd}(r, s) = 1$. Si $\theta^n + \sum_{i=1}^{n-1} a_i\theta^i = 0$, on a $\sum_{i=0}^{n-1} a_i r^i s^{n-i} = -r^n$. Soit p un diviseur premier de s. Le fait que $n - i \geqslant 1$ pour chaque $i \in \{0, \ldots, n-1\}$ prouve que $p \mid \sum_{i=0}^{n-1} a_i r^i s^{n-i} \Rightarrow p \mid r^n$, ce qui est impossible. $\square$

Une autre propriété remarquable des entiers algébriques est la suivante :

Théorème 169. *Soient α et β des entiers algébriques. Alors $\alpha + \beta$ et $\alpha\beta$ sont aussi des entiers algébriques.*

La preuve de ce résultat qui consiste à trouver une équation algébrique pour $\alpha + \beta$ (ou $\alpha\beta$) à partir des équations algébriques de α et β n'est pas évidente. Mais en faisant un peu plus de théorie, on est vite amené à un concept qui permet de gagner du terrain. Dans la suite, pour $\theta \in \mathbb{C}$ donné, on écrit $\mathbb{Z}[\theta] = \{P(\theta) : P \in \mathbb{Z}[X]\}$. Il s'agit clairement d'un sous-anneau de $\mathbb{C}$.

Théorème 170. *Soit $\theta \in \mathbb{C}$. Les conditions suivantes sont équivalentes.*

1) θ est entier algébrique.

2) Le groupe abélien $\mathbb{Z}[\theta]$ possède un nombre fini de générateurs.

3) Il existe un sous-groupe $A \subset \mathbb{C}$ ayant un nombre fini de générateurs tel que $\theta \cdot A \subset A$.

Démonstration. 1) $\Rightarrow$ 2). Par définition, il existe des entiers a_i tels que $\theta^n = a_{n-1}\theta^{n-1} + \cdots + a_0$. Il suit que $\mathbb{Z}[\theta] = \mathbb{Z} \cdot 1 + \cdots + \mathbb{Z} \cdot \theta^{n-1}$.

2) $\Rightarrow$ 3). On prendra $A = \mathbb{Z}[\theta]$.

3) $\Rightarrow$ 1). Soient $\alpha_1, \ldots, \alpha_n$ des générateurs de A. On déduit que

$$\begin{aligned} \theta\alpha_1 &= a_{11}\alpha_1 + a_{12}\alpha_2 + \cdots + a_{1n}\alpha_n \\ \vdots &= \vdots \\ \theta\alpha_n &= a_{n1}\alpha_1 + a_{n2}\alpha_2 + \cdots + a_{nn}\alpha_n, \end{aligned}$$

avec $a_{ij} \in \mathbb{Z}$. Ceci s'écrit comme

$$(a_{ij}) \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \theta \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix};$$

d'où θ est une valeur propre de la matrice (a_{ij}). Il suit que $P(X) = \det(X - a_{ij}) = X^n + \cdots$ s'annule en $X = \theta$. $\square$

Preuve du Théorème 169. D'après le Théorème 170, il existe A et B des sous-groupes de $\mathbb{C}$ qui sont engendrés chacun par un nombre fini d'éléments, et tels que $\alpha \cdot A \subset A$ et $\beta \cdot B \subset B$. Soit $AB = \bigcup_s \{a_1b_1 + \cdots + a_sb_s\ a_i \in A,\ b_i \in B\}$. Si $\{\alpha_i\}$ engendre A et $\{\beta_j\}$ engendre B, alors $\{\alpha_i\beta_j\}$ engendre AB. Donc AB est engendré par un nombre fini d'éléments. Clairement, si $a \in A$ et $b \in B$, alors $\alpha \cdot (ab) = (\alpha a) \cdot b \in AB$ et $\beta(ab) = a(\beta b) \in AB$. Donc, $\alpha\beta(AB) \subset \alpha(AB) \subset AB$ et $(\alpha + \beta)(AB) \subset AB$. On conclut à l'aide du Théorème 170. $\square$

Exemple 171. Soient $\alpha = \sqrt{2}$ et $\beta = \sqrt{3}$. On écrit $A = \mathbb{Z} + \mathbb{Z}\alpha$ et $B = \mathbb{Z} + \mathbb{Z}\beta$. Il suit que $\alpha \cdot A \subset A$ et $\beta \cdot B \subset B$. Soit $AB = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma$, où on a posé $\gamma = \alpha\beta$. On considère $\varepsilon = 1 + \alpha + \beta$. Donc

$$\begin{aligned} \varepsilon \cdot 1 &= 1 + \alpha + \beta + 0\gamma, \\ \varepsilon \cdot \alpha &= 2 + \alpha + 0\beta + \gamma \\ \varepsilon \cdot \beta &= 3 + 0\alpha + \beta + \gamma \\ \varepsilon \cdot \gamma &= 0 \cdot 1 + 3\alpha + 2\beta + \gamma, \end{aligned}$$

et ε est valeur propre de la matrice

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 1 & 0 & 1 \\ 3 & 0 & 1 & 1 \\ 0 & 3 & 2 & 1 \end{pmatrix},$$

et on voit que son poly caractéristique s'annule en ε, c'est-à-dire, $\varepsilon^4 - 4\varepsilon^3 - 4\varepsilon^2 + 16\varepsilon - 8 = 0$.

Les caractères comme entiers algébriques

Dans la suite, on fixe une représentation simple S de caractère χ. L'idée fondamentale derrière la preuve du Théorème 166 est la famille de nombres complexes $\{\lambda_C\}_{C \in \mathrm{Cl}_G}$ construite dans la suite.

Pour chaque $C \in \mathrm{Cl}_G$, soit $\delta_C : G \to \mathbb{C}$ la fonction centrale définie par

$$\delta_C(g) = \begin{cases} 1, & \text{si } g \in C, \\ 0, & \text{si } g \notin C. \end{cases}$$

On sait, d'après la Proposition 146 que

$$\sum_{g \in C} g_S \ : S \longrightarrow S$$

est un endomorphisme G-équivariant (il s'agit de $|G| \cdot M^S_{\delta_C}$) et donc

$$\sum_{g \in C} g_S = \lambda_C \operatorname{id}_S$$

où λ_C est un nombre complexe. En fait, prenant la trace :

$$\begin{aligned} \lambda_C \cdot \dim S &= \mathrm{Tr}(\lambda_C \operatorname{id}_S) \\ &= \sum_{g \in C} \mathrm{Tr}(g_S) \\ &= |C| \chi(C) \end{aligned}$$

En particulier, $\lambda_C \cdot \overline{\chi(C)} = \dfrac{|C|}{\dim S}$ et donc

Proposition 172. *On a*

$$\sum_{C \in \mathrm{Cl}_G} \lambda_C \cdot \overline{\chi(C)} = \frac{|G|}{\dim S}.$$

□

La preuve tu Théorème 166 viendra ainsi en démontrant que $\sum_{C \in \mathrm{Cl}_G} \lambda_C \cdot \overline{\chi(C)}$ est un nombre entier. Ceci sera obtenu en montrant que λ_C est un entier algébrique.

Si $B \in \mathrm{Cl}_G$ alors l'ensemble

$$CB := \{cb \ : \ c \in C,\, b \in B\}$$

est stable par conjugaison (vérifiez !) et on obtient

$$CB = \bigsqcup_{\substack{A \in \mathrm{Cl}_G \\ A \subset CB}} A.$$

Soit

$$m : C \times B \longrightarrow CB, \quad (c, b) \mapsto cb$$

la multiplication.

Lemme 173. *Si $A \in \mathrm{Cl}_G$ et $A \subset CB$, alors pour n'importe quel deux éléments $a, a' \in A$, on a*

$$\#m^{-1}(a) = \#m^{-1}(a').$$

Démonstration. On écrit $x \mapsto {}^g x$ pour la conjugaison par g : il s'agit d'un morphisme de groupes. Donc, si $a' = {}^g a$ alors

$${}^g(-) : m^{-1}(a) \longrightarrow m^{-1}(a')$$

est une bijection. $\square$

Ceci étant, on écrira

$$m_A(C, B)$$

pour le cardinal de $m^{-1}(a) \subset C \times B$ pour n'importe quel $a \in A$.

Lemme 174. *La multiplication par le nombre complexe λ_C préserve le sous-groupe abélien $\sum_{A \in \mathrm{Cl}_G} \mathbb{Z}\lambda_A$. Plus précisément,*

$$\lambda_C \cdot \lambda_B = \sum_{\substack{A \in \mathrm{Cl}_G \\ A \subset CB}} m_A(C, B) \cdot \lambda_A.$$

Démonstration. On a

$$\begin{aligned}
\lambda_C \lambda_B \operatorname{id}_S &= \sum_{c\in C} c_S \sum_{b \in B} b_S \\
&= \sum_{(c,b)\in C\times B} (cb)_S \\
&= \sum_{\substack{A\in \mathrm{Cl}_G \\ A\subset CB}} \sum_{(c,b)\in m^{-1}(A)} (cb)_S \\
&= \sum_{\substack{A\in \mathrm{Cl}_G \\ A\subset CB}} \sum_{a\in A} \sum_{(c,b)\in m^{-1}(a)} (cb)_S \\
&= \sum_{\substack{A\in \mathrm{Cl}_G \\ A\subset CB}} \sum_{a\in A} \# m^{-1}(a) \cdot a_S \\
&= \sum_{\substack{A\in \mathrm{Cl}_G \\ A\subset CB}} m_A(C,B) \lambda_A \operatorname{id}_S.
\end{aligned}$$

□

Via le Théorème 170, on déduit :

Corollaire 175. *Pour $C \in \mathrm{Cl}_G$, le nombre λ_C est un entier algébrique.*

Preuve du Théorème 166. Pour chaque $g \in G$, les valeurs propres de g_S sont des racines de l'unité et par conséquent $\chi(C) \in \overline{\mathbb{Z}}$. Donc, $\sum_C \lambda_C \cdot \overline{\chi(C)} \in \overline{\mathbb{Z}}$. Mais on a vu que $\sum_C \lambda_C \cdot \overline{\chi(C)} = \dfrac{|G|}{\dim S}$ est rationnel. Par le Lemme 168, $\dfrac{|G|}{\dim S}$ est entier. □

Références

[Alperin et Bell] J. L. Alperin et R. B. Bell, *Groups and representations*. Springer Verlag. Disponible sur la bibliothèque numérique de Sorbonne Université.

[Chevalley] Claude Chevalley, *Theory of Lie Groups*. Princeton Landmarks.

[Dat] Jean-François Dat, *Polycopié*, 2009-2010.

[Lang] S. Lang, *Algebra*. Springer.

[Malliavin] Marie-Paule Malliavin, *Les groupes finis et leurs représentations complexes*. Paris, Masson, 1981.

[Varadarajan] V. S. Varadarajan, *Lie groups, Lie algebras and their representations*.