Théorie des groupes, Théorie des representations
Classe sino-française, USTC

Prof. Bernhard Keller*

Polycopié par *CHEN Ruikai*†et *LI Xiao*‡

Novembre 2020 -Janvier 2021

Résumé

C'est le cours d'algèbre pour la classe sino-français de deuxième année donné par Prof. Keller. Les sujets incluent principalement le théorie des groupes et les représentations de groupes, les groupes classiques et les quaternions.

*https://webusers.imj-prg.fr/∼ bernhard.keller/
†chen1794147489@mail.ustc.edu.cn
‡home.ustc.edu.cn/∼cnlx

Table des matières

Première partie

Théorie générale des groupes

1 Groupes abéliens de type fini

1.1 Structure de groupe abéliens de type fini

Soit $(A, +)$ un groupe abélien.

Rappel 1.1. *A est **de type fini** s'il admet une partie génératrice finie, i. e. une partie $\{a_1, \cdots, a_r\} \subset A$ telle que tout $a \in A$ s'écrit $a = x_1a_1 + x_2a_2 + \cdots + x_ra_r$ pour des $x_1, \cdots, x_r \in \mathbb{Z}$. Autrementdit, le morphisme*

$$\mathbb{Z}^r \to A, \quad \begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} \mapsto x_1a_1 + x_2a_2 + \cdots + x_ra_r$$

est surjectif. Alors tout quotient de A est encore de type fini.

Exemple 1.2. Le groupe $(\mathbb{Q}, +)$ n'est pas de type fini !

Exemple 1.3. les groupes $\mathbb{Z}^r, r \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ sont de type fini.

Proposition 1.4. *Si A est de type fini (et abélien !), tout sous-groupe $B \subset A$ est (abélien) de type fini .*

Remarque 1.5. cette proposition est faute pour les groupes non abéliens !

Démonstration. Soit $p : \mathbb{Z}^r \to A$ un morphisme surjectif. Alors $B \subset A$ est quotient de $C = p^{-1}(B) \subset \mathbb{Z}^r$. Il suffit donc de montrer que $C \subset \mathbb{Z}^r$ est de type fini. On procède par récurrence sur r. Pour $r = 0$, il n'y a rien à démontrer. Notons $\mathbb{Z} \subset \mathbb{Z}^r$ le sous-groupe $\mathbb{Z} \times \{0\}^{r-1}$ Alors $\mathbb{Z} \cap C$ est un sous-groupe de $\mathbb{Z}$. Donc $\mathbb{Z} \cap C$ est engendré par un seul élément $c \in \mathbb{Z} \cap C$. Considérons le diagramme(avec suites exactes)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}^r & \xrightarrow{\pi} & \mathbb{Z}^{r-1} & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & \mathbb{Z} \cap C & \longrightarrow & C & \longrightarrow & \pi(C) & \longrightarrow & 0 \end{array}$$

La projection $\pi : \mathbb{Z}^r \to \mathbb{Z}^{r-1}$, $\begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} \mapsto \begin{bmatrix} x_2 \\ \vdots \\ x_r \end{bmatrix}$ induit un isomorphisme de $C/(\mathbb{Z} \cap C)$ sur $\pi(C)$.
Par l'hypothèse de récurrence sur r, le sous-groupe $\pi(C) \subset Z^{r-1}$ est engendré par un nombre fini d'éléments $\pi(c_2), \cdots, \pi(c_s)$. Alors il est clair que C est engendré par $c_2, \cdots, c_s$. □

Définition 1.6. Le groupe A est (abélien) **libre de type fini** s'il est isomorphe à $\mathbb{Z}^r$ pour un $r \in \mathbb{N}$. Une famille $a_1 \cdots a_r$ d'éléments de A est une **base** de A si le morphisme $\mathbb{Z}^r \to A, e_i \mapsto a_i$ est un isomorphisme.

Remarque 1.7. Une famille $a_1, \cdots, a_r$ est une base s.s.i. elle est génératrice et libre , i. e. $\forall x_1, \cdots x_r \in \mathbb{Z}$. on a

$$x_1 a_1 + \cdots x_r a_r = 0 \quad \Longrightarrow \quad x_1 = \cdots = x_r = 0$$

Théorème 1.8. *Toutes les bases d'un groupe abélien libre de type fini ont le même nombre d'éléments, appelé* ***le rang du groupe abélien libre****.*

Démonstration. Soit A abélien libre avec deux bases $a_1, \cdots, a_r$ et $b_1, \cdots, b_s$. Soient $\varphi : \mathbb{Z}^r \to A, e_i \mapsto a_i$ et $\psi : \mathbb{Z}^s \to A, e_i \mapsto b_i$ les isomorphismes associés. Alors $\psi^{-1} \circ \varphi : \mathbb{Z}^r \to \mathbb{Z}^s$ est un isomorphisme. Donc les $v_i := \psi^{-1} \circ \varphi(e_i)$ forment une famille génératrice et libre dans $\mathbb{Z}^s$. Mais alors ils forment aussi une famille génératrice et libre dans le $\mathbb{Q}-$espace vectoriel $\mathbb{Q}^s$. En effet, tout e_i est combinaison linéaire à coefficients entiers des v_i et si on a une relation

$$y_1 v_1 + \cdots + y_r v_r = 0$$

à coefficients rationnels, il suffit de multiplier par le produit des dénominateurs pour conclure $y_1 = \cdots = y_r = 0$. Donc les $v_1, \cdots, v_r$ forment une base du $\mathbb{Q}-$espace vectoriel $\mathbb{Q}^s$. Donc $r = s$. □

Remarque 1.9. Si $V \neq 0$ est un espace vectoriel, tout $0 \neq v \in V$ se complète en une base. Cette propriété est fausse pour riété les groupes abéliens libre. Par exemple $0 \neq 2 \in \mathbb{Z}$ ne se complète pas en une base de $\mathbb{Z}$ car les seules bases de Z sont 1 et -1.

Définition 1.10. Soit $n \geq l$ un entier. Le $GL_n(\mathbb{Z})$ est le groupe des éléments inversibles de l'anneau $M_n(\mathbb{Z})$.

Exercice 1.11. Une matrice $M \in M_n(\mathbb{Z})$ est dans $GL_n(\mathbb{Z})$ s.s.i. $\det(M) \in \{\pm 1\}$.

Théorème 1.12. *Soit $A \in M_{p\times q}(\mathbb{Z})$. Alors il existe $P \in GL_p(\mathbb{Z})$ et $Q \in GL_q(\mathbb{Z})$ telles que*

$$PAQ = \begin{bmatrix} d_1 & & & & & & \\ & \ddots & & & 0 & & \\ & & d_s & & & & \\ & & & 0 & & & \\ & 0 & & & \ddots & & \\ & & & & 0 & \cdots & 0 \end{bmatrix}.$$

où $d_1, \cdots, d_s$ sont des entiers ≥ 1 tels que $d_l | \cdots | d_s$. Les d_i sont déterminés par la matrice A et s'appellent ***les facteurs invariants de A****.*

Démonstration. Montrons d'abord l'unicité. Notons B la matrice PAQ et $ImB \subset \mathbb{Z}^p$ le sous-groupe formé des $Bx, x \in \mathbb{Z}^p$. Alors il est clair que l'automorphisme $\mathbb{Z}^p \to \mathbb{Z}^p$ induit un isomorphisme de ImA sur ImB et donc un isomorphisme $\mathbb{Z}^p/ImA \to \mathbb{Z}^p/ImB$. Il est clair que ImB est le sous-groupe $d_1\mathbb{Z} \oplus \cdots \oplus d_s\mathbb{Z} \oplus 0 \oplus \cdots \oplus 0 \subset \mathbb{Z}^p$. Or si M_1 et M_2 sont deux groupes abéliens et $M_1' \subset M_1$ et $M_2' \subset M_2$ des sous-groupes, alors $M_1 \oplus M_2/M_1' \oplus M_2' \xrightarrow{\sim} M_1/M_1' \oplus M_2/M_2'$. Donc

$$\mathbb{Z}^p/ImB \simeq \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_s \oplus \mathbb{Z}^{p-s}.$$

Notons $T := \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_s$, l'isomorphisme $\mathbb{Z}^p/ImA \simeq \mathbb{Z}^p/ImB$ entre T et le **sous -groupe de torsion** de $\mathbb{Z}^p/ImA$:

$$(\mathbb{Z}^p/ImA)_t = \{y \in \mathbb{Z}^p/ImA \mid ny = 0 \text{ pour un } n \in \mathbb{Z} \setminus \{0\}\}$$

Donc T et $(\mathbb{Z}^p/ImA)_t$ sont fini et isomorphes. Donc

$$(\mathbb{Z}^p/ImA)_t \simeq \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_s, \quad d_1 | \cdots | d_s.$$

Par la classification des groupes abéliens finis, les d_i sont déterminés par le groupe $(\mathbb{Z}^p/ImA)_t$, et donc parla matrice A.

— Montrons l'existence. On procède comme pour les matrices à coefficients dans un corps : on utilise les opérations élémentaires qui correspondent à des multiplications à droite et à

gauche par des matrices dans $Gl_p(\mathbb{Z})$ resp. $GL_q(\mathbb{Z})$, par exemple

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \cdots$$

On peut supposer que $A \neq 0$.

Etape 1 : En permutant les lignes et les colonnes on transforme A en une matrice telle que $|a_{11}|$ soit minimal parmi les les $|a_{ij}|$. Si nécessaire, on multiplie la première ligne par -1 pour obtenir $a_{11} > 0$. Dans la suite, on va retourner plusieurs fois à l'étape 1 mais à chaque fois la valeur de $|a_{11}|$ va diminuer strictement de façon que le processus doit s'arrêter après un nombre fini d'itérations.

Etape 2 : Supposons qu'il y a un coefficient $a_{i1}, i > 1$, non nul à la première colonne . Effectuons une **division euclidienne** $a_{i1} = q \cdot a_{11} + r$ où $0 \leq r < a_{11}$. Soustrayons q fois la ligne 1 à la ligne i. Cette opération transforme a_{i1} en $r < a_{11}$. Si $r \neq 0$, on retourne à l'étape 1.

Etape 2' : Comme l'étape 2 mais pour les colonnes. Après un nombre fini d'itérations des étapes 1,2 et 2', on obtient une matrice de la forme

$$\begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{bmatrix}.$$

mais il est possible que a_{11} ne divise pas tous les coefficients de B. Alors on prend un b_{ij} non divisible par a_{11}, on ajoute la colonne j à la colonne 1 et on retourne à l'étape 1. Après un nombre fini d'itérations on obtient une matrice

$$\begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{bmatrix}.$$

où a_{11} divise tous les coefficients de B. On conclut par récurrence sur la taille de la matrice. □

Remarque 1.13. Si k est un corps, on a une division euclidienne pour l'anneau des polynômes en une variable $k[T]$. Si on remplace la valeur absolue par le degré et qu'on demande que les d_i soient des polynômes unitaires, alors on un théorème analogue (avec la "même "

démonstration) pour des matrices $A \in M_{p,q}(k[T])$ avec $P \in GL_p(k[T]) = \{P \mid \det P \in k^*\}$ et $Q \in GL_q(k[T])$.

Théorème 1.14 (la base adaptée)**.** *Soit M un groupe abélien libre de rang fini p. Soit $L \subset M$ un sous-groupe.Alors L est (abélien) libre de rang $s \leq p$ et il existe une base $e_1, \cdots, e_p$ de M et des entiers strictement positifs $d_1 | \cdots | d_s$ tels que $d_1 e_1, \cdots, d_s e_s$ forment une base de L.*

Démonstration. Choisissons un isomorphisme $\varphi : \mathbb{Z}^p \to M$. On sait que $\varphi^{-1}(L) \subset \mathbb{Z}^p$ est de type fini. Soit $a_1, \cdots, a_q$ une famille génératrice de $\varphi^{-1}(L)$. Soit $A \in M_{p \times q}(\mathbb{Z})$ la matrice de colonnes $a_1, \cdots, a_q$. Soient $P, Q, d_1, \cdots d_s$ comme dans le Thm. On considère le diagramme

$$\begin{array}{ccccc} \mathbb{Z}^q & \xrightarrow{A} & \mathbb{Z}^p & \xrightarrow[\varphi]{\sim} & M \\ {\scriptstyle\sim}\downarrow{\scriptstyle Q} & & {\scriptstyle\sim}\downarrow{\scriptstyle P} & & \\ \mathbb{Z}^q & \xrightarrow[D]{} & \mathbb{Z}^p & & \end{array}$$

où $D = \begin{bmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_s & & \\ & & & 0 & 0 \end{bmatrix}$. On a $\varphi^{-1}(L) = ImA$ et P induit un isomorphisme de ImA sur

$$ImD = d_1\mathbb{Z} \oplus \cdots \oplus d_s\mathbb{Z} \oplus 0 \oplus \cdots \oplus 0 \subset \mathbb{Z}^s$$

Alors il est clair que les $\varphi^{-1}(p^{-1}e_i), 1 \leq i \leq p$ forment une base de $\mathbb{Z}^P$ avec les propriétés souhaitées. □

Théorème 1.15 (Théorème de structure)**.** *Soit A un groupe abélien de type fini. Alors il existe des entiers r et s et des entiers $1 < d_1 | d_2 | \cdots | d_s$ déterminés par A tels que*

$$A \simeq \mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z}$$

Définition 1.16. Le **rang** de A est $rgA = p$.

Remarques 1.17. *(i) A est fini s.s.i. $r = 0$. Il est abélien libre s.s.i. $s = 0$.*

(ii) Soit $\varphi : \mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z} \xrightarrow{\sim} A$ un isomorphisme (choix !) . Alors l'image

$$A_1 = \varphi(0 \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z}) \subset A$$

ne dépend pas de choix de φ. En effet, le sous-groupe $0 \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z}$ est le sous-groupe de torsion de $\mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z}$. Donc son image par φ est le sous-

groupe de torsion de A : $A_t = \{a \in A \mid na = 0$ pour un $n \in \mathbb{N} \setminus \{0\}\}$. Ce sous-groupe est clairement indépendant du choix de φ. Mais $A_2 = \varphi(\mathbb{Z}^r \oplus 0) \subset A$ dépend du choix de φ. Exemple :

$$\mathbb{Z} \oplus \mathbb{Z}/2 \xrightarrow{\varphi=id} \mathbb{Z} \oplus \mathbb{Z}/2 = A, \quad A_2 = \mathbb{Z} \oplus 0$$

$$\mathbb{Z} \oplus \mathbb{Z}/2 \xrightarrow{\varphi'} \mathbb{Z} \oplus \mathbb{Z}/2, \ (n, \bar{m}) \mapsto (n, \bar{n} + \bar{m})$$

Alors $A_2' = \{(n, \bar{n} + \bar{m}) \mid n \in \mathbb{Z}, \bar{m} \in \mathbb{Z}/2\} \neq A_2$. Car l'image de A_2' par la projection $Z \oplus \mathbb{Z}/2 \to \mathbb{Z}/2$ est non nulle.

(iii) Notons A_t le sous-groupe de torsion de A. Alors on a une suite exacte canonique

$$0 \to A_t \to A \to A/A_t \to 0$$

Le groupe A/A_t est isomorphe (de façon non canonique !) à $\mathbb{Z}^r$. La suite est scindée : le sous-groupe A_t admet un supplémentaire isomorphe à A/A_t : $A \simeq A_t \oplus A/A_t$ Mais elle n'est pas canoniquement scindée !

Définition 1.18. Un groupe abélien est **indécomposable** s'il est non nul et n'est pas la somme directe de deux sous-groupes non nuls.

Corollaire 1.19. *Tout groupe abélien de type fini est somme directe de groupes abéliens indécomposables qui sont uniques à isomorphisme et permutation près.*

Démonstration. l'existence est claire par le théorème de structure et le lemme chinois (voir l'exemple). Montrons l'unicité. Dans la décompose en indécomposables, le nombre de facteurs $\mathbb{Z}$ est le rang du groupe, donc unique. Il suffit de montrer l'unicité pour un groupe abélien fini B. Le groupe B est la somme directe de ses $p-$Sylow. Donc on peut supposer que B est un $p-$groupe. Alors la classification des groupes abéliens finis donne

$$B \simeq \mathbb{Z}/p^{m_1} \oplus \mathbb{Z}/p^{m_2} \oplus \cdots \oplus \mathbb{Z}/p^{m_s}$$

□

Exemple 1.20. Soit $A = \mathbb{Z}/2 \oplus \mathbb{Z}/6 \oplus \mathbb{Z}/60 \oplus \mathbb{Z}/600$. Par le lemme chinois,

$$\begin{aligned} & \mathbb{Z}/2 \simeq \mathbb{Z}/2 \\ 6 = 2 \times 3 \quad & \mathbb{Z}/6 \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/3 \\ 60 = 2^2 \times 3 \times 5 \quad & \mathbb{Z}/60 \simeq \mathbb{Z}/4 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/5 \\ 600 = 2^3 \times 3 \times 5^2 \quad & \mathbb{Z}/600/2 \simeq \mathbb{Z}/8 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/25 \end{aligned}$$

La décomposition en groupes abéliens indécomposables de A est donnée par la somme des groupes à droite des equations.

1.2 Illustration : le théorème de Mordell

Une **courbe elliptique sur** $\mathbb{Q}$ est l'ensemble E des solutions $(x, y) \in \mathbb{Q}^2$ d'une équation $y^2 = x^3 + ax + b$, où $a, b \in \mathbb{Q}$ t.q. $4a^3 + 27b^2 \neq 0$. On admet aussi le "point à l'infini " $O = (0, \infty)$ comme solution. Toutes les droites verticales passent par O. On peut munir E d'une structure de groupe abélien, d'élément neutre O telle que

$$P + Q + R = 0 \iff P, Q, R \text{ sont alignes.}$$

Il est non trivial de montrer que $(E, +)$ est un groupe (associativite !). Il est clair que $(E, +)$ est abélien.

Théorème 1.21 (Mordell 1922)**.** *Le groupe abélien $(E, +)$ est de type fini.*

Théorème 1.22 (Mazur, 1977)**.** *Le groupe de torsion E_t est isomorphe à l'un des groupes suivants : $\mathbb{Z}/n, 1 \leq n \leq 10, \mathbb{Z}/2 \oplus \mathbb{Z}/d$ où $d \in \{2, 4, 6, 8\}$.*

1.3 Les groupes $GL_n(\mathbb{Z})$ et $SL_n(\mathbb{Z})$

Soit $n \geq 1$ un entier. Considérons les matrices suivantes :

— Transvection élémentaires : $E_{ij}(a) = I_n + aE_{ij},\ a \in \mathbb{Z}, i \neq j$.

— Dilatations : $D_i(\epsilon) = diag(1, \cdots, 1, \epsilon, 1, \cdots, 1), \epsilon \in \{1, -1\} = \mathbb{Z}^*$.

— Transpositions : $\begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & 1 & & 0 & & \\ & & & & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{bmatrix}$, où $a_{ii} = a_{jj} = 0,\ a_{ij} = a_{ji} = 1$.

Théorème 1.23. *(i) Toute matrice $A \in GL_n(\mathbb{Z})$ s'écrit $A = L \cdot diag(l, \cdots, \det A)$, où L est un produit de transvections élémentaires.*

(ii) Le groupe $SL_n(\mathbb{Z})$ est engendré par les transvections élémentaires $E_{i,i+1}(1),\ E_{i+1,i}(1),\ 1 \leq i \leq n-1$.

Démonstration. (i) Soit E le sous-groupe de $SL_n(\mathbb{Z})$ engendré par les transvection élémentaires. Soit $D \subset GL_n(\mathbb{Z})$ le sous-groupe engendré par les dilatations. Pour $\epsilon \in \{\pm 1\}$ et $a \in \mathbb{Z}$, on a $D_i(\epsilon)E_{kl}(a)D_i(\epsilon)^{-1} = E_{kl}(\pm a)$. Donc $DE = ED$. Nous avons

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

donc les transpositions sont ED. La démonstration du "Thm PAQ" montre alors que $ED = GL_n(\mathbb{Z})$. Notons que $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$. Si $g \in GL_n(\mathbb{Z})$, on a $g = ed$ pour $e \in E$ et $d \in D$ et la dernière remarque montre que l'on a aussi $g = e' \cdot \det(1, \cdots, 1, \det g)$ pour un $e' \in E$.
(ii) On note que $E_{ij}(a) = E_{ij}(1)^a,\ a \in \mathbb{Z}$, et que $[E_ij(a), E_{jk}(b)] = E_{ik}(ab)$ pour $i < j < k,\ a, b \in \mathbb{Z}$. Donc E est engendré par les $E_{i,i+1}(1),\ E_{i+1,i}(1),\ 1 \leq i \leq n-1$. □

2 Groupes simples et suites de composition

Rappel 2.1. *Un groupe G est simple s'il est non trivial et ses seuls sous-groupes distingués sont $\{e\}$ et G.*

Remarque 2.2. G est simple s.s.i. G admet exactement deux sous-groupes distingués s.s.i. G est non trivial et n'admet aucun quotient autre que $\{e\}$ et G.

Rappel 2.3. *Les groupes simples abéliens sont exactement les groupes $\mathbb{Z}/p\mathbb{Z}$, où p est premier (à isomorphisme près !). Le groupe alterné $\mathfrak{A}_n$ (A : Agothique) est simple pour $n = 3$ ou $n \geq 5$. Le groupe $\mathfrak{A}_4$ n'est pas simple : le groupe de Klein $V = \{Id, (12)(34), (13)(24), (14)(23)\}$ est un sous-groupe distingué (V : "Vierergruppe"="groupe des quatres", allemand : "Vier"="four "="quatre".) Le groupe $PSL_n(\mathbb{F}_p)$ est simple sauf si $n = 2$ et $p \in \{2, 3\}$.*

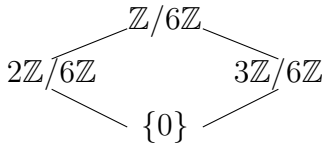
Théorème 2.4 (Feit-Thompson 1963)**.** *Tout groupe fini simple non abélien est d'ordre pair.*

Remarque 2.5. La démonstration faisait 255 pages et n'a pas été beaucoup simplifiée depuis.

2.1 Le théorème de Jordan - Holder

Soit G un groupe. Une **suite de composition** de G est une suite finie $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{e\}$ de sous-groupes emboîtés tels que chaque sous-quotient $G_i/G_{i+1},\ 0 \leq i < r$ est simple.

Exemples 2.6. (i) Le groupe $\mathbb{Z}/6\mathbb{Z}$ a pour treillis de sous-groupes



Donc $\mathbb{Z}/6\mathbb{Z}$ admet exactement deux suites de compositions : $\mathbb{Z}/6\mathbb{Z} \rhd 2\mathbb{Z}/6\mathbb{Z} \rhd \{0\}$ et $\mathbb{Z}/6\mathbb{Z} \rhd 3\mathbb{Z}/6\mathbb{Z} \rhd \{0\}$. sous-quotients : $\mathbb{Z}/2$ et $\mathbb{Z}/3$.

(ii) Le groupe $\mathbb{Z}/p^n\mathbb{Z}$, p premier, $n \geq 1$, a pour treillis de sous-groupes

$$\mathbb{Z}/p^n\mathbb{Z} - p\mathbb{Z}/p^n\mathbb{Z} - \cdots - p^{n-1}\mathbb{Z}/p^n\mathbb{Z} - \{0\}$$

Il admet donc l'unique suite de composition

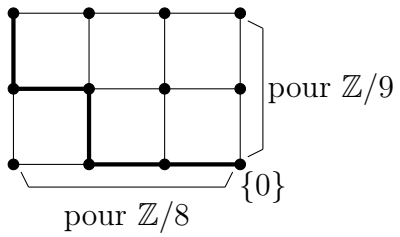
$$\mathbb{Z}/p^n\mathbb{Z} \rhd p\mathbb{Z}/p^n\mathbb{Z} \rhd \cdots \rhd p^{n-1}\mathbb{Z}/p^n\mathbb{Z} \rhd \{0\}$$

où tous les sous-quotients sont isomorphes à $\mathbb{Z}/p\mathbb{Z}$.

(iii) Le groupe $\mathbb{F}_2^2 = \mathbb{Z}/2 \oplus \mathbb{Z}/2$ a pour treillis de sous-groupes où $D_1 = \mathbb{F}_2 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix}, D_2 = \mathbb{F}_2 \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix}, D_3 = \mathbb{F}_2 \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.Il y a exactement 3 suites de composition : $\mathbb{F}_2^2 \rhd D_i \rhd \{0\},\ 1 \leq i \leq 3$. Sous-quotients : Deux fois $\mathbb{Z}/2\mathbb{Z}$!

Remarque 2.7. Les suites de compos. de $\mathbb{Z}/4\mathbb{Z}$ ont aussi comme sous-quotients deux fois $\mathbb{Z}/2\mathbb{Z}$ mais $\mathbb{Z}/2 \oplus \mathbb{Z}/2 \not\simeq \mathbb{Z}/4$.

(iv) Considérons $A = \mathbb{Z}/72\mathbb{Z} \simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$. Alors tout sous-gr. de $\mathbb{Z}/8 \oplus \mathbb{Z}/9$ est de la forme $A \oplus B$ où A est un sous-groupe de $\mathbb{Z}/8$ et B un sous-groupe de $\mathbb{Z}/9$. En effet, si $C \subset \mathbb{Z}/8 \oplus \mathbb{Z}/9$, alors C est la somme de son $2-$Sylow C' et de son $3-$Sylow C" et $C' = C \cap (\mathbb{Z}/8 \oplus 0),\ C'' = C \cap (0 \oplus \mathbb{Z}/9)$. Donc le treillis des sous-groupes est

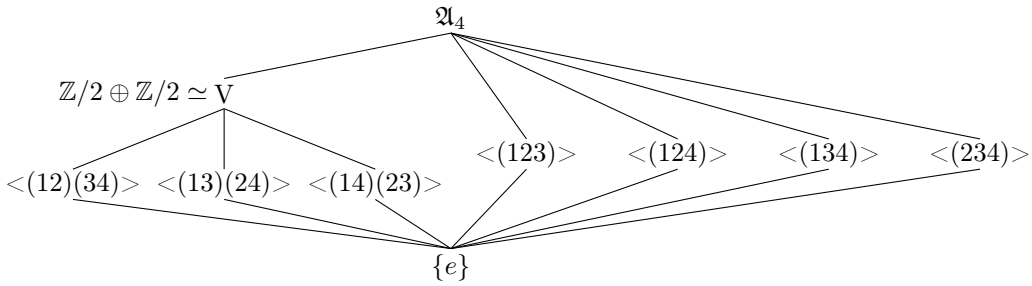


Les suites de composition sont en bijection avec les chemins du sommet du treillis vers

$\{0\}$. Il y en a 10 car tout chemin est de longueur 5 et déterminé par la position des deux segments. Or $\binom{5}{2} = 10$. Les sous-quotients sont $\mathbb{Z}/2, \mathbb{Z}/2, \mathbb{Z}/2, \mathbb{Z}/3, \mathbb{Z}/3$ à une permutation près.

(v) Pour $n = 3$ ou $n \geq 5$, le groupe sym. $\mathfrak{S}_n$ admet une suite de composition $\mathfrak{S}_n \rhd \mathfrak{A}_n \rhd \{e\}$ aux sous-quotients $\mathbb{Z}/2\mathbb{Z}$ et $\mathfrak{A}_n$.

(vi) Le treillis des sous-groupes de $\mathfrak{A}_4$ est



Il y a 3 suites de composition aux sous-quotients $\mathbb{Z}/3\mathbb{Z} \simeq \mathfrak{A}_4/V, \mathbb{Z}/2, \mathbb{Z}/2$.

(vii) Le groupe $\mathbb{Z}$ n'admet pas de suite de composition : Supposons que $G_1 \rhd \mathbb{Z}$ est un sous-groupe t.q. $\mathbb{Z}/6$, est simple. Alors $G_1 = p\mathbb{Z}$ pour un nombre premier p. Donc $G_1 \simeq \mathbb{Z}$. On obtient forcément une suite infinie

$$\mathbb{Z} \supset p_1\mathbb{Z} \supset p_1p_2\mathbb{Z} \supset p_1p_2p_3\mathbb{Z} \supset \cdots$$

(dans le treillis des sous-groupe de $\mathbb{Z}$, il n'y a pas de chemin fini du haut vers le bas)

Exercice 2.8. Tout groupe abélien fini A admet (en général : plusieurs) une suite de composition dont les sous-quotients sont les $\mathbb{Z}/p\mathbb{Z}$, où p parcourt les diviseurs premiers de l'ordre $|A|$ de A avec leurs multiplicités. Combien y a-t-il de suites de composition ? (Cela dépend de la structure de A, pas seulement de $|A|$ comme le montre l'exemple de $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ et $\mathbb{Z}/4$).

Définition 2.9. Deux suites de composition $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{e\}$ et $G = H_0 \rhd H_1 \rhd \cdots \rhd H_s = \{e\}$ sont **équivalentes** si $r = s$ et il existe une permutation $\sigma \in \mathfrak{S}_r$ telle que $G_i/G_{i+1} \simeq H_{\sigma(i)}/H_{\sigma(i)+1}, 0 \leq i < r$.

Théorème 2.10 (Jordan-Holder)**.** *(i) Tout groupe fini admet une suite de composition.*

(ii) Si un groupe fini admet deux suites de composition, elles sont équivalentes.

Remarques 2.11. *(i) Les termes G_i d'une suite de composition ne sont pas uniques (voir les exemples), seulement les sous-quotients sont unique à isomorphisme près.*

(ii) On dit que G est une ***extension de K par H*** *s'il existe une suite exacte $0 \to H \to G \to K \to 0$. La partie (i) du thm dit que tout groupe fini est extension itérée de groupes finis simples. La partie (ii) dit que les groupes simples qui interviennent dans l'extension itérée sont uniques à isomorphisme et permutation près. Le théorème ne dit rien sur la nature de l'extension : $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ et $\mathbb{Z}/4$ sont deux extensions de $\mathbb{Z}/2$ par $\mathbb{Z}/2$. Le thm réduit la classification des groupes finis à deux problèmes :*

(a) la classification des groupes finis simples.

(b) la classification de leurs extensions itérées.

Le problème (b) a été résolu au milieu des années 80. La démonstration occupe plusieurs milliers de pages.

Lemme 2.12. *Soient G un groupe et H_1 et K_1 deux sous-groupes distingués t.q. G/H_1 et G/K_1 sont simples. Alors $H_1 \cap K_1$ est distingué dans H_1 et K_1 et on a $G/H_1 \simeq K_1/(H_1 \cap K_1)$ et $G/K_1 \simeq H_1/(H_1 \cap K_1)$.*

Démonstration. On a le diagramme

$$\begin{array}{ccccc} H_1 & \hookrightarrow & G & \xrightarrow{\pi} & G/H_1 \\ \uparrow & & \uparrow & & \uparrow \\ H_1 \cap K_1 & \hookrightarrow & K_1 & \xrightarrow[\pi|_{K_1}]{} & \pi(K_1) \qquad \simeq K_1/(H_1 \cap K_1) \end{array}$$

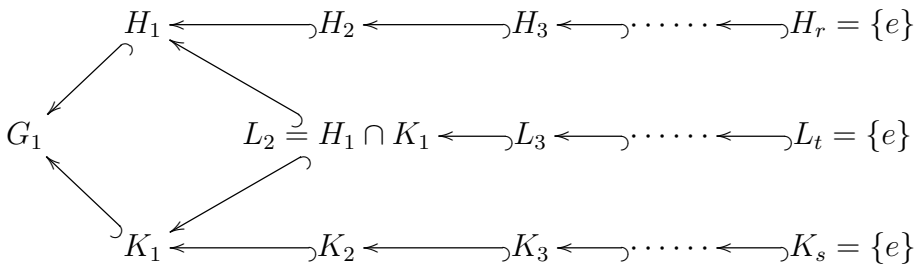
Comme G/H_1 est simple, on a ou bien $\pi(K_1) = G/H$, ou bien $\pi(K_1) = \{e\}$. Montrons que le deuxième cas est impossible : Si $K_1/(K_1 \cap H_1) = \{e\}$, alors $K_1 \subset H_1$ et H_1/K_1 est un sous-groupe distingué du groupe simple G/K_1. Comme $H_1 \neq G$, on doit avoir $H_1/K_1 = \{e\}$ ce qui est impossible car $H_1 \neq K_1$. □

Démonstration du Théorème. (i) On peut supposer G non trivial. Si G est simple , il n'y a rien à démontrer. Sinon, on a une suite exacte $0 \to H \to G \to K \to 0$ pour des groupes H et K d'ordre strictement plus petit que $|G|$. Par récurrence sur $|G|$, ils admettent des suites de composition : $H = H_0 \rhd \cdots \rhd H_r = \{e\}$ et $K = K_0 \rhd \cdots \rhd K_s = \{e\}$. Alors G admet la suite de composition

$$G = G_0 \rhd \pi^{-1}(K_1) \rhd \cdots \rhd \pi^{-1}(K_s) = H = H_0 \rhd \cdots \rhd H_r = \{e\}$$

(ii) G est un groupe fini. Soient $(H_1, \cdots, H_r)$ et $(K_1, \cdots, K_s)$ deux suites de composition t.q. $r \leq s$. Si $H_1 = K_1$, on applique à ce groupe l'hypothèse de récurrence (sur la longueur

de la suite de composition) : elle donne l'équivalence des suites $(H_2, \cdots, H_r)$ et $(K_2, \cdots, K_s)$ du groupe $H_1 = K_1$. Comme on a aussi $G/H_1 = G/K_1$, on obtient l'affirmation. Supposons que $H_1 \neq K_1$. On considère le diagramme



Soit (L_i) une suite de composition de L_2 (existe car $|L_2| < \infty$). Par le lemme, tous les quotients de termes consécutifs dans ce diagramme sont simples. Donc H_1 admet deux suites de composition : $H_1 \rhd H_2 \rhd H_3 \rhd \cdots \rhd H_r = \{e\}$ et $H_1 \rhd L_2 \rhd L_3 \rhd \cdots \rhd L_t = \{e\}$. Comme la suite de première composition est de longueur $r - 1 < r$, on peut appliquer l'hypothèse de récurrence pour conclure que $r = t$ et qu'on a des isomorphisme entre les sous-quotients convenablement permutés. Le groupe K_1 aussi admet deux suites de composition : $K_1 \rhd L_2 \rhd L_3 \rhd \cdots \rhd L_t = \{e\}$ et $K_1 \rhd K_2 \rhd K_3 \rhd \cdots \rhd K_s = \{e\}$. Comme la première est de longueur $r-1 < r$, on peut encore appliquer l'hypothèse de récurrence pour obtenir que $t = s$ et qu'on a des isomorphismes entre les sous-quotients permutés. Comme $G/K_1 \simeq H_1/L_2$ et $G/H_1 \simeq K_1/L_2$, on en déduit l'affirmation. □

APPENDICE : le théorème de Jordan-Holder pour des groupes quelconques

Lemme 2.13 (Lemme du papillon (Zassenhaus))**.** *Soient G un groupe. Supposons qu'on a des sous-groupes $B \lhd A \leq G$ et $D \lhd C \leq G$. Alors on a $B(A\cap D) \lhd B(A\cap C)$ et $(B\cap C)D \lhd (A\cap C)D$ et*

$$B(A \cap C)/B(A \cap D) \xleftarrow{\sim} (A \cap C)/(B \cap C)(A \cap D) \xrightarrow{\sim} (A \cap C)D/(B \cap C)D$$

Démonstration. Comme $D \rhd C$, on a $A \cap D \rhd A \cap C$ et $B \cap (A \cap D) \rhd B(A \cap C)$. De même pour $(B \cap C)D \rhd (A \cap C)D$. Rappelons que si H est un sous-groupe et N un sous-groupe distingué, alors $H/(H \cap N) \xrightarrow{\sim} HN/N$. Pour $H = A \cap C$ et $N = B(A \cap D)$ dans A, nous obtenons

$$(A \cap C)/(A \cap C) \cap B(A \cap D) \xrightarrow{\sim} (A \cap C)B(A \cap D)/B(A \cap D)$$

Or nous avons $(A \cap C) \cap B(A \cap D) = (B \cap C) \cdot (A \cap D)$ et $(A \cap C)B(A \cap D) = B(A \cap C)$. De même, on montre que $(A \cap C)/(B \cap C)(A \cap D) \xrightarrow{\sim} (A \cap C)D/(B \cap C)D$. □

Définition 2.14. Soit une suite de sous-groupes $G = G_1 \rhd G_2 \rhd \cdots \rhd G_r$. Un **raffinement** est une suite de sous-groupes obtenue en insérant un nombre fini de sous-groupes $G_i = G_{i1} \rhd \cdots \rhd G_{im_i} = G_{i+1}$ entre G_i et G_{i+1}, pour chaque $1 \leq i < m$. Une suite $G = H_1 \rhd \cdots \rhd H_s$ est **équivalente** à $G = G_1 \rhd \cdots \rhd G_r$ si $r = s$ et $G_i/G_{i+1} \simeq H_{\sigma(i)}/H_{\sigma(i)+1}$ pour tout $1 \leq i \leq r$ pour une permutation $\sigma \in \mathfrak{S}_r$.

Théorème 2.15 (Schreier)**.** *Soit G un groupe. Deux suites de sous-groupes de G : $G = G_1 \rhd \cdots \rhd G_r = \{e\}$ et $G = H_1 \rhd \cdots \rhd H_s = \{e\}$ ont un raffinement commun.*

Démonstration. Pour $1 \leq i \leq r-1$ et $1 \leq j \leq s$, on pose $G_{ij} = G_{i+1}(H_j \cap G_i)$. Alors $G_{is} = G_{i+1}$ et nous avons un raffinement de $G = G_1 \rhd \cdots \rhd G_r = \{e\}$ donné par

$$G = G_{11} \rhd G_{12} \rhd \cdots \rhd G_{1,s-1} \rhd G_2 = G_{2,1} \rhd G_{2,2} \rhd \cdots \rhd G_{r-1,1} \rhd \cdots \rhd G_{r-1,s-1} \rhd \{e\}$$

De même, on pose $H_{ji} = H_{j+1}(G_i \cap H_j)$ pour $j = 1, \cdots, s-1$ et $i = 1, \cdots, r$. Ceci donne un raffinement de $G = H_1 \rhd \cdots \rhd H_s$. Par le lemme du papillon, pour $1 \leq i \leq r-1$ et $1 \leq j \leq s-1$, on a un isomorphisme $G_{ij}/G_{i,j+1} \simeq H_{ji}/H_{j,i+1}$ $(*)$. Nous considérons les deux suites à $(r-1)(s-1)+1$ termes formées de $G_{ij}, 0 < i < r,\ 0 < j < s$, et $\{e\}$ et de $H_{ij}, 0 < i < r,\ 0 < j < s$, et $\{e\}$. Pour chaque couple (i,j), on a l'isomorphisme $(*)$. Il s'ensuit que les deux suites à $(r-1)(s-1)+1$ termes sont équivalentes. □

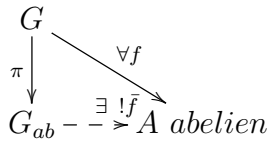
Théorème 2.16 (Jordan-Holder)**.** *Deux suites de composition d'un groupe G : $G = G_1 \rhd \cdots \rhd G_r = \{e\}$, G_i/G_{i+1} simple $\forall i$, $G = H_1 \rhd \cdots \rhd H_s = \{e\}$, H_j/H_{j+1} simple $\forall j$ sont équivalentes.*

Démonstration. On considère le raffinement (G_{ij}) comme dans la démonstration du Thm de Schreier. On observe que pour tout i, comme G_i/G_{i+1} est simple, il existe exactement un indice j t.q. $G_i/G_{i+1} \simeq G_{ij}/G_{i,j+1}$. Donc la suite des sous-quotients non triviaux de la suite (G_i) et de la suite raffinée (G_{ij}) est la même (à des isomorphismes près). Par la démonstration du théorème de Schreier, elle est aussi la même à permutation près pour (H_{ji}) et (H_j). □

3 Groupes résolubles

Rappel 3.1. *Soit G un groupe. Le **groupe dérivé $D(G)$** est le sous-groupe de G engendré par les commutateurs $[g,h] = ghg^{-1}h^{-1},\ g,h \in G$. Si $f : G \to H$ est un morphisme, alors $f(D(G)) \subset D(H)$. En particulier, $D(G)$ est distingué dans G. Le quotient $G_{ab} = G/D(G)$*

est abélien. C'est le plus grand quotient abélien de G. Il s'appelle ***l'abélianisé de G****. Le morphisme $\pi : G \to G_{ab}$ est* ***universel*** *parmi les morphismes de G vers un groupe abélien :*



Autrement dit, π induit une bijection $Mor(G_{ab}, A) \to Mor(G, A),\ \bar{f} \mapsto \bar{f} \circ \pi$.

Définition 3.2. La **suite dérivée** de G est la suite $G := D^0G \rhd D^1G \rhd \cdots \rhd D^{n+1}G \rhd \cdots$, où $D^{n+1}G = D(D^n(G)),\ \forall n \geq 0$.

Remarque 3.3. Si $f : G \to H$ est un morphisme, alors $f(D^nG) \subset D^nH$(récurrence sur n). En particulier, D^nG est distingué dans G (et donc dans $D^{n-1}G$) pour tout $n \geq 1$. Le quotient $D^nG/D^{n+1}G = (D^nF)_{ab}$ est abélien.

Proposition 3.4. *G est* ***résoluble*** *s'il vérifie les conditions équivalentes suivantes :*

(i) il existe $n \in \mathbb{N}$ t.q. $D^nG = \{e\}$.

(ii) il existe une suite $G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_r = \{e\}$ de sous-groupes emboîtés t.q. G_i/G_{i+1} est abélien, $\forall 0 \leq i < r$.

Démonstration. $(i) \Longrightarrow (ii)$ est clair : $G_i = D^iG$.
$(ii) \Longrightarrow (i)$: Comme G/G_1 est abélien, on a $G_1 \supset D^1G$. Par récurrence sur i, on montre de même que G_i contient D^iG pour $1 \leq i \leq r$. Donc D^rG est trivial. □

Remarque 3.5. À un polynôme $P \in \mathbb{Q}[X]$, on peut associer un groupe fini : son groupe de Galois G. On peut montrer (théorie de Galois) que G est résoluble s.s.i. l'équation $P(x) = 0$ est résoluble par radicaux, voir l'année prochaine.

Exemples 3.6. (i) Tout groupe abélien est résoluble (alors $D^1G = \{e\}$).

(ii) Le groupe symétrique $\mathfrak{S}_n$ est résoluble pour $n \leq 4$ mais non pas pour $n \geq 5$ car alors on a $D^m\mathfrak{S}_n = \mathfrak{A}_n$ pour tout $m \geq 1$ (car alors $D^1\mathfrak{S}_n = \mathfrak{A}_n$, $D\mathfrak{A}_n = \mathfrak{A}_n$). Donc $\mathfrak{S}_n$ n'est pas résoluble pour $n \geq 5$. Cela entraînera que l'équation générale de degré $n \geq 5$ n'admet pas de solution par radicaux.

(iii) Un groupe G qui est résoluble et simple est cyclique d'ordre premier. En effet, on a $D(G) \subsetneq G$ (sinon, on aurait $D^nG = G,\ \forall n \geq 0$). Comme G est simple, on a $D(G) = \{e\}$. Mais alors G est abélien et simple, si $G \neq \{e\}$, il contient un $g \neq e$. Cet élément doit engendrer G. Donc G est cyclique. Comme G n'a pas de sous-groupes autres que G et $\{e\}$, G est cyclique d'ordre premier.

(iv) Si k est un corps, le **groupe affine**

$$GA(k) = \{f : k \to k \mid \exists a \in k^\times \text{ et } b \in k \text{ t.q. } f(x) = ax + b\}$$

est résoluble, car on a la suite $\{id\} \rhd T \rhd GA(k)$, où T est le groupe des translations $x \mapsto x + b$, $b \in k$, et $GA(k)/T \xrightarrow{\sim} k^\times$. Mais pour $n \geq 2$ et $k = \mathbb{F}_p$, $p \neq 2, 3$, les groupes $SL_n(k)$ et $GL_n(k)$ ne sont pas résolubles car $D(GL_n(k)) = SL_n(k)$ et $D(SL_n(k)) = SL_n(k)$.

Proposition 3.7. *(i) Tout sous-groupe et tout quotient d'un groupe résoluble est résoluble.*

(ii) Soit $0 \to H \to G \to K \to 0$ une suite exacte. Alors G est résoluble s.s.i. H et K sont résolubles.

Démonstration. (i) : Si $H \leq G$, alors $D^n H \leq D^n G$ et si $\pi : G \to K$, alors $\pi(D^n G) = D^n K$. (ii) : On a "$\Longrightarrow$" par (i). Montrons "$\Longleftarrow$" : Soit $n_k \in \mathbb{N}$ t.q. $D^{n_k}(K) = \{e\}$. Alors $\pi(D^{n_k}(G)) = D^{n_k} K = \{e\}$. Donc $D^{n_k}(G) \subset H$. Mais alors $D^{n+n_k}(G) = D^n(D^{n_k}(G)) \subset D^n H$ et $D^n H = \{e\}$ pour $n > 0$. Donc G est résoluble. □

Exemple 3.8. Pour $n \geq 2$, le groupe $SL_n(\mathbb{Z})$ n'est pas résoluble. Comme $SL_2(\mathbb{Z}) \leq SL_n(\mathbb{Z})$, il suffit de montrer que $SL_2(\mathbb{Z})$ n'est pas résoluble (par (i)). En effet, la projection $\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} = \mathbb{F}_5$ (morphisme d'anneaux) induit un morphisme surjectif $SL_2(\mathbb{Z}) \to SL_2(\mathbb{F}_5)$ (car $SL_2(\mathbb{F}_5)$ est engendré par les transactions élémentaires). Donc si $SL_2(\mathbb{Z})$ était résoluble, alors $SL_2(\mathbb{F}_5)$ serait résoluble ce qui n'est pas le cas car $D(SL_2(\mathbb{F}_5)) = SL_2(\mathbb{F}_5)$.

Terminologie. *Un **sous-quotient** d'un groupe G est un quotient d'un sous-groupe de G.*

Remarques 3.9. *(i) Par (i), tout sous-quotient d'un groupe résoluble est résoluble .*

*(ii) On a des suites exactes $0 \to D^{n+1}G \to D^n(G) \to (D^n G)_{ab} \to 0$, $\forall n \geq 0$. Si G est résoluble, il s'ensuit que G est dans la clôture par extensions de la classe des groupes abéliens ($D^n G$ est dans cette clôture par récurrence descendante sur n). Avec (i), cela implique que **la classe des groupes résolubles est la clôture par extensions de la classe des groupes abéliens.***

Proposition 3.10. *Un groupe fini G est résoluble s.s.i. ses sous-quotients simples sont cycliques d'ordre premier.*

Démonstration. "$\Longleftarrow$" : Soit $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{e\}$ une suite de composition. On procède par récurrence sur r. Si $r = 0$, il n'y a rien à démontrer. Supposons $r > l$. Par

l'hypothèse de récurrence, le groupe G_1 est résoluble et le groupe G/G_1 est résoluble. Donc G est résoluble.

"$\Longrightarrow$" : Si G est résoluble, tout sous-quotient de G est résoluble. En particulier, les sous-quotients simples sont résolubles. Or un groupe simple et résoluble est cyclique d'ordre premier. □

Exemple 3.11. Soit G un groupe d'ordre impair. Alors ses sous-quotients sont d'ordre impair. Donc ses sous-quotients simples sont d'ordre impair. Par le théorème de Feit-Thompson, les seuls groupes simples d'ordre impair sont les groupes cycliques d'ordre premier $p \geq 3$. Par la proposition précédente, G est résoluble.

4 Groupes nilpotents

Définition 4.1. Soit G un groupe. **Sa suite centrale descendante** est la suite

$$G = C^1G,\ C^2G = [G,G] := DG,\ C^3G = [G,[G,G]], \cdots, C^{n+1}G = [G, C^nG]$$

où $[G, C^nG]$ est le sous-groupe engendré par les commutateurs $[g,c], g \in G, c \in C^nG$.

Lemme 4.2. *(i) si $f : G \to H$ est un morphisme, alors $f(C^nG) \subset C^nH$. En particulier, $C^nG \lhd G,\ \forall n \geq 1$.*

(ii) On a $G = C^1G \rhd C^2G \rhd \cdots \rhd C^nG \rhd \cdots$.

Démonstration. Pour (i), on fait récurrence sur n et (ii) résulte de (i). □

Proposition 4.3. *Soit $\pi : G \to G/C^{n+1}G$. Alors $\pi(C^nG)$ est central dans $G/C^{n+1}G$ et $C^{n+1}G$ est le plus petit sous-groupe distingué de G avec cette propriété.*

Exercice 4.4. Vérifier **l'identité de Hall-Witt** :

$$\forall x,y,z \in G,\ [[x,y^{-1}],z]^y \cdot [[y,z^{-1}],x]^z \cdot [[z,x^{-1}],y]^z = e$$

où $x^g := gxg^{-1}$ et déduire que $[C^iG, C^jG] \subset C^{i+j}G, \forall i,j \geq 1$ (d'où la convention $C^1G = G$).

Définition 4.5. Un groupe G est **nilpotent** s'il existe $n \in \mathbb{N}$ t.q. $C^{n+1}G = \{e\}$. Alors le plus petit $n \geq 0$ avec cette propriété s'appelle **la classe de nilpotence** de G.

Remarques 4.6. *(i) Tout groupe nilpotent est résoluble car $D^nG \subset C^{n+1}G$ (récurrence).*

(ii) Si G est nilpotent tout sous-groupe $H \leq G$ et tout quotient $K = G/N$ sont nilpotents car $C^nH \subset C^nG$ et $C^nK = \pi(C^nG)$ où $\pi : G \to G/N$, pour tout $n \geq 1$.

(iii) On a $C^n(G \times H) = C^nG \times C^nH$. Donc tout produit fini de groupes nilpotents est nilpotent.

Exemples 4.7. (i) Soit $n \geq 2$ et soit G le groupes des **matrices unitriangulaires** $n \times n$:

$$G = \begin{bmatrix} 1 & & & * \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix} = \{A \in M_n(\mathbb{Z}) \mid a_{ij} = 0,\ \forall i > j \text{ et } a_{ii} = 1,\ \forall i\}$$

Alors

$$C^2G = \begin{bmatrix} 1 & 0 & * & * & \\ & 1 & 0 & & * \\ & & \ddots & \ddots & * \\ & & & \ddots & 0 \\ & & & & 1 \end{bmatrix}, \quad C^3G = \begin{bmatrix} 1 & 0 & 0 & * & \\ & 1 & \ddots & \ddots & * \\ & & & \ddots & 0 \\ & & & \ddots & 0 \\ & & & & 1 \end{bmatrix}, \cdots,\ C^nG = \{I_n\}$$

Donc G est nilpotent de classe $n-1$. De même pour des matrices unitriangulaires à coefficients dans n'importe quel anneau commutatif.

(ii) Supposons que G est un $p-$groupe d'ordre $p^n,\ n > 1$. Alors G est nilpotent. En effet, c'est clair si $n \leq 1$, et pour $n > 1$, G est une extension centrale (voir plus loin) : $0 \to Z(G) \to G \to G/Z(G) \to 0$, où $Z(G)$ est non trivial, $G/Z(G)$ est un $p-$groupe d'ordre $< p^n$ qui eat nilpotent par récurrence. Donc G est nilpotent.

Définition 4.8. Soit $0 \to H \to G \to K \to 0$ une suite exacte telle que H est central dans G. Alors on dit que G est une **extension centrale** de K par H.

Lemme 4.9. *Dans cette situation, si K est nilpotent, G est aussi nilpotent.*

Démonstration. Supposons que $C^nK = \{e\}$. Alors $\pi(C^nG) = \{e\}$ et $C^nG \subset H$. Mais alors $C^{n+1}G = [G, C^nG] \subset [G, H] = \{e\}$. □

Rappel 4.10. *La classe des groupes résolubles est la clôture par extensions quelconques de la classe des groupes abéliens.*

Proposition 4.11. *La classe des groupes nilpotents est la clôture par extensions centrales de la classe des groupes abéliens.*

Remarque 4.12. Explication du mot "clôture" (en anglais : closure) : Soit $\mathcal{C}$ une classe de groupes et $\mathcal{O}$ une opération qui à 2 groupes G_1 et G_2 associe une classe de groupes $\mathcal{O}(G_1, G_2)$ (p. ex. la classe de toutes les extensions de G_1 par G_2). Alors **la clôture de C par** $\mathcal{O}$ est la plus petite classe $\bar{\mathcal{C}}$ de groupes telle que

— $\bar{\mathcal{C}} \supset \mathcal{C}$.

— Si $G_1,\ G_2 \in \mathcal{C}$, alors $\mathcal{O}(G_1, G_2) \subset \bar{\mathcal{C}}$.

Démonstration. Soit $\mathcal{N}$ la classe des groupes nilpotents. On sait que $\mathcal{N}$ contient les groupes abéliens et qu'elle est stable par extensions centrales. Donc elle contient la clôture $\mathcal{E}$ de la classe des groupes abéliens par extensions centrales. Soit G un groupe. On a $G/C^1G = \{e\}$ et on a des extensions centrales

$$0 \to C^pG/C^{p+1}G \to G/C^{p+1}G \to G/C^pG \to 0, \quad p \geq 1$$

Par récurrence sur p, il s'ensuit que $G/C^{p+1}G \in \mathcal{E}$ pour tout $p \geq 1$. Donc $G \in \mathcal{E}$ si G est nilpotent. Donc $\mathcal{N} \subset \mathcal{E}$. □

Définition 4.13. Soit G un groupe. On pose $Z_0(G) = \{e\}$, $Z_1(G) = Z(G) =$ centre de G. Pour $n \geq l$, on pose

$$\begin{aligned} Z_{n+1}(G) &= \{\textit{image reciproque dans } G \textit{ du centre de } G/Z_n(G)\} \\ &= \{g \in G \mid \textit{on a } gxg^{-1}x^{-1} \in Z_nG, \textit{ pour tout } x \in G\} \end{aligned}$$

Remarques 4.14. *(i) On obtient une suite croissante* $\{e\} = Z_0G \lhd Z_1G \lhd Z_2G \lhd \cdots$ *et pour tout* $p \geq 0$ *une extension centrale*

$$0 \to Z_{p+1}G/Z_pG \to G/Z_pG \to G/Z_{p+1}G \to 0 \quad (*)$$

— *Si* $H \leq G$ *est central dans* G*, on n'a pas toujours* $Z_nG = \pi^{-1}(Z_n(G/H))$*, où* $\pi : G \to G/H$*. Par exemple, soit* $G = \{\pm 1, \pm i, \pm j, \pm k\}$ *le groupe quaternionigue. On a* $Z(G) = \{\pm 1\}$ *et* $G/Z(G)$ *est abélien. Donc* $Z_1(G/Z(G)) = G/Z(G)$ *et* $\pi^{-1}(Z_1(G/Z(G))) = G \neq Z_1(G) = Z(G)$.

Lemme 4.15. *G en nilpotent s.s.i.* $Z_nG = G$ *pour un* $n \gg 0$.

Démonstration. "$\Longleftarrow$" : On a $G/Z_nG = \{e\}$. Par récurrence descendante sur $p \leq n$, on trouve grâce à $(*)$ que G/Z_pG est nilpotent pour tout $p \geq 0$. Donc $G = G/Z_0G$ est nilpotent.

"$\Longrightarrow$" : On procède par récurrence sur la classe de nilpotence de G. (c'est le plus petit entier n tel que $C^{n+1}G = \{e\}$). Supposons que $C^nG = \{e\}$. Montrons par récurrence sur $m \in \{0, \cdots, m\}$ que $C^{n-m}(G) \subset Z_m(G)$. Pour $m = n$, on obtiendra que $G = C^0G \subset Z_n(G)$. Pour $m = 0$, on a $C^nG \subset Z_0(G) = \{e\}$ par hypothèse. Supposons que $C^{n-m}(G) \subset Z_m(G)$. Soit $y \in G^{n-m-1}(G)$. Si $x \in G$, on a alors $[x, y] \in C^{n-m}(G) \subset Z_m(G)$. Donc $\pi(x)$ est central dans $G/Z_m(G)$ et $y \in Z_{m+1}(G)$. □

5 Croissance des groupes de type fini

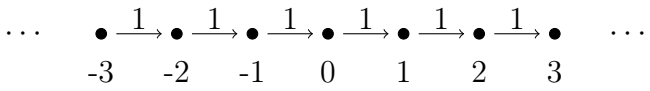
Soient G un groupe de type fini et $A = \{a_1, \cdots, a_r\}$ une partie génératrice. Pour $m \geq 0$, on note $B_{G,A}(m) \subset G$ l'ensemble des produits d'au plus m facteurs dans $A \cup A^{-1}$. On a la **fonction de croissance** $\beta_{G,A} : \mathbb{N} \to \mathbb{N},\ m \mapsto \big|B_{G,A}(m)\big|$.

Définition 5.1. Le **graphe de Cayley** de G par rapport à A est le graphe orienté étiqueté qui a

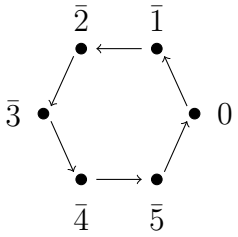
— pour sommets les éléments de G

— une flèche étiquetée a $a \in A$ de x vers ax pour tous $a \in A$ et tous $x \in G$.

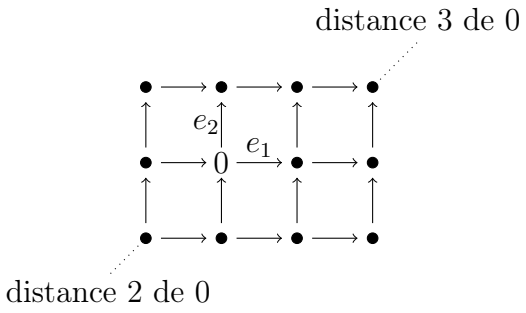
Exemples 5.2. (i) $G = (\mathbb{Z}, +)$ et $A = \{1\}$, graphe de Cayley :



(ii) $G = (\mathbb{Z}/6\mathbb{Z}, +)$, $A = \bar{1}$, graphe de Cayley :



(iii) $G = \mathbb{Z}^2$, $A = \{e_1, e_2\}$, $e_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, graphe de Cayley :



Remarque 5.3. La fonction croissance nous renseigne sur la géométrie du graphe de Cayley :

$$\begin{aligned} B_{G,A}(m) =& \{ \text{ sommets à distance} \leq \text{m de e dans le graphe de Cayley } \} \\ &= \text{nombre de points dans la boule de rayon m autour de 0 dans le graphe} \\ &\quad \text{de Cayley considéré comme espace métrique.} \end{aligned}$$

Exemples 5.4. (i) Dans $G = (\mathbb{Z}, +)$ avec $A = \{1\}$, on a $B_{\mathbb{Z},A}(0) = \{0\}$ et $B_{\mathbb{Z},A}(m) = \{-m, \cdots, 0 \cdots, m\}$. Donc $\beta_{\mathbb{Z},A}(m) = 2m + 1, \ \forall m \geq 1$.

(ii) La partie $B = \{2, 3\} \subset \mathbb{Z}$ est encore génératrice. On peut montrer (ce n'est pas complètement trivial) que

$$\beta_{\mathbb{Z},B}(m) = \begin{cases} 1 & m = 0 \\ 5 & m = 1 \\ 14 + 6(m-2) & m \geq 2 \end{cases}$$

Remarque 5.5. On a toujours $\beta_{G,A}(m) \leq (2|A| + 1)^m$ (compter les mots en l'alphabet $A \cup \{e\} \cup A^{-1}$). Donc la croissance est au plus exponentielle.

Définition 5.6. Soit $\beta_1, \beta_2 : \mathbb{Z} \to \mathbb{Z}$ deux fonctions croissantes. On définit

$$\beta_1 \preccurlyeq \beta_2 \ \ \textit{s.s.i. il existe } c > 0 \textit{ et } a \in \mathbb{N} \setminus \{0\} \textit{ t.q. } \beta_1(m) \leq c\beta_2(am), \ \forall m \in \mathbb{N} \setminus \{0\}$$

En particulier, $\beta_1 \sim \beta_2$ s.s.i. $\beta_1 \preccurlyeq \beta_2$ et $\beta_2 \preccurlyeq \beta_1$.

Exemples 5.7. (i) Toute fonction croissante bornée est équivalente à fonction constante.

(ii) Deux fonctions polynomiales (croissantes) sont équivalentes s.s.i. elles ont même degré.

(iii) Pour tout $a > 0,\ a \in \mathbb{N}$, les fonctions $m \mapsto 2^m$ et $m \mapsto 2^{am}$ sont équivalentes.

Proposition 5.8. *Soient $A_1, A_2 \subset G$ deux parties génératrices. Alors $\beta_{G,A_1} \sim \beta_{G,A_2}$.*

Démonstration. Il suffit de montrer que $\beta_{G,A_1} \preccurlyeq \beta_{G,A_2}$. Soit a un entier tel que les éléments de A_1 se trouvent dans $\beta_{G,A_2}(a)$. Alors on a $A_1^{-1} \subset B_{G,A_2}(a)$. On en déduit $B_{G,A_1}(m) \subset B_{G,A_2}(am)$. □

On note $\beta_G = \beta_{G,A}$ pour n'importe quelle partie génératrice finie $A \subset G$. Donc β_G est bien définie à équivalence près.

Définition 5.9. G est **à croissance polynomiale de degré** $\leq d$ si $\beta_G \preccurlyeq (m \mapsto m^d)$. G est **à croissance exponentielle** si $\beta_G \sim (m \mapsto 2^m)$.

Exemples 5.10. (i) Tout groupe fini est à croissance polynomiale de degré 0.

(ii) $\mathbb{Z}$ est à croissance polynomiale de degré 1.

(iii) $\mathbb{Z}^r$ est à croissance polynomiale de degré r, $\forall r \geq 0$.

(iv) Un groupe abélien A de type fini et de rang r (Donc $A \simeq \mathbb{Z}^r \oplus A_t,\ A_t =$ sous-groupe de torsion fini) est à croissancepolynomiale de degré r.

(v) Pour $n \geq 2$, les groupes $SL_n(\mathbb{Z})$ sont à croissance exponentielle. Esquisse de démonstration : On peut supposer que $n = 2$. On considère le sous-groupe H engendré par $M = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ et $N = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$. On montre que le produit $M^{a_1}N^{b_1} \cdots M^{a_r}N^{b_r} \neq I_2$ pour $r > 0$ et $a_i, b_i \in \mathbb{Z} \setminus \{0\}$. Cela suffit car si $H \rhd G$ sont de type fini, alors $\beta_H \preccurlyeq \beta_G$ (exercice !).

Remarque 5.11. Il existe des groupes de type fini qui ne sont ni à croissance polynomiale ni à croissance exponentielle ! C'est la réponse par Rostislav I, Grigorchute en 1984 à une question de John Milnor en 1968.

Proposition 5.12. *Soit G un groupe de type fini. Les groupes $C^nG/C^{n+1}G$, $n \geq 1$, sont (abéliens) de type fini.*

Démonstration. Montrons l'affirmation par récurrence sur $n \geq l$. Soit $a_1, \cdots, a_r$ des générateurs de G. Alors leurs classes engendrent bien sur $G/C^2G = G/[G,G] = G_{a,b}$. Supposons $n \geq 2$. Soient $b_1, \cdots, b_s \in C^nG$ des éléments dont les classes engendrent $C^nG/C^{n+1}G$. On va montrer que $C^{n+1}G/C^{n+2}G$ est engendré par les classes des $[a_i^{\pm 1}, b_j^{\pm 1}],\ 1 \leq i \leq r,\ 1 \leq j \leq s$.

Il suffit de montrer que, modulo $C^{n+2}G$, tout commutateur $[x,z]$, $x \in G, z \in C^nG$, est produit de ces éléments . Pour des éléments x, y, z d'un groupe quelconque, on a

$$[xy,z] = [y,z][[z,y],x][x,z] \qquad (1)$$

$$[x,yz] = [x,y][x,z][[z,x],y] \qquad (2)$$

(exercice de calcul !). Si on prend $z \in C^nG$ dans (1), on obtient

$$[xy,z] = [y,z][[z,u],x][x,z] \equiv [y,z][x,z] \qquad \mod C^{n+2}G$$

Donc le groupe $C^{n+1}G/C^{n+2}G$ est engendré par $[a_i^{\pm 1}, z], 1 \leq i \leq r, z \in C^nG$. Par (2), chaque $[a_i^{\pm 1}, z]$ est dans le sous-groupe de $C^{n+1}/C^{n+2}G$ engendré par les $[a_i^{\pm 1}, b_j^{\pm 1}],\ 1 \leq i \leq r,\ 1 \leq j \leq s$. □

Théorème 5.13 (J. A. Wolf 1968)**.** *Tout groupe nilpotent de type fini est à croissance polynomiale.*

Remarque 5.14. C'est plausible car les groupes nilpotents "ressemblent beaucoup" aux groupes abéliens.

Esquisse de la démonstration. Supposons que $C^3G = [G,[G,G]] = \{e\}$, c'est-à-dire que tout commutateur de G est central. Soit $A = \{a_1, \cdots, a_r\}$ une partie génératrice finie de G qui contient e et est stable par passage à l'inverse. Pour tout entier $m \geq 0$, un élément g de $B_{G,A}(m)$ est produit de exactement m éléments de A. Si ce produit contient un sous-produit $a_j a_i$, où $j > i$, on le remplace par $a_i a_j [a_j^{-1}, a_i^{-1}]$. Comme $[a_j^{-1}, a_i^{-1}]$ est central, on peut le déplacer tout à la droite du produit. Après un nombre fini d'étapes (au plus $1+2+\cdots+(m-1)$ étapes), on arrive à une expression $g = a_1^{k_1} a_2^{k_2} \cdots a_r^{k_r} c$ où $k_i \geq 0$, $k_1 + \cdots + k_r = n$ et c est un produit d'au plus $\frac{1}{2}m(m-1)$ commutateurs. On en déduit

$$\beta_{G,A}(m) \leq O(m^r) \cdot \beta_{[G,G],[A,A]}(\frac{1}{2}m(m-1))$$

Comme le groupe dérivé $[G,G]$ est abélien de type fini. On en déduit que G est à croissance polynomiale de degré $\leq r + r^2$. Dans le cas général, on procède par récurrence sur la classe de nilpotence de G et à chaque étape, on utilise un argument similaire. □

Définition 5.15. Un groupe G est **virtuellement nilpotent** s'il contient un sous-groupe nilpotent d'indice fini.

Corollaire 5.16. *Tout groupe de type fini virtuellement nilpotent est à croissance polynomiale.*

Exercice 5.17. Démontrer le corollaire.
Etapes : Soit G un groupe fini. Soit $H \leq G$ un sous-groupe.

— Supposons H de type fini. Montrer que $\beta_H \preccurlyeq \beta_G$.

— Montrer que si H est d'indice fini, alors il est automatiquement de type fini et $\beta_H \sim \beta_G$.

Remarque 5.18. De façon très surprenante, la réciproque du corollaire est vrai aussi !

Théorème 5.19 (M.Gromov 1981)**.** *Un groupe de type fini est à croissance polynomiale s.s.i. il est virtuellement nilpotent.*

Remarque 5.20. Quid des groupes resolubles de type fini ? On peut montrer (Milnor, Wolf 1968) qu'il existe des groupes résolubles de type fini à croissance exponentielle (on sait en construire explicitement) !

Deuxième partie

Représentations de groupes

Soient G un groupe et K un espace vectoriel.

Définition 5.21. Une **représentation** de G dans un k-espace vectoriel V est un morphisme de groupes $\rho : G \to GL(V)$.

Notation. *On note (V, ρ) la donnée d'une représentation et on utilise ρ ou V comme abréviation pour (V, ρ). Si on a une représentation (V, ρ), **l'action associée** de G sur V : $G \times V \to V$ est définie par*

$$g.v = \rho(g)(v), \quad \forall g \in G, \forall v \in V$$

La donnée de l'action associée est équivalente à celle de la représentation.

Exemples 5.22. (i) Si V est de dimension 1, alors le choix d'une base $v_1 \in V$ donne un isomorphisme $k^\times \to GL(V)$, $\lambda \mapsto (v \mapsto \lambda v)$ qui est canonique, i.e. indépendant du choix de v_1. Donc une représentation $\rho : G \to GL(V)$ est équivalente à un morphisme $G \to k^\times$. Si G est abélien et $k = \mathbb{C}$, alors $\rho : G \to \mathbb{C}^\times$ est simplement un caractère du groupe abélien G (voir la 1^{re} partie du cours).

(ii) Si G est un sous-groupe d'un groupe $GL(V)$ (par exemple si $\dim V < \infty$, on a $G = SL(V) \subset GL(V)$), alors l'inclusion $G \hookrightarrow GL(V)$ s'appelle la représentation **standard** ou **tautologique** de G.

(iii) Une représentation de G dans $V = k^n$ est donnée par une famille de matrices $\rho(g) \in GL_n(k)$ t.q. $\rho(gh) = \rho(g)\rho(h),\ \forall g, h \in G$.

(iv) Soit X un $G-$ensemble, c'est-à-dire un ensemble X muni d'une action de G (à gauche). Soit $V = kX$ l'espace vectoriel des combinaisons linéaires formelles d'éléments de X. Donc par définition, les éléments $1.x = e_x$ de X forment une base de kX. Pour tout $g \in G$, l'application $e_x \mapsto e_{gx}$ s'étend linéairement en un automorphisme linéaire $\rho(g) : kX = V \to kX = V$. On appelle (V, ρ) la **représentation de permutation** associée au $G-$ensemble X. Sous-exemples :

— $G = \mathfrak{S}_3$ agissant sur $X = \{1, 2, 3\}$. Alors kX s'identifie avec $V = k^3$ et $\rho : \mathfrak{S}_3 \to GL(kX)$ s'identifie avec la représentation $\rho : \mathfrak{S}_3 \to GL_3(k)$ par des matrices de permutation :

$$Id \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ (12) \mapsto \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \cdots, (123) \mapsto \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \cdots$$

— $X = G$ avec l'action $G \times X \to X$ donnée par la multiplication de G. Alors $V = kG$ devient une représentation de G (de dimension finie sur $|G| \leq \infty$).

Terminologie. *Le* ***degré*** *ou la* ***dimension*** *d'une représentation* (ρ, V) *est* $\dim V$.

6 Sous-représentations

Définition 6.1. Soit (ρ, V) une représentation. Une **sous-représentation** est un sous-espace $W \subset V$ t.q. $g.W \subset W$ pour tous $g \in G$. On appelle W aussi un **sous-espace invariant (ou G-invariant)**.

Remarque 6.2. Dans ce cas, l'action induite $G \times W \to W,\ (g, v) \mapsto gv$ fait de W une représentation de G, et l'action induite $G \times V/W \to V < W,\ (g, \bar{v}) \mapsto \overline{gv}$ fait de V/W une représentation.

Exemples 6.3. (i) Si (ρ, V) est une représentation, le sous-espace des vecteurs fixes $V^G = \{v \in V \mid g.v = v.\ \forall g \in G\}$ est toujours une sous-représentation de V.

(ii) Si $V = k^n$ est la représentation de permutation de $\mathfrak{S}_n$ (associée à l'action canonique $\mathfrak{S}_n \times \{1, \cdots, n\} \to \{1, \cdots, n\}$), alors $V_0 = \{x \in k^n \mid \sum_{i=1}^n x_i = 0\}$ est une sous-représentation. De même, la droite $V_1 = k \cdot \begin{bmatrix} 1 \\ \cdots \\ 1 \end{bmatrix}$ est une sous-représentation. D'ailleurs, on a $V = V_0 \oplus V_1$ s.s.i. $car(k)$ ne divise pas n.

Remarque 6.4. Soit ρ une représentation de G dans un espace vectoriel V de dimension finie. Soit $W \subset V$ un sous-espace. Soit $v_1, \cdots, v_p, v_{p+1}, \cdots, v_n$ une base de V t.q. $v_1, \cdots, v_p$ forment une base de $W \subset V$. Notons $T(g) \in GL_n(k)$ la matrice de $\rho(g)$ dans la base $v_1 \cdots, v_p \cdots, v_n$. (Les $T(g)$ définissent une représentation de G dans k^n.) le sous-espace $W \subset V$ est une sous-représentation de V s.s.i. on a

$$\forall g \in G, \quad \left[\begin{array}{c|c} T_1(g) & * \\ \hline 0 & T_2(g) \end{array}\right] \Big\} p$$

et alors la représentation induite dans W est décrite par les matrices $T_1(g),\ g \in G$ et la représentation induite dans V/W est décrite par les $T_2(g),\ g \in G$, dans la base $\pi(v_{p+1}), \cdots, \pi(v_n)$, où $\pi : V \to V/W$.

7 Morphismes

Définition 7.1. Si (V_1, ρ_1) et (V_2, ρ_2) sont deux représentations, un **morphisme** $f : (V_1, \rho_1) \to (V_2, \rho_2)$ est une application linéaire $f : V_1 \to V_2$ t.q. $f \circ \rho_1(g) = \rho_2(g) \circ f,\ \forall g \in G$.

Remarque 7.2. De façon équivalente : $f(g.v) = g.f(v), \forall v \in V,\ \forall g \in G$. Alors $ker(f)$, $im(f)$ et $cok(f)$ héritent de structures de représentations. ($ker(f) \subset V_1$, et $im(f) \subset V_2$ sont des sous-représentations et $cok(f) = V_2/im(g)$ une représentation quotient) :

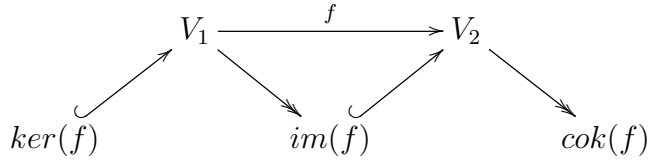


diagramme de représentations.

Définition 7.3. Un morphisme $f : (V_1, \rho_1) \to (V_2, \rho_2)$ est un **isomorphisme** si $f : V_1 \to V_2$ est bijective.

Remarques 7.4. *(i) Dans ce cas, la réciproque $f^{-1} : V_2 \to V_1$ est encore un morphisme.*

(ii) Deux représentations $\rho_1 : G \to GL_n(k)$ et $\rho_2 : G \to GL_n(k)$ sont isomorphes s.s.i. il existe une matrice $P \in GL_n(k)$ t.q. $\rho_2(g) = P\rho_1(g)P^{-1}$, $\forall g \in G$. Autrement dit, les familles de matrices $(\rho_1(g))_{g\in G}$ et $(\rho_2(g))_{g\in G}$ sont simultanément conjugués.

Exemples 7.5. (i) Une représentation $\rho : \mathbb{Z} \to GL_n(k)$ est équivalente à la donnée d'une seule matrice inversible $\rho(1)$ (car $\rho(k) = \rho(1)^k$, $k \in \mathbb{Z}$). Deux telles représentations sont isomorphes s.s.i. les matrices $\rho_1(1)$ et $\rho_2(1)$ sont semblables ($\Longleftrightarrow$ conjugués).

(ii) Une représentation de $\mathbb{Z}^2 \to GL_n(k)$ est équivalente à la donnée de deux matrices inversibles $A = \rho(\begin{bmatrix}1\\0\end{bmatrix})$ et $B = \rho(\begin{bmatrix}0\\1\end{bmatrix})$ qui commutent : $AB = BA$. Deux représentations données par (A_1, B_1) et (A_2, B_2) sont isomorphes s.s.i. (A_1, B_1) et (A_2, B_2) sont simultanément conjugués : on a $\begin{cases} PA_1P^{-1} = A_2 \\ PB_1P^{-1} = B_2 \end{cases}$ pour un $P \in GL_n(k)$.

8 Représentations indécomposables

Définition 8.1. Soient ρ_1 et ρ_2 des représentations de G dans des espaces V_1 et V_2, leur **somme directe** est la représentation de G dans $V_1 \oplus V_2$ donnée par

$$\begin{aligned} \rho_1(g) \oplus \rho_2(g) : V_1 \oplus V_2 &\to V_1 \oplus V_2 \\ (v_1, v_2) &\mapsto (\rho_1(g)(v), \rho_2(g)(v)) \end{aligned}$$

Remarque 8.2. Soient ρ_1 et ρ_2 des représentation dans k^p resp. k^q données par des familles de matrices $T_1(g) \in GL_p(k)$ et $T_2(g) \in GL_p(k)$. Alors $\rho_1 \oplus \rho_2$ est la représatation dans k^{p+q} donnée par les matrices

$$\left[\begin{array}{c|c} T_1(g) & 0 \\ \hline 0 & T_2(g) \end{array}\right] \in GL_{p+q}(k),\ g \in G$$

Définition 8.3. Une représentation est **indécomposable** si elle est non nulle et n'est pas isomorphe à la somme directe de deux représentations non nulles.

Exemple 8.4. Supposons $k = \mathbb{C}$ (ou k alg. clos quelconque). Soit $\lambda \in \mathbb{C}^\times$ et soit $n \geq 1$ un

entier. Soit

$$J_n(\lambda) = \begin{bmatrix} \lambda & 1 & 0 & & 0 \\ & \lambda & 1 & \ddots & \\ & & \ddots & \ddots & 0 \\ & & & \ddots & 1 \\ & & & & \lambda \end{bmatrix} \in GL_n(\mathbb{C}).$$

Soit $V_{n,\lambda}$ la représentation de $\mathbb{Z}$ dans k^n donnée par $J_n(\lambda)$. Alors clairement (forme normale de Jordan), toute représentation de dimension finie de $\mathbb{Z}$ est isomorphe à une somme directe de représentations $V_{n,\lambda} : V \simeq V_{n_1,\lambda_1} \oplus \cdots \oplus V_{n_r,\lambda_r}$.

Lemme 8.5. *$V_{n,\lambda}$ est indécomposable et donc toute représentation de de dimension finie de $\mathbb{Z}$ est isomorphe à une somme directe de représentations indécomposables uniques à isomorphisme et permutation près.*

Démonstration. Soit $U \subset V_{n,\lambda}$ une sous-représentation non nulle. On va montrer que $ke_1 \subset U$. Soit $u \in U$ un vecteur non nul. Ecrivons $u = c_1e_1 + \cdots + c_le_l$, où $c_l \neq 0$. Alors

$$U \ni (J_n(\lambda) - \lambda \cdot Id)^{l-1}(v) = \begin{bmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & 0 \end{bmatrix}^{l-1} (v) = c_le_1 \neq 0$$

Donc $0 \neq c_le_1 \in U$ et $ke_1 \subset U$. Donc si U_1 et U_2 sont deux sous-représentations non nulles, on ne peut avoir $U_1 \oplus U_2 = V_{n,\lambda}$ car $U_1 \cap U_2 \supset ke_1 \neq \{0\}$. Donc $V_{n,\lambda}$ est bien indécomposable. □

Théorème 8.6 (Krull-Remah-Schmidt)**.** *Soit G un groupe et soit k un corps. Toute représentation de dimemsion finie de G est somme directe de représentations indécomposables uniques à isomorphisme et permutatoion près.*

Remarque 8.7. Ce théorème réduit le problème de classification des représentations de dimension finie de G à celui de la classification des représentations indécomposables de dimension finie. Pour $G = \mathbb{Z}$, on connaît la solution du problème (blocs de Jordan si k est algébriquement clos, matrices compagnons de polynômes $P(X)^l$, $P(X) \in k[X]$ irréductible, $l \geq 1$, si k est quelconque). Pour un groupe G général sur un corps k général, ce problème est ouvert et, dans un certain sens, insoluble (problème "sauvage").

Définition 8.8. Soit V une représentation et $U \subset V$ une sous-représentation. Un **supplémentaire G-invariant** est une sous-représentation (donc $g.W \subset W,\ \forall g \in G$) t.q. $V = U \oplus W$. On dit que U est un **facteur direct (ou un sommand direct)** de V si U admet un supplémentaire G-invariant.

Exemple 8.9. Soient $G = \mathbb{Z}$ et $V = k^2$ avec $\rho : \mathbb{Z} \to GL_2(k),\ l \mapsto \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^l, l \in \mathbb{Z}$. Soit $U = ke_1$. Clairement, U est une sous-représentation. Mais U n'est pas un facteur direct. Si W était un supplémentaire $G-$invariant, alors on aurait $V = U \oplus W$ avec $U \neq \{0\}$ et $W \neq \{0\}$. Alors V serait décomposable. Or on vient de voir que V est indécomposable. Autre raison : la matrice $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ n'est pas diagonalisable. Or si on avait un supplémentaire $G-$invariant W de $U \subset V$, alors dans une base adaptée à la décomposition $V = U \oplus W$ ($\dim U = 1 = \dim W$), toutes les matrices $\rho(l)$ sont diagonales. Reformulation : la suite exacte de représentations $0 \to U \to V \to V/U \to 0$ n'est pas scindée en tant que suite exacte de représentations.

9 Représentations irréductibles

Définition 9.1. Une représentation V est **irréductible** si elle est non nulle et que ses seules sous-représentations sont $\{0\}$ et V.

Remarques 9.2. *(i) Donc V est irréductible s.s.i. V admet exactement deux sous-représentations (à savoir $\{0\}$ et V).*

(ii) Soit V une représentation. Si V est irréductible, alors V est indécomposable (car chaque facteur direct $0 \neq U \neq V$ est aussi une sous-représentation $\neq 0$ et $\neq V$). Par contre, une représentation indécomposable n'est pas irréductible en général. Par exemple, si $V = V_{n,\lambda}$ est la représentation indécomposable associée à

$$J_n(\lambda) = \begin{bmatrix} \lambda & 1 & 0 & & 0 \\ & \lambda & 1 & \ddots & \\ & & \ddots & \ddots & 0 \\ & & & \ddots & 1 \\ & & & & \lambda \end{bmatrix},\ n \geq 1,\ \lambda \in k^\times$$

alors ke_1 est une sous-représentation non nulle. Donc $V_{n,\lambda}$ est irréductible s.s.i. $n = 1$.

Cela peut arriver aussi si G est un groupe fini et $car(k) \mid |G|$, par exemple soit

$$G = \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \subset GL_2(\mathbb{F}_p)$$

alors la représentation tautologique $V = k^2$ est indécomposable mais non irréductible car $U = ke_1$ est une sous-représentation $\neq 0$ et $\neq V$. Notons que $|G| = (p-1)^2 p$. Donc $car(k) \mid |G|$ dans ce cas.

Lemme 9.3. *Soit G un groupe abélien. Supposons que k est algébriquement clos. Alors les représentations irréductibles de dimension finie sont celles de dimension 1.*

Remarques 9.4. *(i) Si G et k sont quelconques, les représentations de dimension 1 sont toujours irréductibles.*

(ii) Le groupe $\mathbb{Z}$ a la représentation $V = k[T, T^{-1}]$, où $l \in \mathbb{Z}$ agit par multiplication par T^l. Elle est irréductible et de dimension infinie.

(iii) Si k n'est pas algébriquement clos, il peut y avoir des représentations irréductibles de dimension finie > 1 même si G est abélien. Par exemple $G = \mathbb{Z}/3\mathbb{Z}$ admet la représentation irréducible $\rho : G \to GL_2(\mathbb{R})$ donnée par

$$\rho(\bar{l}) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^l, \ \bar{l} \in \mathbb{Z}/3\mathbb{Z}, \ \theta = \frac{2\pi}{3}$$

(facile : si $0 \neq U \subset \mathbb{R}^2$ est une sous-représentation, alors $U = \mathbb{R}^2$.)

Démonstration du lemme. Soit V une représentation irréductible de dimension finie de G. Soit $g \in G$. Soit $0 \neq W \subset V$ un sous-espace propre de $\rho(g)$ pour une valeur propre $\lambda \in k$ (k est alg. clos !). Montrons que W est une sous-représentation : Soit $h \in G$. Soit $w \in W$. A montrer : $\forall w \in W$, on a

$$g.(h.w) = (g.h).w = (h.g).w = h.(g.w) = h.(\lambda w) = \lambda h.w$$

Donc $h.w$ est encore vecteur propre pour la valeur propre λ de $\rho(g)$. Donc $h.w \in W$. Comme $0 \neq W$ et V est irréductible, on a $W = V$. Cet argument est valable pour tous les éléments $g \in G$ et montre que les $\rho(g),\ g \in G$ sont des homothéties. Donc toute droite $D \subset V$ est une sous-représentation. Comme V est irréductible, V est une droite. □

Exemple 9.5. Soit $G = \mathbb{Z}/n\mathbb{Z}$ et $k = \mathbb{C}$. Les représentations irréductibles de G sont de

dimension 1. Ce sont exactement les caractères $\chi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^\times$. On sait qu'ils sont de la forme $\chi_\zeta : \bar{k} \mapsto \zeta^k$, où ζ est une racine n-ème de l'unité.

Remarque 9.6. Si $n \geq 2$, les représentations standard de $GL_n(\mathbb{R})$ et $SL_n(\mathbb{R})$ dans $\mathbb{R}^n$ sont irréductibles car ces groupes agissent transitivement sur l'ensemble des droites (vectorielles) de $\mathbb{R}^n$. C'est aussi le cas pour les groupes $O_n(\mathbb{R})$ et $SO_n(\mathbb{R})$ car ces groupes agissent transitivement sur la sphère $S^{n-1} \subset \mathbb{R}^n$, et cette sphère engendre $\mathbb{R}^n$.

Exercice 9.7. Soit $G = \mathfrak{S}_3$ et soit $\widetilde{V} = \mathbb{C}^3$ la représentation de permutation associée au G-ensemble $\{1, 2, 3\}$. Soit $V = \{\ x \in \mathbb{C}^3 \mid \sum_1^3 x_i = 0\ \}$, montrer que V est irréductible et que $\dim V = 2$.

Définition 9.8. Si (V_1, ρ_1) et (V_2, ρ_2) sont deux représentations, leur **produit tensoriel** est l'espace $V_1 \otimes_k V_2$ muni de l'action donnée par les $\rho_1(g) \otimes \rho_2(g),\ g \in G$.

Exemple 9.9. Supposons que V_1 est de dimension 1. Donc $\rho_1 : G \to GL_1(k) = k^\times$ est un caractère. Alors $V_1 \otimes V_2$ est isomorphe à la représentation

$$\rho_{12} : G \to GL(V_2),\ g \mapsto \rho_1(g)\rho_2(g).$$

Clairement, les sous-représentations de ρ_{12} sont les mêmes que celles de ρ_2. En particulier, (V_2, ρ_{12}) est irréductible s.s.i. (V_2, ρ_2) est irréductible. En général, si V_1 et V_2 sont irréductibles et de dimension > 1, alors $V_1 \otimes_k V_2$ n'est pas irréductible, en général.

10 Représentations complètement réductibles

Définition 10.1. Une représentation V de G est **complètement réductible** si chaque sous-représentation $U \subset V$ est un facteur direct (i.e. il existe un sous-représentation $W \subset V$ t.q. $V = U \oplus W$).

Théorème 10.2. *Une représentation est complètement réductible s.s.i. elle est isomorphe à la somme directe d'une famille (éventuellement infinie) de représentations irréductibles.*

Démonstration. Pour la dimension complète voir l'appendice. Montrons que si V est complètement réductible et de dimension finie, alors V est somme directe de sous-représentation irréductibles : On procède par récurrence sur $\dim V$. Si V est irréductible, il n'y a rien à démontrer. Sinon, V admet une sous-représentation $0 \neq U \subsetneq V$. Par l'hypothèse , U est un facteur direct, donc il existe une sous-représentation $W \subset V$ t.q. $V = U \oplus W$. On a

$\dim U < \dim V$ et $\dim W < \dim V$. Par l'hypothèse de récurrence, U et W sont des sommes directes de sous-représentations irréductibles. Donc V aussi. □

Exemple 10.3. Soit $G = \mathbb{Z}$. Soit $k = \mathbb{C}$. Les représentations irréductibles de dimension finie de $\mathbb{Z}$ sont les $V_{1,\lambda},\ \lambda \in \mathbb{C}$, données par des matrices $[\lambda]$. Donc les représentations complètement réductibles $(V, \rho),\ \rho : \mathbb{Z} \to GL_n(\mathbb{C})$ sont à isomorphismeprès les $V_{1,\lambda_1} \oplus \cdots \oplus V_{1,\lambda_n},\ \lambda_i \in \mathbb{C}^\times$, c'est à dire que $\rho(1)$ est diagonalisable avec valeurs propres $\lambda_1, \cdots, \lambda_n$.

$$\rho(1) \underset{\text{semblable}}{\sim} \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}$$

Idée : Les représentations complètement réductibles de dimension $< \infty$ sont des généralisations des matrices diagonalisable.

Appendice : pour le cas de dimension infinie Soient G un groupe et k un corps.

Théorème 10.4. *Soit V une représentation. On a équivalence entre*

(i) V est complètement réductible.

(ii) V est la somme d'une famille de sous-représentations irréductibles.

(iii) V est la somme directe d'une famille de sous-représentations irréductibles.

Démonstration. Seule l'implication $(iii) \implies (ii)$ est claire. Le lemme suivant montre que $(ii) \implies (iii)$.

Lemme 10.5. *Soient V une représentation et $V_i \subset V,\ i \in I$ des sous-représentations irréductibles telles que $V = \sum_{i\in I} V_i$. Alors il existe $J \subset I$ tel que $V = \oplus_{i\in J} V_i$.*

Démonstration du lemme. Soit $J \subset I$ maximal tel que la somme $\oplus_{i\in J} V_i$ est directe. Montrons que $\oplus_{i\in J} V_i = V$. Soit $j \in J$. Si l'intersection $V_j \cap \oplus_{i\in J} V_i$ était nulle, alors V_j serait en somme directe avec $\oplus_{i\in J} V_i$ ce qui contredit la maximalité de J. Donc $V_j \cap \oplus_{i\in J} V_i$ est non nulle. Comme V_j est irréductible, l'intersection est égale à V_j et $V_j \subset \oplus_{i\in J} V_i$. Comme $j \in I$ est quelconque, on a $E = \sum_{i\in I} V_i \subset \oplus_{i\in J} V_i$. □

Montrons que $(iii) \implies (i)$: Supposons que $V = \oplus_{i\in I} V_i$, où les V_i sont irréductibles. Soit $F \subset V$ une sous-représentation. Soit $J \subset I$ maximal tel que la somme $F + (\oplus_{i\in J} V_i)$ est

directe. Soit $j \in I$. Alors $V_j \cap (F + (\oplus_{i\in J} V_i))$ est ou bien égal à V_j ou bien nul. Si c'est nul, la somme $F + (\oplus_{i\in J\cap\{j\}} V_i)$ est encore directe ce qui contredit la maximatité de J. Donc $V_j \subset F \oplus (\oplus_{i\in J} V_i)$ et comme j est quelconque, on a $F \oplus (\oplus_{i\in J} V_i) = V$.

Montrons que $(i) \Longrightarrow (ii)$: Montrons d'abord que toute sous-représentation non nulle de V contient une sous-représentation irréductible. Soit $0 \neq v \in V$. Considérons la sous-représentation

$$U = \left\{ \sum_{g\in G} c_g g.v \;\middle|\; c_g \in k,\ c_g = 0 \text{ sauf pour un nombre fini de } g \in G \right\}$$

Par le lemme de Zorn , elle admet une sous-représentation maximale $M \subset U$ telle que $V \notin M$. Par l'hypothèse, nous avons $V = M \oplus M'$ pour une sous-représentation $M' \subset V$. Nous avons alors $U = M \oplus (M' \cap U)$ (car si $u \in U$, alors $u = m + m'$ avec $m \in M$ et $m' \in M'$ et alors $m' = u - m \in M' \cap U$). Comme M est maximal dans U, le quotient $U/M \xrightarrow{\sim} M' \cap U$ est irréductible et bien sûr contenu dans U. Soit maintenant $V_0 \subset U$ la somme de toutes les sous-représentations irréductibles de V. Si on a $V_0 \neq V$, alors on a $V = V_0 \oplus W$ pour une sous-représentation $W \neq 0$ de V. Mais alors W contient une sous-représentation simple $S \subset V$ et on devrait avoir $S \subset V_0$. Contradiction ! □

A titre d'information, nous montrons aussi

Proposition 10.6. *Toute sous-représentation et tout quotient d'une représentation complètement réductible est complètement réductible.*

Démonstration. Soit V une représentation complètement réductible et soit $U \subset V$ une sous-représentation. Soit $U_0 \subset U$ la somme des sous-représentations irréductibles de U. Nous avons $V = U_0 \oplus W$ pour une sous-représentations W de V. Il s'ensuitque $U = U_0 \oplus (U \cap W)$ (car pour $u \in U$, on a $u = u_0 + w$ pour $u_0 \in U_0$ et $w \in W$ et alors $w = u - u_0 \in U \cap W$). Si $U \cap W$ est non nul, il contient une sous-représentation irréductible. C'est une contradiction. Donc $U = U_0$ et U_0 est complètement réductible. Si V/U est un quotient, on choisit U' tel que $U \oplus U' = V$ et alors on a $V/U \xrightarrow{\sim} U'$ qui est complètement réductible en tant que sous-représentation de V. □

Théorème 10.7 (Maschke)**.** *Si G est un groupe fini dont l'ordre n'est pas divisible par la caractéristique de k, alors toute représentation de G est complètement réductible. (par exemple c'est le cas si k est de caractéristique nulle)*

Première démonstration pour $k = \mathbb{R}$ ou $k = \mathbb{C}$ et $\dim V < \infty$. Soit $k \in \{\mathbb{R}, \mathbb{C}\}$. Soit (V, ρ) une représentation de dimension finie de G. Soit $< \cdot, \cdot >$ un produit scolaire resp. un produit scolaire hermitien si $k = \mathbb{R}$ resp. $k = \mathbb{C}$. (par exemple si $V = \mathbb{C}^n$, on peut prendre $< x, y >= \sum_{i=1}^n \bar{x}_i y_i$). Posons

$$\ll v, w \gg := \frac{1}{|G|} \sum_{g \in G} < g.v, g.w >$$

Exercice 10.8. (i) $\ll , \gg$ est encore un produit scolaire resp. un produit scalaire resp. un produit scalaire hermitien.

(ii) $\ll , \gg$ est G-invariant. i.e. $\ll h.v, h.w \gg = \ll v, w \gg$, $\forall v, w \in V$, $\forall h \in G$.

(iii) Soit $U \subset V$ une sous-représentation. Soit W son orthogonal pour $\ll , \gg$:

$$W = \{w \in V \mid \ll u, w \gg = 0, \ \forall u \in U \ \}$$

Alors $V = U \oplus W$ (car $\ll , \gg$ est un produit scolaire resp. scalaire hermitien) et W est $G-$invariant : $g.W \subset W$, $\forall g \in G$.

□

Deuxième démonstration dans le cas général. Soit $U \subset V$ une sous-représentation. Alors U est un sous-espace vectoriel. Soit $p_0 : V \to V$ une projection linéaire sur $U \subset V$, i.e. $im(p_0) = U$. Posons

$$p(v) = \frac{1}{|G|} \sum_{g \in G} g.p_0(g^{-1}v)$$

Alors $p : V \to V$ est encore une projection (exercice !) et son image est encore U (exercice !) On utilise que $g.U \subset U$, $\forall g \in G$. En outre, $p : V \to V$ est un morphisme de représentations (exercice !). Donc $ker(p) \subset V$ est une sous-représentation, on a

$$V = ker(p) \oplus im(p) = ker(p) \oplus U$$

Donc $W = ker(p)$ est bien un supplémentaire G-invariant de U. □

Lemme 10.9 (Schur)**.** *Soient G un groupe et soient V_1 et V_2 deux représentations irréductibles. Soit $f : V_1 \to V_2$ un morphisme. Alors*

(i) Ou bien f est nul ou bien f est un isomorphisme.

(ii) Si k est alg. clos et $V_1 = V_2$ et $\dim V_i < \infty$, alors f est une homothétie (= multiplication par un scalaire).

Démonstration. (i) : Si $f \neq 0$, alors $ker(f) \subsetneqq V_1$ et $0 \neq Im(f) \subset V_2$. Or V_1 et V_2 sont irréductible, et $ker(f)$ et $im(f)$ sont des sous-représentations. Donc $\{0\} = ker(f)$ et $Im(f) = V_2$. Donc f est un isomorphisme.

(ii) : Comme k est alg. clos et V_1 de dimension finie, l'endomorphisme $f : V_1 \to V_1$ admet une valeur propre λ. Alors $f - \lambda \cdot Id : V_1 \to V_1$ est un endomorphisme non inversible. Comme V_1 est irréductible, par (i), on a $f - \lambda \cdot Id = 0$. □

Terminologie. *La représentation de permutation kG associée à l'action $G \times G \to G$ de G sur lui-même par multiplication à gauche s'appelle* ***la représentation régulière****.*

Lemme 10.10. *Soit V une représentation. Alors pour tout $v \in V$, il existe un unique morphisme $f_v : kG \to V$ t.q. $f(e) = v$.*

Remarque 10.11. Soit $Hom_G(kG, V)$ espace des morphismes $kG \to V$, Alors autrement dit, on a un isomorphisme d'espaces vectoriel $Hom_G(kG, V) \xrightarrow{\sim} V,\ f \mapsto f(e)$ (propriété universelle de kG).

Démonstration. Pour $v \in V$, on définit $f_v : kG \to V$ par $f_v(g) = f_v(g.e) = g.f_v(e) = g.v$. Alors $f_v(e) = v$ et f_v est un morphisme (exercice !) et c'est la seule possibilité. □

Lemme 10.12. *Soit G un groupe. Alors toute représentation irréductible V de G est un quotient de kG. En particulier, si $|G| < \infty$, alors* $\dim V \leq \dim kG = |G|$.

Démonstration. Soit $0 \neq v \in V$. Soit $f : kG \to V$ l'unique morphisme t.q. $f(e) = v$. Alors $Im(f) \subset V$ est une sous-représentation non nulle. Comme V est irréductible, $Im(f) = V$ et V s'identifie au quotient de kG par $ker(f)$. □

Proposition 10.13. *Soit G un groupe fini dont l'ordre n'est pas divisible par $car(k)$. Alors toute représentation irréductible est un facteur direct de la représentation régulière kG. En outre, G n'admet qu'un nombre fini de représentations irréductibles à isomorphisme près et elles sont toutes de dimension $\leq |G|$*

Démonstration. Les hypothèses sur G et k impliquent que toute représentation de G est complètement réductible et donc somme directe d'une famille de représentations irréductibles. En particulier, on a $kG = V_1 \oplus \cdots \oplus V_r$ pour des sous-représentations irréductibles V_i. Soient V une représentation irréductible, $0 \neq v \in V$ et $p : kG \to V$ le morphisme t.q. $p(e) = v$. Alors p est surjectif car V est irréductible et $Im(p)$ est une sous-représentation non nulle. Soit $p_i : V_i \to V$ la restriction de p à $V_i \subset V$. Comme $p \neq 0$, on a $p_i \neq 0$ pour un i. Mais alors, par le lemme de Schur, p_i est un isomorphisme. Donc $V \sim V_i$ est facteur direct de kG. □

Exemple 10.14. Soit G un groupe. Alors G admet toujours la **représentation triviale** $V = k$ avec $g.v = v$, $\forall v \in V,\ \forall g \in G$. Elle est irréductible (toute représentation de dim 1 est irréductible) . Si $G = \{e\}$, alors pour tout espace vectoriel V, il n'y a qu'un seul morphisme $\rho : G \to GL(V)$. Donc la donnée de (V, ρ) est équivalente de celle de V et tout sous-espace vectoriel est $G-$invariant. Donc pour $G = \{e\}$,

$$\{ \text{ représentations de } G \} = \{ \text{ espaces vectoriels } \}$$

$$\{ \text{ morphismes } \} = \{ \text{ applications linéaire } \}$$

Donc comme tout espace vectoriel V de dimension ≥ 2 admet un sous-espace $U \subset V$ t.q. $0 \neq U \neq V$, les représentation irréductible de G sont exactement les espaces vectoriels de dimension 1. Ils sont tous isomorphes à k. Donc k est l'unique représentation irréductible à isomorphisme près. Dans ce cas, le lemme 10.5 est équivalent au fait suivant bien connu : Toute famille génératrice $(v_i)_{i\in I}$ d'un espace vectoriel V contient une base $(v_i)_{i\in J}$, où $J \subset I$.

Proposition 10.15. *Soit V une représentation.*

*(i) Soit S une représentation irréductible. Soit $V_S := \sum_{f:S\to V} Im(f)$, où f parcourt l'ensemble des morphismes $f : S \to V$. Alors $V_s \subset V$ est la plus grande sous-représentation de V isomorphe à une somme directe de copies de S. On l'appelle **la composante isotypique de type S** de V.*

(ii) Soit $\mathcal{J}$ un système de représentants des classes d'isomorphisme de représentations irréductibles de G. Alors la somme $\sum_{S\in\mathcal{J}} V_S$ est directe et $\oplus_{S\in\mathcal{J}} V_S$ est la plus grande sous-représentation complètement réductible de V. En particulier, V est complètement réductible s.s.i. $V = \oplus_{S\in\mathcal{J}} V_S$

Démonstration. (i) : Par le lemme 10.5, la somme $V_s = \sum_{f:S\to V} Im(f)$ est bien isomorphe à une somme directe de copies de S. Soit $U \subset V$ une sous-représentation telle qu'il existe un isomorphisme $\varphi : \oplus_{i\in I} S \xrightarrow{\sim} U$ Soit $inc_j : S \hookrightarrow \oplus_{i\in I} S$ l'inclusion du facteur étiqueté par $j \in I$. Alors la composition $inc_j : S \hookrightarrow \oplus_{i\in I} S \xrightarrow[\varphi]{\sim} U \hookrightarrow V$ est un morphisme $f : S \to V$. Donc son image est dans V_s. Comme $j \in I$ est quelconque , on a $U \subset V_S$.

(ii) : Soit $S \in \mathcal{J}$. Considérons $U = \sum_{S'\in\mathcal{J}\setminus\{S\}} V_{S'}$. Par le lemme 10.5, on a $U \sim \oplus_{i\in I} S_i$ où les S_i sont irréductibles et non isomorphes à S. On a aussi $V_S \sim \oplus_{i\in J} S$ pour un ensemble J. Comme $V_S \cap U \subset V_S$ est un facteur direct (car V_S est complètement réductible), il existe un morphisme $p : V_S \to V_S \cap U$ t.q. $p|_{V_S\cap U} = Id_{V_S\cap U}$. Alors la composition $\oplus_{i\in J} S \sim V_S \xrightarrow{p} V_S \cap U \hookrightarrow U = \oplus_{i\in I} S_i$ est un morphisme $\oplus_{i\in J} S \xrightarrow{f} \oplus_{i\in I} S_i$. Notons $proj_l : \oplus_{i\in I} S_i \to S_l$ la

projection sur le facteur S_l. Alors $proj_l \circ f \circ inc_j$ est un morphisme $S \xrightarrow{g} S_l$. Or S et S_l sont irréductibles et non isomorphes. Donc $g = O$ (lemme de Schur). Donc $f = 0$ et $V_S \cap U = \{0\}$. Montrons que $\oplus_{S\in\mathcal{J}} V_S \subset V$ est la plus grande sous-représentation complètement réductible de V. Soit $U \subset V$ une sous-représentation complètement réductible. On a un isomorphisme $\oplus_{i\in I} S_i \xrightarrow[\varphi]{\sim} U$, où les S_i sont irréductibles. Alors $\varphi(S_i) \subset V_S$ si $S \in \mathcal{J}$ et $S_i \sim S$. Donc $\varphi(S_i) \subset \oplus_{S\in\mathcal{J}} V_S$ et $U = \oplus_{i\in I}\varphi(S_i) \subset \oplus_{S\in\mathcal{J}} V_S$. □

Soit G un groupe fini dont l'ordre n'est pas divisible par la caractéristique de k.

Rappel 10.16. *Toute représentation de G est complètement réductible ($\iff$ somme directe de représentation irréductibles). À isomorphisme près, G n'admet qu'un nombre fini de représentations irréductibles $S_1, \cdots, S_l$ et $\dim S_i \leq |G|$.*

Corollaire 10.17. *Soit V une représentation de dimension finie de G. Alors V est la somme directe de ses composantes isotypique V_{S_i}, et $V_{S_i} \sim S_i^{n_i}$ pour des entiers $n_i \geq 0$ uniques.*

Remarque 10.18. En particulier une représentation de G de dimension finie est irréductible s.s.i. elle est indécomposable.

Proposition 10.19. *Par la proposition, on a $V = \oplus_{i=1}^{l} V_{S_i}$ et $V_{S_i} \sim S_i^{n_i}$. Il reste à montrer l'unité des n_i. Montrons que si S est irréductible et $S^P \sim S^n$, alors $p = n$.(voir la remarque après la démonstrationpour un argument simple) Soit $\varphi : S^P \to S^n$ un isomorphisme. Procédons par récurrence sur $p \geq 0$. Si $p = O$, alors $S^P = \{0\}$ et $S^n = \{0\}$ et $n = 0$. Supposons $p \geq 1$. Notons $proj_i : S^n \to S$ la projection sur les facteur étiqueté par i et $inc_j : S \to S^P$ l'inclusion du facteur étiqueté par j. Posons $\varphi_{ij} = proj_i \circ \varphi \circ inc_j$. Si $x = \begin{bmatrix} x_1 \\ \vdots \\ x_p \end{bmatrix} \in S^p$, alors on a $\varphi(x) = \sum_{i=1}^{n} \varphi_{ij}(x_j)$. Autrement dit, φ est donné par la matrice*

$$(\varphi_{ij}) = \begin{bmatrix} \varphi_{11} & \cdots & \varphi_{1p} \\ \vdots & & \vdots \\ \varphi_{n1} & \cdots & \varphi_{np} \end{bmatrix}$$

à coefficients dans $D = Hom(S, S) = \{f : S \to S \mid f \text{ morphismes }\}$ Notons que D est une algèbre non commutative en général, mais où tout élément non nul est inversible. On dit que D est une "algèbre à division" ou un "corps gauche". Si la première colonne est nulle, alors $ker(\varphi) \neq 0$. C'est une contradiction car φ est un isomorphisme. Quitte à renuméroter

les facteurs, on peut supposerque $\varphi_{11} \neq 0$ *et donc* φ_{11} *est inversible, Quitte à composer à gauche avec l'automorphisme de* S^n *de matrice* $\begin{bmatrix} \varphi_{11}^{-1} & & & \\ & Id_S & & \\ & & \ddots & \\ & & & Id_S \end{bmatrix}$ *on peut supposer que* $\varphi_{11} = Id_S$. *Alors si on compose successivement avec l'automorphisme de* S^n *de matrice* $\begin{bmatrix} Id_S & & & \\ & \ddots & & \\ -\varphi_{i1} & & \ddots & \\ & & & Id_S \end{bmatrix}$, *on peut supposer que la première colonne de la matrice est* $\begin{bmatrix} Id_S \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ *Alors* $\varphi : S^p \xrightarrow{\sim} S^n$ *envoie le premier facteur* $S \subset S^p$ *par* Id_S *sur le premier facteur* $S \subset S^n$. *Donc on a un diagramme commutatif aux lignes exactes*

$$\begin{array}{ccccc} S & \xrightarrow{inc_1} & S^p & \twoheadrightarrow & S^p/inc_1(S) \sim S^{p-1} \\ {\scriptstyle Id}\downarrow\sim & & {\scriptstyle \varphi}\downarrow\sim & & {\scriptstyle \bar{\varphi}}\downarrow\sim \\ S & \xrightarrow[inc_1]{} & S^n & \twoheadrightarrow & S^n/inc_1(S) \sim S^{n-1} \end{array}$$

où φ *est encore un isomorphisme. Donc* $p - 1 = n - 1$ *par récurrence.*

Remarque 10.20. Soit S une représentation irréductible et soient $p, n \in \mathbb{N}$ tels que $S^p \sim S^N$. **Si** $\dim S < \infty$**, il est immédiat que** $p = n$ **car alors**

$$p \cdot \dim S = \dim S^P = \dim S^n = n \cdot \dim S.$$

La démonstration ci-dessus montre que l'on a $p = n$ même si S est de dimension infinie !

Exemple 10.21. $G = \mathbb{Z}/2\mathbb{Z}$, $k = \mathbb{C}$, alors il y a 4 de représentations de dimension 3 de G à isomorphisme près. En effet, G est fini et $car(\mathbb{C}) = 0$ ne divise par $|G| = 2$. Donc chaque représentation est somme directe de représentations irréductibles. G est abélien. Donc ses représentations irréductibles de dimension finie sont de dimension 1. Donc elles sont données par des caractères, i.e. des morphismes $\rho : (\mathbb{Z}/2, +) \to \mathbb{C}^*$. Il y en a 2 :

$$\begin{aligned} &\rho_1 : \mathbb{Z}/2 \to \mathbb{C}^\times, \quad \bar{k} \mapsto 1 \quad \text{trivial} \ : \ V_1 \\ &\rho_2 : \mathbb{Z}/2 \to \mathbb{C}^\times, \quad \bar{k} \mapsto (-1)^k \quad \text{sign} \ : \ V_2 \end{aligned}$$

Toute représentation de dimension 3 V est somme directe $V \sim V_1^{n_1} \oplus V_2^{n_2}$ pour des n_1, n_2

uniques t.q. $n_1 + n_2 = 3$. Donc

$$\left|\left\{ V \,\middle|\, V \text{ représentation de dimension } 3 \right\}/\text{isomophisme}\right| = \left|\left\{ (n_1, n_2) \in \mathbb{N}^2 \,\middle|\, n_1 + n_2 = 3 \right\}\right| = 4$$

Appendice : la réciproque du Théorème de Maschke

Proposition 10.22. *Si G est un groupe fini dont l'ordre est divisible par la caractéristique du corps, alors la représentation régulière kG n'est pas complètement réductible.*

Démonstration. Soit d l'élément $\sum_{h\in G} h$ de kG et $D = kd$ la droite de kG engendrée par d. Clairement $D \subseteq kG$ est une sous-représentation (isomorphe à la représentation triviale). Supposons qu'on a $kG = D \oplus E$ pour une sous- représentation $E \subseteq KG$. Montrons que $E = H$ où H est l'hyperplan $H = \{\sum_{g\in G} c_g g | \sum_{g\in G} c_g = 0\}$. Nous avons $dimH = |G| - 1 = dimE$. Donc il suffit de montrer que $E \subseteq H$. En effet soit $x = \sum_{g\in G} c_g g$ dans E. Alors on a aussi $\sum_{h\in G} h.x \in E$. Or nous avons $\sum_{h\in G} h.x = \sum_{h\in G} h \sum_{g\in G} c_g g = \sum_{g\in G} c_g \sum_{h\in G} hg = \sum_{g\in G} c_g \dot{d}$. Donc l'élément $\left(\sum_{g\in G} c_g\right)\cdot$dest dans $E \cap D = \{0\}$ et on doit avoir $\sum_{g\in G} c_g = 0$ car le vecteur d est non nul. Or, comme $car(k)$ divise $|G|$, le vecteur $d = \sum_{h\in G} h$ est dans H et donc $D \subseteq H = E$. C'est une contradiction car $E \cap D = \{0\}$. □

11 Caractères

Hypothèses : On considère les représentations d'un groupe fini G sur le corps $k = \mathbb{C}$.

Définition 11.1. Soit (V, ρ) une représentation de dimension finie de $|G|$. Le **caractère** $\chi_V = \chi_\rho$ de (V, g) est la fonction

$$G \to \mathbb{C} \quad g \mapsto \mathrm{tr}(\rho(g))$$

Lemme 11.2. *(i)* $\chi_V(e) = \dim V$.

(ii) $\chi_V(gxg^{-1}) = \chi(x),\ \forall g, x \in G$, *c'est-à-dire que* χ *est une* ***fonction centrale sur G****.*

Démonstration. *(i)* $\chi_V(e) = \mathrm{tr}(\rho(e)) = \mathrm{tr}(Id_V) = \dim V$.

(ii) $\chi_V(gxg^{-1}) = \mathrm{tr}(\rho(gxg^{-1})) = \mathrm{tr}(\rho(g)\rho(x)\rho(g^{-1})) = \mathrm{tr}(\rho(x)) = \chi_V(x)$. □

Notation. *Si $f : G \to \mathbb{C}$ est une fonction centrale, et C une classe de conjugaison, on note $f(C) = f(x)$, pour n'importe quel $x \in C$. On note $C(G)$ l'espace des fonctions centrales sur G. Les fonctions caractéristiques des classes de conjugaison de G forment une base de $C(G)$. Donc*

$$\dim C(G) = \left| \{ \textit{classes de conjugaison de } G \} \right|$$

Exemples 11.3. — Soit $V = \mathbb{C}G$ la représentation régulière. Pour tout $g \in G - \{e\}$, on a $gx \neq x, \forall x \in G$.Donc les coeff. diagonaux de la matrice de $\rho(g)$ ddans la base des $x \in G$ de $\mathbb{C}G$ sont nuls si $g \neq e$. D'où

$$\chi_{\mathbb{C}G}(g) = \begin{cases} |G| & g = e \\ 0 & g \neq e \end{cases}$$

— Soit Dn le groupe diédral d'ordre 2n, on a

$$Dn \subseteq O(2) \subseteq GL_2(\mathbb{R}) \subseteq GL_2(\mathbb{C}).$$

On obtient une représentation de D_n, dans $\mathbb{C}^2$. On a

$$D_n = \{e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

où

$$r = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \theta = \frac{2\pi}{n}, s = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

On a $\chi_V(e) = 2,\ \chi_V(r^k) = 2\cos(k\theta) = \chi_V(r^{-k})$, donc $\chi_V(sr^k) = 0, \forall 0 \leq k \leq n-1$, car sr^k est une symétrie par rapport à une droite donc semblable à $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

— Le groupe $\mathfrak{S}_3$ possède 3 classes de conjugaison :
$\{e\}, \{(12), (13), (23)\}, \{(123), (132)\}$(notons que $\mathfrak{S}_3 \simeq D_3$). Le caractère de la représ. de permutation dans$\mathbb{C}^3$ associée à $\{1, 2, 3\}$ avec l'action naturelle est donné par $\chi_V(e) = 3, \chi_V((12)) = 1, \chi_V((123)) = 0$.

— Plus généralement, on saitque les classes de conjugaison du g_σ : gym. $\mathfrak{S}_n$ sont en bijection avec les partitions de n , c'est- à - dire les suites $1 \leq k_1 \leq k_2 \leq \ldots \leq k_r, k_1 + \ldots + k_r = n$ qui donnent les longueurs des cycles (y compris les cycles de longueur 1) dans la décampas. en produitde cycles à supports disjoints d'unepermutation. P.ex

$$\sigma = (123)(45)(67)(8)(9) \rightsquigarrow (k_i) = (1, 1, 2, 2, 3)$$

Si V= en est la repr̀s. de permutation de $\mathfrak{S}_n$ associée à $\{1, 2, \ldots, n\}$ alors $\chi_V(\sigma) = |\{points\ fixes\ de\ \sigma\}| = |\{\ i|\ k_i(\sigma) = 1\ \}|$

Définition 11.4. Soient V, W des représentations. On définit des structures de représentations sur

(a) V^* par $(g \cdot f)(v) = f(g^{-1}\ v)$, $\forall g \in G, \forall f \in V^*, \forall v \in V$

(b) $V \otimes W$ par $g.(v \otimes w) = (g.v) \otimes (g.w)$, $\forall g \in G, \forall v, w \in V$

Lemme 11.5. *Soient V, W des repr̀s. de dim. finie,*

a) Si $V \simeq W$, alors $\chi_V = \chi_W$

b) On a $\chi_{V\oplus W} = \chi_V + \chi_W$

c) Si $W \subseteq V$ est une ss-repr̀s, alors $\chi_V = \chi_W + \chi_{V/W}$

d) On a $\chi_{V\otimes W} = \chi_V \cdot \chi_W$

Démonstration. a) Soit $f : V \xrightarrow{\sim} W$ un isomorphisme,

$$tr(\rho_W(g)) = \mathrm{tr}(f \circ \rho_V(g) \circ f^{-1}) = \mathrm{tr}(\rho_V(g))$$

b) $tr(\rho_V(g) \oplus \rho_W(g)) = tr(\left[\begin{array}{c|c} \rho_V(g) & 0 \\ \hline 0 & \rho_W(g) \end{array}\right]) = tr(\rho_V(g)) + tr(\rho_W(g))$

c) On choisit une base adaptée à l'inclusion $W \subseteq V$, On écrit $R_V(g)$pour la matrice de $\rho_V(g)$, etc.

$$tr(R_V(g)) = tr(\left[\begin{array}{c|c} R_W(g) & \star \\ \hline 0 & R_{V/W}(g) \end{array}\right]) = \mathrm{tr}(R_W(g)) + tr(R_{V/W}(g))$$

d) On montre (en choisissant des bases) que

$$tr(\alpha \oplus \beta) = tr(\alpha)tr(\beta)$$

Si $\alpha : V \to V$ et $\beta : W \to W$ sont des appl. linéaires. Soit $\mathbb{C}^G$ l'espace des fonctions $f : \mathbb{C} \to \mathbb{C}$. On munit $\mathbb{C}^G$ de la forme bilinéaire symétrique

$$< f_1, f_2 >= \frac{1}{|G|} \sum_{g\in G} f_1(g^{-1}) f_2(g)$$

Pour $g \in G$, soit $\epsilon_g : G \to \mathbb{C}$ la fonction caractéristique de $\{g\}$. On a $< f, \epsilon_g >= \frac{1}{|G|} f(g^{-1})$, Cela montre que $<,>$ est non dégénérée

□

Théorème 11.6. *Les caractères des représentations irréductibles de dimension finie de G forment une base orthonormée de l'espace $\mathcal{C}(G) \subseteq \mathbb{C}^G$, Plus précisément, soit$V_1, \ldots, V_r$ un système de représentants des classes d'isomorphisme des représ. irréductibles de dim. finie. Alors $\chi_{V_1}, \ldots, \chi_{V_r}$ forment une base orthonormée de $\mathcal{C}(G)$.*

Remarque 11.7. En particulier , le nombre de représ. irréductibles (à isomorphismeprès) est égal au nombre de classes de conjugaison de G.

Démonstration. Soient V, W deux représentations et $\mathrm{Hom}_{\mathbb{C}}(\mathrm{V}, \mathrm{W})$ l'espace des applications linéaires $V \to W$.On munit $\mathrm{Hom}_{\mathbb{C}}(\mathrm{V}, \mathrm{W})$ d'une structure de représentation par

$$g.u = \rho_W(g) \circ u \circ \rho_V(g)^{-1} \quad u \in \mathrm{Hom}_{\mathbb{C}}(\mathrm{V}, \mathrm{W}), g \in G$$

Alors le ss-espace

$$\mathrm{Hom}_{\mathbb{C}}(\mathrm{V}, \mathrm{W})^G = \{u \in \mathrm{Hom}_{\mathbb{C}}(\mathrm{V}, \mathrm{W}) |\ g.u = u\}$$

est exactement l'espace $\mathrm{Hom}_{\mathbb{C}}(\mathrm{V}, \mathrm{W})$ des morphismes $V \to W$

On définit

$$\begin{aligned} \pi : \mathrm{Hom}_{\mathbb{C}}(\mathrm{V}, \mathrm{W}) &\longrightarrow \mathrm{Hom}_{\mathbb{C}}(\mathrm{V}, \mathrm{W}) \\ u &\longmapsto \frac{1}{|G|} \sum_{g \in G} g.u \end{aligned}$$

Lemme 11.8. *l'application π est un projecteur d'image* $\mathrm{Hom}_{\mathbb{C}}(\mathrm{V}, \mathrm{W})$ *et $tr(\pi) = dim\mathrm{Hom}_{\mathbb{C}}(\mathrm{V}, \mathrm{W}) =< \chi_V, \chi_W >$*

Démonstration. Montrons que π est un morphisme

$$\pi(h.u) = \frac{1}{|G|} \sum_{g \in G} g.(h.u) = \frac{1}{|G|} \sum_{g \in G} (gh).u = \frac{1}{|G|} \sum_{k \in G} k.u = \pi(u)$$
$$h.\pi(u) = \frac{1}{|G|} \sum_{g \in G} h.(g.u) = \frac{1}{|G|} \sum_{g \in G} (hg).u = \frac{1}{|G|} \sum_{k \in G} k.u = \pi(u)$$

Donc π en un morphisme, $Im(\pi) \subseteq Hom_G(V, W)$ et on voit que $\pi_{Hom_G(V,W)} = Id_{Hom_G(V,W)}$

Il s'ensuit que $\pi \circ \pi = \pi$ et $Im(\pi) = Home_G(V, W)$. Calulons $tr(\pi)$: Soient $v_1, \ldots, v_p$ une base de V, $w_1, \ldots, w_q$ une base de W. Soit $e_{i,j} : V \longrightarrow W$ l'appl. lin. de matrice $E_{i,j}$ (1 en

position (i,j), 0 ailleurs). Les $e_{i,j}$ forment une base de $Hom_G(V,W)$, et on a

$$(g.e_{i,j})_{k,l} = \left(\rho_W(g) \circ e_{i,j} \circ \rho_V(g)^{-1}\right)_{k,l} = \rho_W(g)_{k,i} \circ \rho_V(g^{-1})_{j,l}$$

On en déduit que l'on a

$$tr(\pi) = \sum_{i,j} \pi(e_{i,j})_{i,j} = \sum_{i,j} \frac{1}{|G|} \sum_{k\in G} \rho_W(g)_{i,i} \circ \rho_V(g^{-1})_{j,j}$$
$$= \frac{1}{|G|} \sum_{k\in G} (\sum_i \rho_W(g)_{i,i})(\sum_j \rho_V(g^{-1})_{j,j}) =< \chi_V, \chi_W > .$$

Si V, W sont irréductibles, alors, par le lemme de Schur, on a

$$Hom_G(V,W) \cong \begin{cases} \mathbb{C} & V \cong W \\ 0 & V \ncong W \end{cases}$$

Il s'ensuit que $< \chi_{V_i}, \chi_{V_j} >= \delta_{ij}$. Il reste à montrer que les χ_{V_i} engendrent $\mathcal{C}(G)$ □

Lemme 11.9. *Soit V une reprès de dim. finie de G, Soit $f \in \mathcal{C}(G), Onpose$*

$$f_V = \frac{1}{|G|} \sum_{g\in G} f(g)\rho(g^{-1}) \in End_{\mathbb{C}}(V)$$

a) On a $f_V \in End_G(V)$ et $tr(f_V) =< f, \chi_V >$

b) Si V est irréductible, f_V est l'homothétie de rapport $< f, \chi_V > /dimV$

Démonstration. a) Soit $h \in G$, On a

$$h.f_V = \rho(h) \circ f_v \circ \rho(h)^{-1} = \frac{1}{|G|} \sum_{g\in G} f(g)\rho(h)\rho(g^{-1})\rho(h)^{-1}$$
$$= \frac{1}{|G|} \sum_{g\in G} f(g)\rho(hg^{-1}h^{-1}) = \frac{1}{|G|} \sum_{a\in G} f(h^{-1}ah)\rho(a) = f_v$$

$$tr(f_V) = \frac{1}{|G|} \sum_{g\in G} f(g)tr(\rho(g^{-1})) =< \chi_V, f >$$

b) Si V est irréductible , alors f_V est une homothétie par le lemme de Schur car $dimV \leq \infty$ et $\mathbb{C}$ est alg. clos, comme la trace de f_V vaut $< \chi_V, f >$, son rapport vaut $< f, \chi_V > /dimV$.

□

Fin de la dém du Thm Soit $f \in \mathcal{C}(G)$. Supposons que f est orthogonale à tous les caractères de repés. irréductibles. Par le lemme 2, on a $f_V = 0$ pour toute représentation irréductible V de G.Or toute représ. W est somme directe de représentations irréductibles (Maschke). En outre, on a $f_{V_1 \oplus V_2} = f_{V_1} \oplus f_{V_2} : V_1 \oplus V_2 \longrightarrow V_1 \oplus V_2$ pour toutes les représ. V_1, V_2. Donc $f_V = 0$ pour toute représentation de dimension finie. En particulier $f_V = 0$ si $V = \mathbb{C}G$ est la représentation régulière. On a

$$0 = f_{\mathbb{C}G}(e) = \frac{1}{|G|} \sum_{g \in G} f(g) \rho_{\mathbb{C}G}(g^{-1})(e) = \frac{1}{|G|} \sum_{g \in G} f(g) g^{-1} \in \mathbb{C}G$$

Comme les g^{-1} forment une base de $\mathbb{C}G$, on a $f(g) = 0, \forall g \in G$. □

Corollaire 11.10. *a) Le nombre de classes de conjugaison de G est égal au irréductibles nombre de classes de d'isomorphisme de représentations irréductibles de G.*

b) Soit $\chi_1, \ldots, \chi_l$les caractères d'un système de représentations des classes d'isomorphisme de représentants irréductibles. Soient C_1, C_2 deux classes de conjugaison. Alors

$$\sum_{i=1}^{l} \chi_i(C_1^{-1}) \chi_i(C_2) = \begin{cases} \frac{|G|}{|C_1|} & si\ C_1 = C_2 \\ 0 & sinon \end{cases}$$

Démonstration. a) est clair.

b) Soit 1_{C_1} la fonction caractéristique de la classe de conjugaison C_1 , Comme les χ_i forment une base orthonormée de $\mathcal{C}(G)$, on a

$$1_{C_1} = \sum_{i=1}^{l} < \chi_i, 1_{C_i} > \chi_i = \sum_{i=1}^{l} \left(\frac{1}{|G|} \sum_{g \in G} \chi_i(g^{-1}) 1_{C_1}(g) \right) \chi_i \tag{11.1}$$

$$= \sum_{i=1}^{l} |C_1| \cdot \chi_i(C_1^{-1}) \chi_i \tag{11.2}$$

Si on évalue cette égalité en C_2, on obtient l'affirmation.

□

Théorème 11.11. *Soient $S_1, \ldots, S_l$ un système de représentants des classes d'isom. de représentations irréductibles. Soit (V, ρ) une représentation de dimension finie. Soit $V = \bigoplus_{i=1}^{l} V_{S_i}$*

sa décomposition en composantes isotypiques. Alors la projection sur V_{S_i} est donnée par

$$p_i = \frac{dim\ S_i}{|G|} \cdot \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\rho(g^{-1})$$

où χ_i est le caractère de S_i.

Démonstration. Soit $f \in \mathcal{C}(G)$ une fonction centrale . Rappelons que

$$f_V = \frac{1}{|G|} \sum_{g \in G} f(g)\rho(g^{-1})$$

est un endomorphisme de V. Clairement, si on restreint$f_V : \bigoplus V_{S_i} \longrightarrow \bigoplus V_{S_i}$ à V_{S_j}, on obtient f_{V_Sj}. On sait par le lemme 2 que f_{Sj} est l'homothétie de rapport $< f, \chi_j > /dimS_j$. Comme V_{Sj} est une somme directe de copies de S_j , la restriction de f_V à V_{Sj} est aussi l'homothétie de rapport $< f, \chi_j > /dimS_j$. On applique ceci à la fonction centrale $f = \chi_i$ et on utilise l'orthonormalité de la base des χ_i pour déduire l'affirmations. □

Théorème 11.12. *Soient $S_1, \ldots, S_l$ comme avant. Soit V une représ. de dimension finie. Décomposons-la en $V \cong \bigoplus_{i=1}^{l} S_i^{n_i}$. Soit χ le caractère de V et soit χ_i le caractère de S_i*

a) On a $n_i =< \chi, \chi_i >$ et $< \chi, \chi >= \sum_{i=1}^{l} n_i^2$.

b) V est isomorphe à une autre représentation V' ssi $\chi = \chi'$, où χ' est le caractère de V'.

c) La représentation Vest irréductible ssi $< \chi, \chi >= 1$.

d) La représentation régulière $\mathbb{C}G$ se décompose en

$$\mathbb{C}G \cong \bigoplus_{i=1}^{l} S_i^{dimS_i}$$

En particulier, on a $|G| = \sum_{i=1}^{l} (dim\, S_i)^2$.

Démonstration. a) On a $\chi = \sum_{i=1}^{l} n_i\, \chi_i$ et par l'orthonormalité, on a $n_i =< \chi, \chi_i >$ et $< \chi, \chi >= \sum_{i=1}^{l} n_i^2$.

b) Donc χ détermine les n_i et $V \cong \bigoplus_{i=1}^{l} S_i^{n_i}$.

c) la représentation V est irréductible ssi exactement l'un des n_i vaut 1 et les autres 0 ssi $\sum_{i=1}^{l} n_i^2 = 1$ ssi $< \chi, \chi >= 1$.

d) Si $V = \mathbb{C}G$, on sait que $\chi = |G| \cdot 1_{\{e\}}$. Donc $< \chi_i, \chi_i >= \frac{1}{|G|} \sum_{g \in G} |G| \cdot 1_{\{e\}}(g)\chi_i(g^{-1}) = \chi_i(e) = dim\, S_i$. Donc $\mathbb{C}G \cong \bigoplus_{i=1}^{l} S_i^{dim S_i}$.

□

Proposition 11.13. *G est abélien ssi toutes ses représentations irréductibles sont de dimention 1.*

Remarque 11.14. G est est abélien Ssi le nombre de ses classes de conjugaison est égal à son ordre $|G|$.

Démonstration. " $\Rightarrow$ " déjà connu.

" $\Leftarrow$ " : Soient $S_1, \ldots, S_l$ comme avant. Supposons que $dim\, S_i = 1$, $\forall i$. Alors $|G| = \sum_{i=1}^{l} (dim\, S_i)^2 = l$. Mais l est égal au nombre de classes de conjugaison . Par la remarque, G est abélien. □

12 Table des caractères

Soient G un groupe fini et (V, ρ) une représentation complexe de dimension finie de G.

Remarques 12.1. *1) Soit $n = /G/$. Alors $g^n = e$, $\forall g \in G$, et donc $\rho(g)^n = Id_V$ pour tout $g \in G$. Donc $\rho(g)$ est diagonalisable et ses valeurs propres sont des racines n - èmes de l'unité.*

2) Il s'ensuit que $\chi(g^{-1}) = tr(\rho(g)^{-1}) = \overline{tr(\rho(g))} = \overline{\chi(g)}$ On a donc

$$< \chi_V, f >= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_V(g)} f(g) \quad \textit{pour toute } f \in \mathbb{C}^G.$$

3) Si $\chi_1, \ldots, \chi_l$sont les caractères de $S_1, \ldots, S_l$ comme avant, on sait que pour des classes de conjugaison C_1, C_2, on a

$$\sum_{i=1}^{l} \overline{\chi_i(C_1)} \chi_i(C_2) = \begin{cases} \frac{|G|}{|C_1|} & si\ C_1 = C_2 \\ 0 & sinon \end{cases}$$

4) Comme $\chi_V(g)$ est la somme des valeurs propres de $\rho(g)$, on a

$$|\chi_V(g)| \leq dim\, V = \chi_V(e).$$

5) On a $|\chi_V(g)| = \dim V$ *ssi* $\rho(g) = Id_V$*. On a donc*

$$G_\chi \stackrel{\text{def}}{=} \{g \in G \,|\, \chi_V(g) = \chi_V(e)\} = ker(\rho : G \longrightarrow Gl(V)) \trianglelefteq G$$

6) On a $|\chi_V(g)| = dim\, V$ *ssi* $\rho(g)$ *est une homothétie. Comme le ss-groupe des homothéties* $\mathbb{C}^\times \cdot Id_V \subseteq Gl(V)$ *est distingué dans* $Gl(V)$*, la partie*

$$\{g \in G \,|\, |\chi_V(g)| = \chi_V(e)\}$$

est un ss-groupe distingué de G

Définition 12.2. Soient $S_1, \ldots, S_l$ comme avant et $\chi_1, \ldots, \chi_l$ leurs caractères. Soient $C_1, \ldots, C_l$ les classes de conjugaison(même l!). La table des caractères de G est la matrice $l \times l$ de coefficients $\chi_i(C_j)$, $1 \leq i, j \leq l$. On la note parfois $T(G)$(notation non standard).

Remarque 12.3. Souvent on suppose que $C_1 = \{e\}$ et χ_1 est le caractère de la représentation triviale.

Exemple 12.4. Soit $G = (\mathbb{Z}/n\mathbb{Z}, +)$. Alors les représentations irréductibles sont (à isom. près) les $\rho_z : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}^\times$, $\bar{k} \longmapsto z^k$, où z parcourt les racines n-èmes de l'unité. Fixons une racine primitive de l'unité ζ. Alors les caractères χ_i sont les $\rho_{\zeta^i} : \overline{k} \longmapsto z^{ik}$, $0 \leq i \leq n-1$, les classes de conjugaison sont les $C_j = \{j\}, 0 \leq j \leq n-1$, et la table des caractères est la matrice$(\zeta^{ij})_{0 \leq i,j \leq n-1}$.

Revenons au cas général :G, $C_1, \ldots, C_l$, $\chi_1, \ldots, \chi_l$ comme avant.

Remarque 12.5. On munit $\mathbb{C}^l$ du produit scolaire hermitien standard :

$$< x, y >= \sum_{i=1}^{l} \overline{(x_i)} y_i$$

1) Les colonnes de $T(G)$ sont orthogonales.

2) Le carréde la norme de la j- ème colonne est $\frac{|G|}{|C_j|}$.

3) Pour des fonctions centrales f_1, f_2 sur G, on a

$$< f_1, f_2 >= \sum_{g \in G} f_1(g^{-1}) f_2(g) = \sum_{i=1}^{l} \frac{|C_i|}{|G|} f_1(C_i^{-1}) f_2(C_i)$$

Donc les lignes de $T(G)$ sont orthogonales pour le produit scolaire hermitien

$$< x, y >_L = \sum_{i=1}^{l} |C_i| \cdot \overline{x_i}\,\overline{y_i} \quad x, y \in \mathbb{C}^l.$$

La norme de chaque ligne pour $<,>_L$ vaut $|G|$.

4) On a

$$\chi_{\mathbb{C}G} = \sum_{i=1}^{l} < \chi_i, \chi_{\mathbb{C}G} > \chi_i = \sum_{i=1}^{l} \chi_i(e)\chi_i$$

Donc la somme pondérée par les $\chi_i(e) = dim\, S_i$ des lignes de $T(G)$ est égal à $[|G|, 0, \ldots, 0]$ si $C_1 = \{e\}$.

Exemple 12.6. Soit $G = \mathfrak{S}_3 \cong \mathcal{D}_3$. On sait que $\mathbb{C}G \cong \bigoplus_{i=1}^{l} S_i^{dimS_i}$ et donc $|G| = \sum_{i=1}^{l} n_i^2$ où $n_i = dim\ S_i$. Or les seules façons d'écrire $6 = |G|$ comme somme de carrés sont

$$6 = 1+1+1+1+1+1+1 \quad et \quad 6 = 1+1+4$$

Si on avait $dim\ S_i = 1, \forall i$, alors G serait abélien ce qui n'est pas le cas. Donc les dimensions des représentations rréductibles sont 1,1 et 2. On déjà deux représentations de dimension 1 : la triviale $\mathfrak{S}_3 \longrightarrow \mathbb{C}^\times,\ \sigma \longmapsto 1$ et la signature $syn : \mathfrak{S}_3 \longrightarrow \mathbb{C}^\times,\ \sigma \longmapsto sgn(\sigma)$. La table des caractères est donc de la forme

	$\{e\}$	C_2	C_3
χ_{triv}	1	1	1
χ_{sgn}	1	-1	1
χ_2	2	z_1	z_2

Q : Quels sont z_1, z_2 ? **A :**Pour trouver z_1, z_2 on peut utiliser le fait que

$$\chi_{\mathbb{C}G} = [|G|, 0, 0] = \chi_{triv} + \chi_{sgn} + 2 \cdot \chi_2$$

Il s'ensuit que $\chi_2 = [2, 0, -1]$. Déterminons la représentation irréductible ρ_2 de caractère χ_2. Soit $V = \mathbb{C}^3$ la représentation de permutation associée au G- ens. $\{1, 2, 3\}$. Alors V est la somme directe de $\mathbb{C} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$, isomorphe à la représentation triviale , et de la représentation

$$V_2 = \{x \in \mathbb{C}^3 \,|\, x_1 + x_2 + x_3 = 0\}$$

On a $\chi_V = \chi_{triv} + \chi_{V_2}$ et donc $\chi_{V_2} = \chi_V - \chi_{triv} = [3,1,0] - [1,1,1] = [2,0,-1] = \chi_2$. Donc V_2 est irréductible et de caractère χ_2.

Utilisons la table des caractères our décomposer $V_2 \otimes V_2$ en somme de représentations irréductibles : on a

$$\chi_{V_2 \otimes V_2} = \chi_{V_2} \cdot \chi_{V_2} = [2,0,-1] \cdot [2,0,-1] = [4,0,1] \quad = [1,1,1] + [1,-1,1] + [2,0,-1] = \chi_{triv} + \chi_{sgn} + 2 \cdot \chi_2$$

D'où un isomorphisme $\chi_{V_2 \otimes V_2} \cong V_{triv} \oplus V_{sgn} \oplus V_2$.

On saitqu'on a aussi un isomorphisme canonique

$$\chi_{V_2 \otimes V_2} \xrightarrow{\sim} S^2(V_2) \oplus \Lambda^2(V_2)$$

Cet isomorphisme est compatible avec tout endomorphisme de V_2. Donc c'est aussi un isomorphisme de représentations. On a $dim \Lambda^2 V_2 = 1$ et en fait $\Lambda^2(\rho_2(g)) = det(\rho_2(g))$ qui est $\neq 1$ pour $g = (12)$. Donc $\Lambda^2 V_2 \cong V_{sgn}$ et par conséquent, on a $S^2(V_2) \cong V_{triv} \oplus V_2$ (par l'unicité de la décomposition de $V_2 \otimes V_2$ en somme directe d'irréductibles).

Lemme 12.7. *a) Les représentations de dim. 1 de G sont exactement celles de la forme $\overline{\rho} \circ \pi$, où $\pi : G \longrightarrow G_{ab} = G/[G,G]$, et $\overline{\rho} : G_{ab} \longrightarrow Gl_1(\mathbb{C})$ est une représ. de dim. 1 de G_{ab}.*

b) Le nombre de classes d'isom. de représentations de dim. 1 de G est l'ordre de G_{ab}.

c) G est abélien ssi toutes après, irréd , sont de dim. 1 (déjà démontré d'une autre façon).

Démonstration.

Le groupe $Gl_1\mathbb{C}$ est abélien (car isomorphe à $\mathbb{C}^\times$). Donc tout morphisme $g : G \longrightarrow Gl_1\mathbb{C}$ se factorise $\rho = \overline{\rho} \circ \pi$ pour un unique morphisme $\overline{\rho} : G_{ab} \longrightarrow Gl_1(\mathbb{C}) \cong \mathbb{C}^\times$.

On sait que le nombre de morphisme $A \longrightarrow \mathbb{C}^\times$ et est égal à IAI si A est un groupe abélien fini.

Si toutes les représ. irréd, sont de dimension 1 , alors elles se factorisent toutes par G_{ab} . Comme toute représ. est somme directe de représ. irréd . (Maschke) , toute représ se factorise par G_{ab}. En particulier, la représentation régulière $\rho_{\mathbb{C}G} : G \to Gl(\mathbb{C}G)$ se factorise par G_{ab}. Or le noyau de $\rho_{\mathbb{C}G}$ est trivial (car G agit librement sur G et donc fidèlement sur $\mathbb{C}G$). Donc $ker(G \xrightarrow{\pi} G_{ab}) = [G,G]$ est trivial et $G = G_{ab}$. □

Table des caractères de D_4

Soit $G = \mathcal{D}_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$, où $r = \begin{bmatrix} \cos \pi/2 & -\sin \pi/2 \\ \sin \pi/2 & \cos \pi/2 \end{bmatrix}$, $s = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

On a $r^4 = e = s^2$ et $srs = r^{-1}$. Les classes de conjugaison sont $C_1 = \{e\}$, $C_2 = \{r^2\}$, $C_4 = \{s, sr^2\}$, $C_5 = \{sr, sr^3\}$. Notons que $r^2 = -I_2$ et donc r^2 est central. On a $r^2 = [s, r]$ et $\mathcal{D}_4/ < r^2 >$ est commutatif d'ordre 4. Donc $G_{ab} = \mathcal{D}_4/ < r^2 >$. Les classes de s, r et sr dans G_{ab} sont distinctes er de carré e. Donc $G_{ab} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Donc, par le lemme, G admet exactement 4 représentations de dim. Si (n_i) sont les dimensions des représ. irréd., on a $|G| = 8 = \sum_{i=1}^{5} n_i^2$. La seule possibilité est $|G| = 8 = 1 + 1 + 1 + 1 + 2^2$. On obtient la table suivante

	$\{e\}$	$\{r^2\}$	$\{r, r^3\}$	$\{s, sr^2\}$	$\{sr, sr^3\}$
χ_{triv}	1	1	1	1	1
$\chi_{\text{dét}}$	1	1	1	-1	-1
χ_1	1	1	-1	1	-1
$\chi_1 \cdot \chi_{\text{dét}}$	1	1	-1	-1	1
χ_2	2	-2	0	0	0

Où l'on obtient la dernière ligne grâce à la formule

$$[8, 0, 0, 0, 0] = \chi_{triv} + \chi_{\text{dét}} + \chi_1 + \chi_1 \cdot \chi_{\text{dét}} + 2 \cdot \chi_2$$

Rappelons que si ρ est une représ. (de dim. finie) et χ son caractère. on a

$$Ker(\rho) = \{g \in G | \chi(g) = \chi(e)\}$$

Ici, les noyaux sont respectivement

$$\mathcal{D}_4, \quad < r >, \quad \{e, r^2, s, sr^2\}, \quad \{e, r^2, sr, sr^3\}, \quad \{e\}$$

Définition 12.8. Une représentation (V, ρ) est fidèle si $Ker(\rho) = \{e\}$($\Leftrightarrow$ l'action de G dans V est fidèle).

Remarques 12.9. *1) La reprise régulière est fidèle.*

2) Si (V, ρ) est de dim. fini de caractère χ, alors $Ker(\rho) = \{g \in G | \chi(g) = \chi(e)\} =: G_\chi$ et V est fidèle ssi $G_\chi = \{e\}$.

3) $Ker(\rho_1 \oplus \rho_2) = Ker(\rho_1) \cap Ker(\rho_2)$ pour toutes représ ρ_1, ρ_2 (de dim. finie ou infinie).

Lemme 12.10. *Soient $\rho_1, \ldots, \rho_l$ les représ. irréd.(à isom. près). Alors tout ss groupe distin-*

gué $N \triangleq G$ *est intersection de certains* $Ker(\rho_i)$. *En particulier,* G *est simple* **ssi** $Ker(\rho_i) = \{e\}$ *sauf si* ρ_i *est triviale.*

Remarque 12.11. Donc la table des caractères permet de déterminer si G est simple ou non.

Démonstration. Ll'ensemble $X = G/N$ est un G-ensemble (mult. à gauche). Soit kX la représentation de permutation associée. Alors

$$Ker(\rho_{kX}) = \bigcap_{g \in G} gNg^{-1} = N$$

Soit $\rho \cong \rho_1^{n_1} \oplus \cdots \oplus \rho_l^{n_l}$ une décompose en irréductibles. Alors

$$Ker(\rho) = \bigcap_{i=1}^{l} Ker(\rho_i)^{n_i} = \bigcap_{n_i \neq 0} Ker(\rho_i)$$

□

Exercice 12.12. Vérifierqu'on a la table des caractères suivante pour $G = \mathfrak{A}_4$

$\lvert C\rvert$	1	4	4	3
C	e	(123)	(132)	(12)(34)
χ_{triv}	1	1	1	1
χ	1	ω	ω^2	1
χ^2	1	ω^2	ω	1
χ_V	3	0	0	-1

On voit que $G_\chi = \{e, (12)(34), (13)(24), (14)(23)\}$ est le groupe de Klein. Cela confirme que $\mathfrak{A}_4$ n ;est pas simple. On voit que V est fidèle.

Exercice 12.13. Montrer que la table des caractères de $\mathfrak{A}_5$ est la suivante , où l'on écrit des représentants des classes de conjugaison au lieu des classes elles-mêmes. On voit que les représentations irréd. non triviales de gA_5 sont fidèles. Cela confirme que $\mathfrak{A}_5$ est simple.

Remarque 12.14. Un programme qui donne les tables des caractères : GAP. Il fait partie de SAGE.

13 Propriétés d'intégralité

Buts

1) Montrer que si V est irréductible, alors $dim\, V$ divise $|G|$.
2) Montrer le **Thm de Burnside** : Si $|G|$ n'a que deux facteurs premiers, alors G est résoluble

13.1 Entiers algébriques

soit R un anneau commutatif.

Définition 13.1. Un élément de R est algébrique sur $\mathbb{Z}$ s'il est racine d'unpolynôme unitaire à coeff. dans $\mathbb{Z}$: on a

$$x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0 = 0$$

pour certains n et $a_0, \ldots, a_n - 1 \in \mathbb{Z}$.

On appelle entiers algébriques les nombres complexes qui sont algébriques sur $\mathbb{Z}$.

Exemples 13.2. 1) Les racines de l'unité dans $\mathbb{C}$ sont des entiers algébriques (maispas des entiers engénéral !).

2) Soit $R = \mathbb{Q}$. Soit $x \in \mathbb{Q}$, $x = \frac{r}{s}, r \in \mathbb{Z}, s \in \mathbb{Z}\backslash\{0\}$, $pgcd(r, s) = 0$. Alors x est un entier algébrique ssi x est un entier. En effet :

" $\Leftarrow$ " Si x est entier, il est racine $X - x$.

" $\Rightarrow$ " Si $x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0 = 0$ pour des $a_0, \ldots, a_n - 1 \in \mathbb{Z}$, alors

$$r^n + a_{n-1}sr^{n-1} + \cdots + a_1 s^{n-1} + a_0 s^n = 0$$

comme $pgcd(r, s) = 1$, cela implique que $s = \pm 1$.

Notation. *Soit $x \in R$. On pose $\mathbb{Z}[x] = \{P(x) | \, P \in \mathbb{Z}(X)\}$. C'est le sous- anneau de R engendré par x . C'est aussi le ss-groupe abélien de R engendré par les puissances x^n, $n > 0$, de x.*

Proposition 13.3. *soit $x \in R$. On a équivalence entre*

i) x est algébrique sur $\mathbb{Z}$.

ii) Le groupe abélien $\mathbb{Z}[x]$ est de type fini.

iii) $\mathbb{Z}[x]$ est contenu dans un ss-groupe abélien de type fini de R.

Démonstration. *i)* $\Rightarrow$ *ii)* Si $x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0 = 0$ pour des $a_0, \ldots, a_n - 1 \in \mathbb{Z}$, alors $x^m \in \mathbb{Z}x^{n-1} + \cdots + \mathbb{Z}x + \mathbb{Z} \cdot 1$ pour tout $m \geq 0$(récurrence sur m). Donc $\mathbb{Z}[x]$ est engendré par $1, x, \ldots, x^{n-1}$

ii) $\Rightarrow$ *iii*) est clair.

iii) $\Rightarrow$ *i*) On sait qu'un ss-gr. d'un gr. abélien de type fini est encore de type fini. Soit $P_1(x), \ldots, P_r(x)$, $P_i \in \mathbb{Z}[X]$, une famille génératrice de $\mathbb{Z}[x]$. Soit d le maximum des degrés des P_i . Alors

$$\mathbb{Z}[x] \subseteq \sum_{i=1}^{r} \mathbb{Z} \cdot P_i(x) \subseteq \mathbb{Z} \cdot 1 + \mathbb{Z}x + \cdots + \mathbb{Z}x^d$$

Donc $x^{d+1} \in \mathbb{Z} \cdot 1 + \mathbb{Z}x + \cdots + \mathbb{Z}x^d$ et on a une équation $x^{d+1} + a_d x^d + \cdots + a_1 x + a_0 = 0$ pour des $a_i \in \mathbb{Z}$.

□

Corollaire 13.4. *Les éléments $x \in R$ qui sont algébriques sur $\mathbb{Z}$ forment un ss-anneau de R.*

Exemple 13.5. Si χ est le caractère d'une représ. complexe de dim. fini d'un groupe fini G, alors les valeurs $\chi(g)$, $g \in G$, sont des entiers algébriques car ce sont des sommes de racines de l'unité.

Démonstration. Soient $x, y \in R$ des éléments algébriques sur $\mathbb{Z}$. Supposons que $\mathbb{Z}[x]$ est engendré comme groupe abélien par $1, x, \ldots, x^r$ et $\mathbb{Z}[y]$par $1, y, \ldots, y^s$ pour des $r, s \geq 0$. Alors le groupe abélien $\mathbb{Z}[x, y]$ = (ss-gr. abélien engendré par les $x^i y^j$, $0 \leq i$, $0 \leq j$) est engendrépar les $x^i y^j$, $0 \leq i \leq r$, $0 \leq j \leq s$. Donc $\mathbb{Z}[x, y]$ est de type fini. Il contient $x + y$, $x - y$ et xy qui sont donc algébriques sur $\mathbb{Z}$. □

13.2 Dimensions des représentations irréductibles

Soit G un groupe fini.

Lemme 13.6. *Soit $\mathcal{C}$ une classe de conjugaison de G. Soit (V, ρ) une représentation irréductible de caractère χ. Alors $\mathcal{C}| \cdot \chi(\mathcal{C})/\dim v$ est un entier algébrique.*

Démonstration. Soit $f : G \longrightarrow \mathbb{C}$ la fonction caractéristique de $\mathcal{C}^{-1}$. Alors f est une fonction centrale. On sait que

$$f_V = \frac{1}{|G|} \sum_{g \in G} f(g)\rho(g^{-1}) = \frac{|\mathcal{C}|}{|G|} \sum_{g \in G} \rho(g)$$

est un endomorphisme de V égal à l'homothétie de rapport

$$\frac{< f_V, \chi_\rho >}{\dim V} = \frac{1}{|G|}\frac{|\mathcal{C}| \cdot \chi(\mathcal{C})}{\dim V}$$

Donc $|G| \cdot f_V$ est l'homothétie de rapport $\frac{|\mathcal{C}|\cdot\chi(\mathcal{C})}{\dim V}$. Considérons maintenant $|G| \cdot f_{\mathbb{C}G} = |\mathcal{C}| \cdot \sum_{g\in G} \rho_{\mathbb{C}G}(g) : \mathbb{C}G \longrightarrow \mathbb{C}G$. C'est un endomorphisme de $\mathbb{C}G$ dont la matrice dans la base de h, $h \in G$, est à coefficients entiers (car $\mathbb{C}G$ est une représentation de permutation). Donc le polynôme caractéristique de $|G| \cdot f_{\mathbb{C}G}$ est unitaire et à coeff. entiers. Donc les valeurs propres algébriques . Or V isomorphe à une ss représ. $V' \subseteq \mathbb{C}G$ et la restriction de $|G| \cdot f_{\mathbb{C}G}$ à V' est $|G| \cdot f_{V'}$, qui est l'homothétie de rapport $\frac{|\mathcal{C}|\cdot\chi(\mathcal{C})}{\dim V}$, qui est donc valeur propre de $|G| \cdot f_{\mathbb{C}G}$. □

Théorème 13.7. *Soient G un groupe fini et V une représ. complexe irréductible de G. Alors la dim. de V divise l'ordre de G.*

Démonstration. Soit χ le caractère de V. On sait que $1 =< \chi, \chi >) = \frac{1}{|G|}\sum_{g\in G} \chi(g^{-1})\chi(g)$. Soient $\mathcal{C}_1, \ldots, \mathcal{C}_l$ les classes de conjugaison de G. On a alors

$$\begin{aligned}\frac{|G|}{\dim V} &= \frac{1}{\dim V}\sum_{g\in G}\chi(g^{-1})\chi(g) = \frac{1}{\dim V}\sum_{i=1}^{l}\sum_{c\in\mathcal{C}_i}\chi(c^{-1})\chi(c)\\ &= \frac{1}{\dim V}\sum_{i=1}^{l}|\mathcal{C}_i|\chi(\mathcal{C}_i^{-1})\chi(\mathcal{C}_i) = \sum_{i=1}^{l}\frac{|\mathcal{C}_i|\chi(\mathcal{C}_i)}{\dim V}\chi(\mathcal{C}_i)\end{aligned}$$

Comme les entiers algébriques forment un sous- anneau de $\mathbb{C}$, le rationnel $\frac{|G|}{\dim V}$ est un entier algébrique et donc un entier. Donc $\dim V$ divise bien $|G|$. □

Remarques 13.8. *1) Le théorème n'est plus vrai sur $\mathbb{R}$ ($\mathbb{R}$ n'est pas algébriquement clos). P.ex. la représentation*

$$\rho : \mathbb{Z}/3\mathbb{Z} \longrightarrow Gl_2(\mathbb{R}), \quad \overline{k} \longmapsto \begin{pmatrix}\cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3}\\ \sin\frac{2\pi}{3} & \cos\frac{2\pi}{3}\end{pmatrix}$$

est irréductible (aucune droite n'est stable sous l'action des rotations $\rho(\overline{k})$, $\overline{k} \in \mathbb{Z}/3\mathbb{Z}$. Elle est de dimension 2 et 2 ne divise pas $3 = |\mathbb{Z}3\mathbb{Z}|$.

2) Supposons que $|G| = p^2$, p premier. Les seules dimensions possibles pour les représentations irréductibles sont $1, p, p^2$. Comme la somme des carrés des dimensions vaut $|G|$ et qu'on a au moins une représentation de dimension 1, les dimensions p et p^2 sont exclues. Donc toutes les représentations irréductibles sont de dimension 1 et G est abélien

(connu). Notons que cette démonstration est essentiellement différente de celle sans théorie des représentations

13.3 Le "théorème p^aq^b" de Burnside

Théorème 13.9 (W. Burnside 1904)**.** *Soit G un groupe d'ordre p^aq^b où p, q sont premiers et $a, b \in \mathbb{N}$. Alors G est résoluble.*

Remarques 13.10. *1) Donc l'ordre de toutgroupe simple non abélien a au moins trois diviseurs premiers distincts 2 à 2.*

2) Nous allons présenterla dém. originale de Burnside, basée sur la th. des représ.. La première dém. qui n'utilise pas la théorie des représentations n'a été obtenue qu'en 1970 (pour G d'ordre impair, par Goldschmidt) Msp. en 1970 (pour G d'ordre pair, par Bender). Les deux sont basées sur une idée de John G. Thompson (du théorème de Feit- Thompson).

Lemme 13.11. *Tout p-groupe G est nilpotent.*

Démonstration. On montre d'abord que $\mathcal{Z}(G) \neq \{e\}$. Supposons que $\mathcal{Z}(G = \{e\}$. Alors on a $|G| = 1 + |C_2| + \cdots + |C_l|$, où $C_2 \ldots, C_l$ sont les classes de conjugaison non ponctuelles de G. Comme les C_i sont des orbites sous une action de G (la conjugaison), les cardinaux $|G_i|$ sont des puissances de p. On obtient $0 \equiv 1 \mod p$, $\lightning$. Donc $\mathcal{Z}(G)$ est non trivial. Le groupe $G/\mathcal{Z}(G)$ est nilpotentpar réc. sur $|G|$ et G est ext, centrale de $G/\mathcal{Z}(G)$ par $\mathcal{Z}(G)$. □

Lemme 13.12. *Soit G un groupe fini. Soit $e \neq h$ un élément de G et soit $\mathcal{C}$ la classe de conjugaison de h. Supposons que $|\mathcal{C}|$ est une puissance p^u d'un nombre premier p. Alors G admet une représentation irréductible (V, ρ) de noyau $N \neq G$ telle que $\rho(h)$ est dans le centre de l'image de ρ.*

Démonstration. Montrons d'abord que G admet une représentation irréductible non triviale de caractère χ telle que $\chi(h) \neq 0$ et p ne divise pas $\chi_(e)$. Supposons qu'une telle représentation n'existe pas. Soient $\chi_1, \ldots, \chi_l$ les caractères des représ, irréductibles de G et $\chi_1 = \chi_{triv}$. Par notre hypothèse, si $i \geq 2$, nous avons $\chi_i(h) = 0$ ou p divise $\chi_i(e)$.

comme $\mathcal{C}^{-1} \neq \{e\}$, l'orthogonalalité des colonnes de la table des caractères nous donne $1 + \sum_{i=2}^{l} \chi_i(e)\chi_i(h) = 1 + \sum_{i=2}^{l} \chi_i(e)\overline{\chi_i(h^{-1})}$ Par notre hypothèse, p divise $\chi_i(e)$ pour tout $i \geq 2$ tel que $\chi_i(h) \neq 0$. Il s'ensuit que $-\frac{1}{p}$ est une combinaison linéaire à coefficientsentiers des

$\chi_i(h)$. Donc $-\frac{1}{p}$ est un entier algébrique.↯. Soit donc (V,ρ) une représentation irréductible de caractère χ telle que $\chi_i(h) \neq 0$ et p ne divise pas $\dim V = \chi(e)$. Soit $N = \ker(p)$. Comme χ est non trivial, nous avons $N \neq G$. On sait que $\frac{|\mathcal{C}|}{\dim V}\chi(h)$ est un entier algébrique. Comme p ne divise pas $\dim V$ et $|\mathcal{C}| = p$, les nombres $\dim V$ et $|\mathcal{C}|$ sont premiers entre eux. On a donc une identité de Bézout

$$xq^d + y\dim V = 1, \quad \textit{pour des } x, y \in \mathbb{Z}$$

Mais alors

$$\frac{\chi(h)}{\dim V} = \frac{\chi(h)xq^d + \chi(h)y\dim V}{\dim V} = x \cdot \frac{\chi(h)|\mathcal{C}|}{\dim V} + y\chi(h)$$

est un entier algébrique . Soit $\zeta_1 = \frac{\chi(h)}{\dim V} \in \mathbb{C}$ Soit $p(X \in \mathbb{Q}[X]$ son polynôme minimal, i.e.$P(X)$ est unitaire et engendre l'idéal $\{R(X) \in \mathbb{Q}[X|R(\zeta_1) = 0\}$. Alors $P(X)$ divise (dans $\mathbb{Q}[X]$) un polynôme $X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ à coefficients entiers qui annule ζ_1. Alors $P(X)$ est à coefficients entiers (lemme de Gauss). Soient $\zeta_2 \ldots \zeta_m$ les autres racines de $P(X)$. Comme $\dim V \cdot \zeta_1$, est une somme de $\dim V$ racines de l'unité, le nombre $\dim V \cdot \zeta_i$ est une somme de $\dim V$ racines de l'unité pour tout i. (Raison hors programme : Soit $L \subseteq \mathbb{C}$ le plus petit corps contenant les $\zeta)i.$ et les racines de l'unité en question ; alors $\mathrm{Aut}(L)$ agit transitivement sur les ζ_i , par les débuts de la théorie de Galois).

Donc on a $|\zeta_i| \leq 1$ pour tout i. Ainsi $b = \prod_{i=1}^{n} \zeta_i$ est de norme ≤ 1. Mais $\pm b$ est le coefficient constant de $P(X)$ donc entier. Ainsi on a $b \in \{-1, 0, 1\}$. Comme les ζ_i sont toutes racines d'un même polynôme irréductible , on a $\zeta_i = 0$ pour un i ssi $\zeta_i = 0$, $\forall i$. Comme $\zeta_i = \chi(h)/\dim V \neq 0$, on a $\zeta_i \neq 0$, $\forall i$. Donc $b = \pm 1$ et $|\zeta_i| = 1$ pour tous i. On a donc $|\chi(h)| = \chi(e)$ ce qui implique que $\rho(h)$ est une homothétie. Donc $\rho(h)$ est bien central dans l'image de ρ. □

Démonstration du Thm. Si G est un p-groupe alors il estnilpotent ($\Rightarrow$ résoluble). On peut donc supposer $p \neq q$ et $a, b \geq 1$. On procède par induction sur $(a, b) \in \mathbb{N} \times \mathbb{N}$. Si le centre $\mathcal{Z}$ de G est non trivial , alors $\mathcal{Z}$ est résoluble (car abélien) et $G/\mathcal{Z}$ est résoluble (par l'hyp. de réc.) . Donc G est résoluble en tant qu'extension de groupes résolubles. Supposons donc que le centre de G est trivial . Alors il existe une classe de conj. non ponctuelle $\mathcal{C}$ telle que q ne divise pas $|\mathcal{C}|$. En effet, on a $|G| = |\mathcal{Z}(G)| + |C_2| + \cdots + |C_l|$, où $C_2, \ldots, C_l$ sont les classes de conjugaison non ponctuelles de G. Soit $h \in \mathcal{C}$, Alors $|\mathcal{C}|$ est une puissance de p et $h \neq e$. Par le lemme 13.12, il existe une représ. irréd. (V,ρ) tq $N = Ker(\rho) \neq G$ et $\rho(h)$ est central dans $\mathrm{Im}(\rho)$. Si on a $N = \{e\}$, alors h est central dans G. ↯ Donc N et G/N sont d'ordre $< |G|$ et par l'hyp. de réc. , ils sont résoluble. Donc G est résoluble. □

13.4 L'algorithme de Burnside pour la table des caractères

Cet algorithme ramène la détermination de la table des caractères d'un groupe fini à la diagonalisation simultanée d'une famille (finie) de matrices qui commutent entre elles. Soit G un groupe fini. Soient $\mathcal{A}, \mathcal{B}, \mathcal{C}$ des classes de conjugaison de G. On pose

$$M_{\mathcal{A},\mathcal{B}}^{\mathcal{C}} \overset{\text{def}}{=} \frac{1}{\sqrt{|\mathcal{B}|}\sqrt{|\mathcal{C}|}} \cdot |\{(a,b) \in \mathcal{A} \times \mathcal{B} |\, a,b \in \mathcal{C}\}| \ \in \mathbb{R}$$

Soient $\mathcal{C}_1, \ldots, \mathcal{C}_l$ les classes de conjugaison de G telles que $\mathcal{C}_1 = \{e\}$.

Pour une classe de conjugaison $\mathcal{A}$, on définit $M_{\mathcal{A}} \in M_l(\mathbb{R})$ comme la matrice $l \times l$ à coefficients $M_{\mathcal{A},\mathcal{C}_j}^{\mathcal{C}_i}$, $1 \leq i,j \leq l$.

Théorème 13.13 (algorithme de Burnside)**.** *soit (V,ρ) une représ, irréd. de caractère χ. Alors pour toute classe de conjugaison $\mathcal{A}$. le vecteur $v_\chi = \begin{bmatrix} \sqrt{|\mathcal{C}_1|}\chi(\mathcal{C}_1) \\ \vdots \\ \sqrt{|\mathcal{C}_l|}\chi(\mathcal{C}_l) \end{bmatrix}$ est vecteurpropre de $M_{\mathcal{A}}$ pour la valeur propre $|\mathcal{A}|\chi(\mathcal{A})/\dim V$.*

Remarque 13.14. On a

$$v_\chi = \begin{bmatrix} \sqrt{|\mathcal{C}_1|}\chi(\mathcal{C}_1) \\ \vdots \\ \sqrt{|\mathcal{C}_l|}\chi(\mathcal{C}_l) \end{bmatrix} = \operatorname{diag}(\sqrt{|\mathcal{C}_1|}, \cdots, \sqrt{|\mathcal{C}_l|}) \cdot {}^t[\chi(\mathcal{C}_1), \cdots, \chi(\mathcal{C}_l)]$$

comme les lignes de la table des caractères forment une base orthogonale de $\mathbb{C}^l$ pour

$$< x, y >_L = \sum_{i=1}^{l} |\mathcal{C}_i| \overline{x_i} y_i.$$

Les vecteurs v_χ forment une base orthogonale de $\mathbb{C}^l$ pour le produit scolaire hermitien standard $< x, y >= \sum_{i=1}^{l} \overline{x_i} y_i$. Dans cette base, les $M_{\mathcal{A}}$, où $\mathcal{A}$ parcourt les classes de conjugaison, deviennent donc simultanément diagonales avec coefficients diagonaux.

$$\lambda_i(\mathcal{A}) = \chi_i(\mathcal{A})|\mathcal{A}|/\chi_i(e), \quad 1 \leq i \leq l.$$

Enparticulier, les matrices $M_{\mathcal{A}}$ commutent entre elles. Les espaces propres simultanés.

$$E_i = \{v \in \mathbb{C}^l |\, M_{\mathcal{A}} v = \lambda_i(\mathcal{A}) v, \forall \mathcal{A} \textit{ classe de conj. }\}, \quad 1 \leq i \leq l$$

sont de dimension 1 (Exercice!) ett donc E_i est la droite complexe engendrée par v_χ. Pour chaque caractère χ_i, $1 \leq i \leq l$, on peut recontruiere χ_i à partir de la droite

$$\mathbb{C} \cdot \mathrm{diag}(\sqrt{|\mathcal{C}_1|}^{-1}, \ldots, \sqrt{|\mathcal{C}_l|}^{-1}) \cdot v_{\chi_i}$$

Comme l'unique générateur de norme 1 et dont le premier coefficient est un réel positif. Ainsi, la détermination des caractères est réduite à la diagonalisation simultanée des matrices $M_{\mathcal{A}}$, $\mathcal{A}$ classe de conjugaison.

D'emonstration du Thm : 1^{eme} *étape .* Un calcul dans l'algèbre de groupe $\mathbb{C}G$: on munit l'espace vectoriel $\mathbb{C}G$ de l'unique produit $\mathbb{C}$-bilinéaire $\mathbb{C}G \times \mathbb{C}G \longrightarrow \mathbb{C}G$ tel que $g.h = gh$. On a donc un diagramme com..

$$\begin{array}{ccc} \mathbb{C}G \times \mathbb{C}G & \longrightarrow & \mathbb{C}G \\ \uparrow & & \uparrow \\ G \times G & \longrightarrow & G \end{array}$$

En particulement, pour $a = \sum_{g \in G} a_g g \in \mathbb{C}G$, on a $b = \sum_{g \in G} b_g g \in \mathbb{C}G$, on a

$$ab = \left(\sum_{g \in G} a_g g\right)\left(\sum_{h \in G} b_h h\right) = \sum_{k \in G}\left(\sum_{k=gh} a_g b_h\right) k$$

Muni de ce produit, l'espace vectoriel $\mathbb{C}G$ devient une G-algèbre. Elle est commutative ssi le groupe G est commutatif. On l'appelle l'algèbre de groupe (complexe) du groupe G. Son centre estclairement une ss- algèbre commutative. On a

$$a = \sum_{g \in G} a_g g \in \mathcal{Z}(\mathbb{C}G) \Leftrightarrow gag^{-1} = a \; \forall g \in G \Leftrightarrow la\ fonction\ g \longmapsto a_g\ est\ une\ fonc.\ centrale.$$

Ainsi, on a un isomorphisme d'espaces vectoriels (mais pas d'algèbres!)

$$\mathcal{C}(G) \longrightarrow \mathcal{Z}(\mathbb{C}G), \quad f \longrightarrow \sum_{g \in G} f(g) g.$$

En particulier, si on prend pour f la fonction caractéristique d'une classe de conjugaison $\mathcal{C}$, on obtient l'élément $\mathcal{Z}_{\mathcal{C}} = \sum_{c \in \mathcal{C}} c$ de $\mathbb{C}G$. Ces éléments forment une base de $\mathcal{Z}(\mathbb{C}G)$.

On a donc

$$\mathcal{Z}_{\mathcal{A}}\mathcal{Z}_{\mathcal{B}} = \sum_{\mathcal{C}} = m^{\mathcal{C}}_{\mathcal{A},\mathcal{B}}\mathcal{Z}_{\mathcal{C}} \tag{13.1}$$

pour certains $m^{\mathcal{C}}_{\mathcal{A},\mathcal{B}} \in \mathbb{C}$. Calculons ces nombre $m^{\mathcal{C}}_{\mathcal{A},\mathcal{B}}$!

$$\mathcal{Z}_{\mathcal{A}}\mathcal{Z}_{\mathcal{B}} = \left(\sum_{a\in\mathcal{A}} a\right)\left(\sum_{b\in\mathcal{B}} b\right) = \sum_{a,b} ab = \sum_{g\in G}\left(\sum_{ab=g} g\right)$$

$$= \sum_{\mathcal{C}\ cl.\ de\ conj.}\ \sum_{c\in\mathcal{C}} |\{(a,b)\in\mathcal{A}\times\mathcal{B}|ab=c\}|\cdot c$$

$$= \sum_{\mathcal{C}} |\{(a,b)\in\mathcal{A}\times\mathcal{B}|ab=c\}|\cdot\frac{1}{|\mathcal{C}|}\cdot\sum_{c\in\mathcal{C}} c \tag{13.2}$$

□

2^{eme} *étape* . L'affirmation.

Le morphisme de groupes $\rho : G \longrightarrow Gl(V)$ s'étend en un unique morphisme d'algèbres $\tilde{\rho} : \mathbb{C}G \longrightarrow \mathrm{End}_{\mathbb{C}}(V)$ donné explicitement par $\tilde{\rho}\left(\sum_{g\in G} c_g g\right) = \sum_{g\in G} c_g\rho(g)$.

Pour une classe de conjugaison $\mathcal{C}$, posons $F_{\mathcal{C}} = \tilde{\rho}(\mathcal{Z}_{\mathcal{C}})$. Comme $\mathcal{Z}_{\mathcal{C}}$ commute avec tous les $g \in G$, l'application linéaire $F_{\mathcal{C}} = \tilde{\rho}(\mathcal{Z}_{\mathcal{C}})$ commute avec tous les $\tilde{\rho}(g) = \rho(g)$, $g \in G$. Donc $F_{\mathcal{C}}$ est un endomorphisme de (V,ρ). Comme (V,ρ) est irréductible, $F_{\mathcal{C}}$ est une homothétie. En prenant les traces, nous obtenons $F_{\mathcal{C}} = \frac{|\mathcal{C}|\cdot\chi(\mathcal{C})}{\dim V} Id_V$. Soient $\mathcal{A},\mathcal{B}$ deux classes de conjugaison. Nous avons

$$\frac{1}{(\dim V)^2}|\mathcal{A}|\cdot|\mathcal{B}|\chi(\mathcal{A})\chi(\mathcal{B})Id_V = F_{\mathcal{A}}F_{\mathcal{B}} = \tilde{\rho}(\mathcal{Z}_{\mathcal{A}})\tilde{\rho}(\mathcal{Z}_{\mathcal{B}}) = \tilde{\rho}(\mathcal{Z}_{\mathcal{A}}\mathcal{Z}_{\mathcal{B}})$$

$$= \sum_{\mathcal{C}}\frac{1}{|\mathcal{C}|}M^{\mathcal{C}}_{\mathcal{A},\mathcal{B}}\sqrt{|\mathcal{B}|}\sqrt{|\mathcal{C}|}\sum_{c\in\mathcal{C}}\rho(c) = \frac{\sqrt{|\mathcal{B}|}}{\dim V}\cdot\sum_{\mathcal{C}} M^{\mathcal{C}}_{\mathcal{A},\mathcal{B}}\sqrt{|\mathcal{C}|}\chi(\mathcal{C})\cdot\mathrm{Id}_V\,.$$

Il s'ensuit qu'on a $\sum_{\mathcal{C}} M^{\mathcal{C}}_{\mathcal{A},\mathcal{B}}\sqrt{|\mathcal{C}|}\chi(\mathcal{C}) = \frac{|\mathcal{A}|\chi(\mathcal{A})}{\dim V}\sqrt{|\mathcal{B}|}\chi(\mathcal{B})$ pour tous $\mathcal{B}$. C'est a qu'il fallaitr démentrer. □

Appendice : Remarques sur l'algorithme de Burnside

Question. *D'où viennent les matrices $M_{\mathcal{A}}$ et pourquoi est-ce qu'il faut les diagonaliser simultanément ?*

Réponse. *Soit $\mathcal{A}$ une $\mathbb{C}$- algèbre. Pour chaque $a \in \mathcal{A}$, on a la multiplication à gauche*

$$l_a : \mathcal{A} \longrightarrow \mathcal{A}, b \longmapsto ab$$

On a $l_1 = Id_{\mathcal{A}}$ et $l_{a_1,a_2} = l_{a_1} \circ l_{a_2}$. On obtenir un morphisme d'algèbres

$$\mathcal{A} \longrightarrow \mathrm{End}_{\mathbb{C}}(\mathcal{A}), a \longmapsto l_a$$

Supposons qu'on a un isomorphisme d'algèbre $\mathcal{A} \xleftarrow{\sim} \overbrace{\mathbb{C} \times \cdots \times \mathbb{C}}^{l}$. Pour $1 \leq i \leq l$, soit $e_i = p^{-1}(0, \ldots, 1, \ldots, 0)$. Alors $\mathcal{A} = \mathbb{C}e_1 \oplus \cdot \oplus \mathbb{C}e_l$, $e_i e_j = \begin{cases} e_i & i = j \\ 0 & i \neq j \end{cases}$

Alors clairement la matrice des la dans la base $e_1, \ldots, e_l$ est diagonale

$$\mathrm{diag}(\lambda_1(a), \ldots, \lambda_l(a)), \quad \lambda_i(a) \in \mathbb{C}$$

et les $\mathbb{C}e_i$ sont les espaces propres simultanés de tous les l_a, $a \in \mathcal{A}$. De façon équivalente, les $\mathbb{C}e_i$ sont les espaces propres simultanés des $l_{a_1}, \ldots, l_{a_l}$ pour toute base $a_1, \ldots, a_l$ de A !

Exemple 13.15. Soit G un groupe fini. Soit $A = \mathcal{Z}(\mathbb{C}G)$. Alors $\dim A = l =$ nbre. de classes de conj. Soient $s_1, \ldots, s_l$ les représ. irréd. de G (à isom.près) et $\mathbb{C}G$. On a la décompos. en composantes isotypique, $V = \bigoplus_{i=1}^{l} V_{S_i}$. Soit χ_i le caractère de S_i. On sait que la projection p_i sur V_{S_i}, est donnée par

$$p_i = \frac{\dim S_i}{|G|} \cdot \sum_{g \in G} \overline{\chi_i(g)} \rho(g)$$

Alors on a

$$\begin{array}{ccccc} \prod_{i=1}^{l} \mathbb{C} & \xrightarrow{\sim} & \prod_{i=1}^{l} \mathbb{C}p_i & \xrightarrow{\sim} & \mathcal{Z}(\mathbb{C}G) \\ & & \downarrow & & \\ & & End(\bigoplus_{i=1}^{l} V_{S_i}) & & \end{array}$$

et $e_i = \frac{\dim S_i}{|G|} \cdot \sum_{i=1}^{l} \chi(g^{-1})g$, $1 \leq i \leq l$.

Pour l'autre base $a_1, \ldots, a_l$, on peut choisir des multiples, alors

$$a_i = \star \sum_{c \in \mathcal{C}_i} c$$

où $\mathcal{C}_1, \ldots, \mathcal{C}_l$ sont les

classes de conjugaison. Alors la matrice M_{a_k} de coefficients $M_{a_k,a_j}^{a_i}$ donnés par

$$a_k a_j = \sum_{i=1}^{l} M_{a_k,a_j}^{a_i} a_i$$

est la matrice de l_{a_k} dans la base $a_1, \ldots, a_l$.

Troisième partie

Groupes classiques

14 Rappels et compléments sur les corps

Soit K un corps. On a un unique morphisme d'anneaux $\varphi : \mathbb{Z} \longrightarrow K$ tel que $\varphi(1_{\mathbb{Z}}) = 1_K$. Explicitement :

$$\varphi(n) = \begin{cases} n \cdot 1_K & si\ n \geq 0 \\ -\varphi(-n) & si\ m \leq 0 \end{cases}$$

Le noyau $\ker(\varphi) \subseteq \mathbb{Z}$ est un idéal de $\mathbb{Z}$ donc de la forme $m\mathbb{Z}$ pour un $m \in \mathbb{Z}_{\geq 0}$ unique appelé la caractéristique de K : $car(A) = m$.

Le morphisme φ induit un morphisme d'anneaux injectif $\overline{\varphi} : \mathbb{Z}/m\mathbb{Z} \hookrightarrow K$. Il s'ensuit que $\mathbb{Z}/m\mathbb{Z}$ est intègre ($ab = 0 \Rightarrow a = 0$ ou $b = 0$) et donc $m = 0$ ou $m = p$ pour un nombre premier p. Le sous-corps premier de K est le plus petit sous-corps de K contenant $\mathrm{Im}(\varphi)$. On a les propriétés suivantes :

1) Si $car(K) = 0$, l'injection $\mathbb{Z} \xrightarrow{\varphi}$ s'étend un isomorphisme de Q sur le sous-corps premier.
2) Si $car(K) = p \geq 0$, alors le sous-corps premier est $\mathrm{Im}(\varphi)$ et φ induit un isomorphisme du corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ sur le sous-corps premier.

3) Si $car(K) = p \geq 0$, l'application de Frobenius $F_K : K \longrightarrow K$, $x \longmapsto x^p$ est compatible avec la multiplication (clair) et avec l'addition car

$$(x+y)^p = x^p + C_p^1 x^{p-1} y + \cdots + C_p^i x^{p-i} y^i + \cdots + y^p.$$

puisque p divise C_p^i pour $1 \leq i \leq p-1$. Le morphisme d'anneaux $F_K : K \longrightarrow K$ est toujours injectif($x^p = 0 \Rightarrow x = 0$) mais n'est pas toujours surjectif (non surjectif par exemple pour $K = \mathbb{F}_p(X)$). Le corps K est parfait si F_K est surjectif.

4) Supposons K fini. Alors le morph. $\varphi : \mathbb{Z} \longrightarrow K$ ne peut pas être injectif et donc $car(K) = p \geq 0$. Par $\overline{k}.x = \varphi(k)x$, $\overline{k} \in \mathbb{F}_p$, on définit une "multiplication par les scalaires $\mathbb{F}_p \times K \longrightarrow K$ qui fait du groupe abélien $(K, +)$ un $\mathbb{F}_p$- espace vectoriel de dimension finie $d \geq 0$ (car K est fini). On a donc $|K| = p^\alpha = q$. Comme le morphisme de Frobenius $F_K : K \longrightarrow K$ est injectif et K est fini, F_K est bijectif. Le groupe multiplicatif $(K^\times, \cdot)$ est d'ordre $q-1$. Par le théorème de Lagrange, on a donc $x_{q-1} = 1$ pour tout $x \in K^\times$. Il s'ensuit que $x^q = x$ pour tout $x \in K$. Cela signifie que $F_K^d : K \longrightarrow K$ est l'identité. Pour $K = \mathbb{F}_p$, on obtient que $F_{\mathbb{F}_p} : \mathbb{F}_p \longrightarrow \mathbb{F}_p$ est l'identité. Donc le sous-corps premier $\mathbb{F}_p \subseteq$ est contenu dans l'ensemble des points fixes

$$K^{F_K} = \{x \in K | x^p = x\}$$

des racines du polynôme $X^p - X$. Comme cet ensemble a au plus p éléments, ils sont égaux : $\mathbb{F}_p = \{x \in K | x^p = x\}$.

Théorème 14.1 (admis)**.** *Soit k un corps (p.ex. $k = \mathbb{F}_p$).*

a) Il existe un plongement $k \subseteq K$ dans un corps algébriquement clos et minimal pour cette propriété (i.e. tout corps $k \subseteq K' \nsubseteq K$ n'est pas algébriquement clos).

b) Si $k \subseteq K$ et $k \subseteq K'$ sont deux plongement comme dans a), il existe un isomorphisme (non unique !) $\psi : K \cong K'$ t.q. $\psi_k = Id_k$.

Définition 14.2. La clôture algébrique de k est un corps K algébriquement clos K contenant k.

Remarque 14.3. Par le thm, la clôture algébrique existe et est unique à un isomorphisme (non unique !) près. On la note parfois $\overline{k}$.

Corollaire 14.4. *Soient p un nombre premier, $d \geq 1$ un entier et $q = p^d$. Il existe un corps $\mathbb{F}_q$ contenant $\mathbb{F}_p$ unique à isomorphisme non unique près et tel que $|\mathbb{F}_q| = q$.*

Démonstration. Soit $L = \overline{\mathbb{F}_p}$ la clôture algébrique . Elle est de caractéristiquep et contient $\mathbb{F}_p$ comme sous-corps premier. Soit $K = L^{F_L^d} = \{x \in L | x^q = x\}$. Comme $F_L : L \longrightarrow L$ est un morphisme du corps, K est un sous- corps de L. Le polynôme $p(X) = X^{q-1} - 1$ est premier avec sa dérivée $p'(X) = (q-1)X^{q-2}$. Donc il a $q-1$ racines distinctes dans L. Ainsi $K = \{0\} \cup \{x \in L | x^{q-1} = 1\}$ est bien un corps de cardinal q. □

Exemple 14.5. Les éléments de $\mathbb{F}_4$ vérifient $x^4 - x = 0$. On a $X^4 - X = X(X^3 - 1) = X(X-1)(X^2 + X + 1)$ et le polynôme $X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$ (car il n'a pas de racines dans $\mathbb{F}_2$) . On a $\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2 + X + 1)$. Donc si α est la classe de X, alors et a est un générateur du groupe cyclique $\mathbb{F}_4^\times = \{1, \alpha, \alpha^2 = \alpha + 1\}$, $(\alpha\alpha^2 = \alpha^2 + \alpha = 1)$.

Lemme 14.6. *Soit K un corps fini. Alors le groupe $(K^\times, \cdot)$ est cyclique.*

Démonstration. Soit $q = |K|$. Si $(K^\times, \cdot)$ n'est pas cyclique, il existe un diviseur r de $q-1$, $r \neq q-1$, tel que $x^r = 1$ pour tout $x \in K^\times$ (cela résulte de la classification des groupes abéliens finis) .

Mais alors le polynôme $X^r - 1$ a $q - 1 > r$ racines dans K.↯ □

Remarque 14.7. La démonstration ne fournit pas de générateur pour $K^\times$ et on ne saitpas en construire engénéral (même pour $\mathbb{F}_p^\times$!)

15 le groupe linéaire $Gl_n(K)$

Soit K un corps. Soit $n \geq 1$ un entier. Rappelons que

$$Gl_n(K) = \{A \in M_n(K) | A \; inversible\},$$
$$Sl_n(K) = \{A \in M_n(K) | \det(A) = 1\} \trianglelefteq Gl_n(K)$$

Définissons les matrices suivantes :

a) transvection élémentaires ; $E_{i,j}(a) = I_n + aE_{i,j}$, $a \in K$, $i \neq j$,

b) dilatations ; $D_i(\lambda) = \mathrm{diag}(1, \ldots, \lambda, 1, \ldots, 1)$, $\lambda \in K^\times$.

Lemme 15.1. *a) On a $K^\times \xrightarrow{\sim} \mathcal{Z}(Gl_n(K))$, $\lambda \longmapsto \lambda I_n$.*

b) On a $\mu_n(K) \xrightarrow{\sim} \mathcal{Z}(GL_n(K))$, $\lambda \longmapsto \lambda I_n$, où $\mu_n(K) = \{\lambda \in K^\times | \lambda^n = 1\}$.

Démonstration. Voir la 1ère partie du cours. □

Théorème 15.2. *(a) Tout $g \in Gl_n(K)$ s'écrit $L\cdot$, où L est un produit de transv. él. .*

(b) Tout él. de $Gl_n(K)$ est un produit de transv. élém. .

Démonstration. Voir la 1ère partie du cours. □

Définition 15.3. Le groupe projectif linéaire est $PGl_n(K) = Gl_n(K)/\mathcal{Z}Gl_n(K) = Gl_n(K)/K^\times \cdot I_n$.

Le groupe projectif linéaire spécial est $PSl_n(K) = Sl_n(K)/\mathcal{Z}(Sl_n(K)) = Sl_n(K)/\mu_n(K) \cdot I_n$

Exemple 15.4. les centres de ces groupes sont triviaux (Attention : $\mathcal{Z}(G/\mathcal{Z}(G)) \neq \{e\}$ en général !).

Théorème 15.5. *Supposons $n \geq 2$. Alors*

(a) $D(Gl_n(K)) = Sl_n(K)$ (et donc $D(PGl_n(K)) = PSl_n(K)$) sauf si $n = 2$ et $K = \mathbb{F}_2$.

(b) $D(Sl_n(K)) = Sl_n(K)$ (et donc $D(PSl_n(K)) = PSl_n(K)$) sauf si $n = 2$ et $K = \mathbb{F}_2$ ou $K = \mathbb{F}_3$.

Démonstration. Voir la 1ère partie du cours. □

Remarques 15.6. *1) Si $n \geq 2$ et $K \neq \mathbb{F}_2$, par a), le déterminant induit un isomorphisme $Gl_n(K)_{ab} \xrightarrow{\sim}$, donc dans ce cas,* det : $Gl_n(K) \longrightarrow L^\times$ *" est le morphisme universal vers un groupe abélien, ce qui est une caractérisation jolie (et importante) du* det.

2) L'action de $Sl_2(\mathbb{F}_2) = Gl_2(\mathbb{F}_2)$ sur l'ensemble $\mathbb{P}^1(\mathbb{F}_2)$ des droites de $\mathbb{F}_2^2$ (ily en a 3 !) fournit un isomorphisme $Sl_2(\mathbb{F}_3) \cong \mathfrak{S}_3$ et donc un isom. .

$$D(Sl_2(\mathbb{F}_3)) \cong \mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$$

3) On a $Sl_2(\mathbb{F}_3)_{ab} \cong \mathbb{Z}/3\mathbb{Z}$ (Ex !) er donc $D(Sl_2(\mathbb{F}_3)) \subsetneq Sl_2(\mathbb{F}_3)$.

Rappel 15.7. *Soit V un K-espace vectoriel. Le projectivisé $\mathbb{P}(V)$ est l'ensemble des droites de V. On a une bijection canonique*

$$(V\backslash\{0\})/K^\times \xrightarrow{\sim} \mathbb{P}(V), \quad (\text{classe d. de } v) \longmapsto Kv.$$

où $K^\times$ agit par multiplication sur $V\backslash\{0\}$. Si $n \geq 0$ et $V = K^{n+1}$, on a $V\backslash\{0\} = \{(x_0, \ldots, x_n) | x_i \neq 0$ pour au moins un $i\}$ et $\mathbb{P}(V) = \mathbb{P}^n(K) = \{(x_0 : \ldots : x_n) | x_i \neq 0$ pour au moins un $i\}$ où $(x_0 : \ldots : x_n)$ désigne la classe de $(x_0, \ldots, x_n)$.

Le groupe $Gl(V)$ agit sur $V\backslash\{0\}$ et cette action induit une action de $PGl(V) = Gl(V)/K^\times \cdot Id_V$ sur $\mathbb{P}(V)$. Les applications $\mathbb{P}(V) \longrightarrow \mathbb{P}(V)$, $x \longmapsto g.x$, $g \in Gl(V)$ s'appellent des homographie de $\mathbb{P}(V)$.

L'action de $PGl(V)$ sur $\mathbb{P}(V)$ est fidèle : Si $g \in Gl(V)$ agit par l'identité sur $\mathbb{P}(V)$, alors $g.v = \lambda_v v$ pour un $\lambda_v \in K^\times$ pour tout $v \in V\backslash\{0\}$. Alors $g.(v+w) = \lambda_{v+w}(v+w) = \lambda_v v + \lambda_w w$ pour v, w lin. indép. . Donc la fonction $v \longmapsto \lambda_v$ est constante et $g \in K^\times \cdot Id_V$.

Supposonsque $n = 2$: Alors on a une bijection

$$r : \mathbb{P}^1(K) \xrightarrow{\sim} K \cup \{\infty\}, \quad (x_0 : x_1) \longmapsto \frac{x_1}{x_0} := \begin{cases} x_1/x_0 & si\ x_0 \neq 0 \\ \infty & si\ x_0 = 0. \end{cases}$$

Alors pour $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Gl_2(V)$, l'homographie associée se décrit ainsi

$$\begin{array}{ccc} (x_0 : x_1) \in \mathbb{P}^1(K) & \xrightarrow[\sim]{r} & K \cup \{\infty\} \\ \Big\downarrow g & & \\ (ax_0 + bx_1 : cx_0 + dx_1) \in \mathbb{P}(K) & \xrightarrow[\sim]{r} & K \cup \{\infty\} \end{array} \qquad \begin{array}{c} x \\ \Big\downarrow g \\ \text{"}\frac{ax+b}{cx+d}\text{"} \end{array} \qquad = g.x$$

Par exemple , si $bc \neq 0$, alors l'action $K \cup \{\infty\} \longrightarrow K \cup \{\infty\}$, $x \longmapsto g.x$ se décrit par

$$\begin{aligned} K\backslash\{-\frac{d}{c}\} \ni x &\longmapsto \frac{ax+b}{cx+d} \\ -\frac{d}{c} = x &\longmapsto \infty \\ \infty = x &\longmapsto \frac{a}{c} \end{aligned}$$

Morale : Le coordonnées homogènespermettent d'éviter ces distinctions de cas et de montrer de façon élégante qu'on a effectivement une action !

Exercice 15.8. a) Les groupes suivants admettent des structures naturelles de variétés différentiables telles que la mult. $G \times G \longrightarrow G$ et l'inversion sont des morph. de var. diff. !

- $G = Gl_n(\mathbb{R})$ de dimension n^2, $G = PGl_n(\mathbb{R})$ de dimension $n^2 - 1$.
- $G = Sl_n(\mathbb{R})$ de dimension $n^2 - 1$, $G = PSl_n(\mathbb{R})$ de dimension $n^2 - 1$.

b) Les groupes suivants admettent des structures naturelles de variétés différentiables telles que la mult. $G \times G \longrightarrow G$ et l'inversion sont des morph. de var. diff. !

— $G = Gl_n(\mathbb{C})$ de dimension(complexe !) n^2, $G = PGl_n(\mathbb{C})$ de dimension $n^2 - 1$.

— $G = Sl_n(\mathbb{C})$ de dimension $n^2 - 1$, $G = PSl_n(\mathbb{C})$ de dimension $n^2 - 1$.

Lemme 15.9. *On a*

a) $|Gl_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}}(q^n - 1)(q^{n-1} - 1)\cdots(q - 1)$.

b) $|PGl_n(\mathbb{F}_q)| = |Gl_n(\mathbb{F}_q)|/|\mathbb{F}_q^\times| = q^{\frac{n(n-1)}{2}}(q^n - 1)(q^{n-1} - 1)\cdots(q^2 - 1)$.

c) $|Sl_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-2})\cdot q^{n-1}$.

d) $|PSl_n(\mathbb{F}_q)| = |Sl_n(\mathbb{F}_q)|/\operatorname{pgcd}(n, q - 1)$

Démonstration. a),b),c) sont faciles.

d) :$|PSl_n(\mathbb{F}_q)| = |Sl_n(\mathbb{F}_q)|/\left(Sl_n(\mathbb{F}_q) \cap \mathbb{F}_q^\times \cdot I_n\right)$

$$|Sl_n(\mathbb{F}_q) \cap \mathbb{F}_q^\times \cdot I_n| = \#\{x \cdot I_n |\ x \in \mathbb{F}_q^\times, x^n = 1\} \xrightarrow{\sim} \mathbb{Z}/\operatorname{pgcd}(n, q - 1)$$

□

Tableau des ordres et isomorphismes

q	2	2	2	3	4	4	5	7	8	9
n	2	3	4	2	2	3	2	2	2	2
PSl	$6 \cong \mathfrak{S}_3$	168	$8!/2 \cong \mathfrak{A}_8$	$12 \cong \mathfrak{A}_4$	$60 \cong \mathfrak{A}_5$	$8!/2 \ncong \mathfrak{A}_8$	$60 \cong \mathfrak{A}_5$	$168 \cong PSl_3(\mathbb{F}_2)$	504	$6!/2 \cong \mathfrak{A}_6$
PGl				$24 \cong \mathfrak{S}_4$	$60 \cong \mathfrak{A}_5$		$120 \cong \mathfrak{S}_5$			$6! \ncong \mathfrak{S}_6$
Sl				$24 \ncong \mathfrak{S}_4$						

Exemple 15.10. 1) $PGl_2(\mathbb{F}_2) \xrightarrow{\sim} \mathfrak{S}_3$ par l'action fidèle de $PGl_2(\mathbb{F}_2)$ sur $\mathbb{P}^1(\mathbb{F}_2)$, qui a 3 éléments.

2) $PGl_2(\mathbb{F}_3) \xrightarrow{\sim} \mathfrak{S}_4$ par l'action fidèle de $PGl_2(\mathbb{F}_3)$ sur $\mathbb{P}^1(\mathbb{F}_3)$, qui a 4 éléments.

3) Le ss-groupe $PSl_2(\mathbb{F}_3)$ est d'indice 2 dans $PGl_2(\mathbb{F}_3) \cong \mathfrak{S}_4$. Il est donc distingué et isomorphe à $\mathfrak{A}_4$.

Théorème 15.11. *Soit K un corps. Le groupe $PSl_n(K)$ est simple sauf si $a = 2$ et $K = \mathbb{F}_2$ ou $K = \mathbb{F}_3$.*

Démonstration. Voir la 1ère partie du cours. □

Remarques 15.12. *1) On a donc les séries suivantes de groupes simples non abéliens :*

$$\mathbb{Z}/p\mathbb{Z},\ p \text{ premier},\ \mathfrak{A}_n,\ n \geq 5,\ PSl_n(K),\ n \geq 2,\ \text{sauf } PSl_2(\mathbb{F}_2) \text{ et } PSl_2(\mathbb{F}_3).$$

Tous les isomorphismes entre membres de ces séries sont indiqués dans le tableau.

2) On peut montrer que tous les groupes simples d'ordre

- *60 sont isomorphes. D'où* $\mathfrak{A}_5 \cong PSl_2(\mathbb{F}_4) = PGl_2(\mathbb{F}_4)$.
- *120 sont isomorphes ! D'où* $PSl_2(\mathbb{F}_7) \cong PSl_3(\mathbb{F}_2)$.

16 Formes bilinéaires et quadratiques

Soient K un corps et V un K-espace vectoriel.

Définition 16.1. Une forme bilinéaire sur V est une application $b : V \times V \longrightarrow K$ telle que pour tout $y \in V$, les applications $x \longmapsto b(x, y)$, et $x \longmapsto b(y, x)$ sont linéaires $V \longrightarrow K$. Une telle forme est symétrique si $b(x, y) = b(y, x)$, $\forall x, y \in V$. Elle est alternée si $b(x, x) = 0$ pour tout $x \in V$.

Remarques 16.2. *Si b est alternée, on a* $0 = b(x + y, x + y) = b(x, y) + b(y, x)$. *C'est- à - dire que b est antisymétrique. Si cart*$(k) \neq 2$, *la réciproque est vraie car alors* $b(x, x) = \frac{1}{2}(b(x, x) + b(x, x))$. *La forme* $b(x, y) = x_1y_1 + x_2y_2$ *sur* $\mathbb{F}_2^2$ *est antisymétrique mais n'est pas alternée car* $b(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}) = 1$.

Définition 16.3. Soit b une forme bilinéaire sur V. La forme quadratique associée ert l'application $q_b : V \longrightarrow K$, $x \longmapsto b(x, x)$.

Remarque 16.4. On a alors

$$q_b(x + y) = q_b(x) + q_b(y) + b(x, y) + b(y, x)$$

Si b est symétrique , on a

$$q_b(x + y) = q_b(x) + q_b(y) + 2b(x, y)$$

Si $car(K) \neq 2$, on peut récupérer une forme sym. b à partir de qb par la formule de polarisation.

$$b(x, y) = \frac{1}{2}(q_b(x + y) - q_b(x) - q_b(y))$$

Donc si $car(K) \neq 2$, on a la bijection {formes bilin. sym.} $\xrightarrow{\sim}$ {formes.quad.}, $b \mapsto q$.

Définition 16.5. Supposons que $\dim V \leq \infty$ et que $v_1, \ldots, v_n$ est une base. La matrice M d'une forme bilinéaire b dans la base est définie par $m_{i,j} = b(v_i, v_j)$, $1 \leq i, j \leq n$.

Remarques 16.6. *1) Si $v, w \in V$ ont pour vecteurs de coordonnées $x, y \in K^\times$, alors $b(v,w) = {}^t xMy$.*

2) La forme quadratique associée à b est donnée par le polynôme $q_b(v) = {}^t xMx$ homogène de degré 2 en les x_i.

3) La forme b est (anti)symétrique ssi M est (anti)symétrique.

4) Si Pest la matrice de passage de la base $v_1, \ldots, v_n$ vers une nouvelle base $v'_1, \ldots, v'_n$, alors la matrice M' de b dans la nouvelle base est $M' = {}^t PMP$.

Définition 16.7. Supposons que M est inversible . Le discriminant disc (b) de b est la classe de ditM dans le quotient $K^\times/(K^\times)^2$. Si $car(K) \neq 2$ et q est la forme quad. q_b associée à une forme bilin. sym., on pose $disc(q) = disc(b)$.

Remarque 16.8. Par définition, le discriminant ne dépend pas du choix de la base.

16.0.1 Quadriques

Définition 16.9. Une quadrique affine $Q \subseteq K^n$ est l'ensemble des solutions d'une équation polynomiale de degré 2 :

$$f_2(x_1, \ldots, x_n) + f_1(x_1 \ldots, x_n) + f_0 = 0 \tag{16.1}$$

où f_i est un polynôme homogène de degé i.

Remarques 16.10. *1) Le polynôme homogène est $f_2(x_1, \ldots, x_n) + f_1(x_1 \ldots, x_n)x_0 + f_0 x_0^2$. C'est une forme quadratique sur K^{n+1}. L'équation $f(x_0, \ldots, x_1) = 0$ définit un cône quadratique $Q \subseteq K^{n+1}$. On a l'identification*

$$Q \xrightarrow{\sim} \mathcal{C} \cap \{x_0 = 1\}, \quad (x_1, \ldots, x_n) \longmapsto (1, x_1, \ldots, x_n).$$

2) Par l'homogénéité, on a $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^2 f(x_0, \ldots, x_n)$. Donc si $(x_0, \ldots, x_n) \in K^{n+1}\backslash\{0\}$, alors $f(x_0, \ldots, x_n) = 0 \Leftrightarrow f(\lambda x_0, \ldots, \lambda x_n) = 0$, $\forall \lambda \in K^\times$.

Ainsi la quadrique projective $\overline{Q} = \{(x_0 : x_1 \cdots : x_n) \in \mathbb{P}^n(K) | f(x_0, x_1, \cdots, x_n)\}$ est bien définie. Si on identifie K^n avec son image par $(x_1, \cdots, x_n) \mapsto (1 : x_1 : \cdots : x_n)$ dans $\mathbb{P}^n(K)$, alors on a $Q = \overline{Q} \cap K^n$.

16.0.2 Formes non dégénérées

Supposons que $car(K) \neq 2$. Soit V un K- espace vectoriel de dimension finie. Soit b une forme bilinéaire symétrique ou alternée sur V.

Notation. $\hat{b} : V \longrightarrow V^\star$, $v \mapsto b(\cdot, v)$, $\ker(b) = \ker(\hat{b}) = \{v \in V | b(w, v) = 0, \forall w \in V\}$

Définition 16.11. — b est non dégénérée $\Leftrightarrow \ker(b) = 0$.

— b est une forme symplectique $\Leftrightarrow$ s b est alternée et non dégénérée.

— Le rang de b est $\mathrm{rg}(b) = \mathrm{rg}(\hat{b})$.

Remarque 16.12. Si $v_1, \ldots, v_n$ est un base de V et $v_1^\star, \ldots, v_n^\star$ est un base de $V^\star$ (i.e. $v_i^\star(v_j) = \delta_{ij}$), alors la matrice de $\hat{b}$ dans ces bases est la matrice de b car $\hat{b}(v_j) = b(\cdot, v_j) = \sum_{i=1}^{n} b(v_i, v_j) v_i^\star$.

Proposition 16.13. *On a équivalence entre*

i) b est non dégénérée,

ii) $\hat{b} : V \longrightarrow V^\star$ est bijective ,

iii) la matrice de b dans une base de V est inversible.

Démonstration. **i)⇔ii)** On a $\ker(\hat{b}) = \{0\}$. Donc $\hat{b}$ est injective. Comme $\dim V = \dim V^\star$, l'appel. $\hat{b}$ est bijective. La réciproque en claire.

ii)⇔iii) Clair par la remarque.

□

16.0.3 Groupes d'isométries

supposons que $car(K) \neq 2$. Soient (V, b) et (V', b') deux espaces vectoriels munis de formes b et b' du même type (symétrique ou alterné).

Définition 16.14. Une isométrie $(V, b) \longrightarrow (V', b')$ est une application linéaire injective $u : V \longrightarrow V'$ telle que

$$b'(u(v_1), u(v_2)) = b(v_1, v_2), \quad \forall v_1, v_2 \in V \tag{16.2}$$

Remarques 16.15. *1) Si b, b' sont symétriques, l'égalité 16.2 est équivalente à $q_{b'}(u(v)) = q_b(v)$, $\forall v \in V$.*

2) l'égalité 16.2 se traduit par

$$\begin{array}{ccc} V & \xrightarrow{\hat{b}} & V^\star \\ {\scriptstyle u}\downarrow & & \uparrow{\scriptstyle u^\star} \\ V' & \xrightarrow[\hat{b'}]{} & V'^\star \end{array}$$

car

$$u^\star \circ \hat{b'} \circ u(v) = u^\star(b'(\cdot, u(v))) = b'(u(\cdot), u(v)) = b(\cdot, v) = \hat{b}(v)$$

Donc si b est non dégénérée ($\Leftrightarrow$ $\hat{b}$injectif), alors u est automatiquement injectif.

3) Si $(V, b) = (V', b')$, alors toute isométrie est un isomorphisme et l'ensemble des isométries forme un groupe pour la composition

Notation. — *Si q est une forme quadratique , on note $O(V, q)$ le groupe des isométries de (V, q) et on l'appelle le groupe orthogonal de $(V.q)$.*

— *Si b est une forme alternée, on note $Sp(V.b)$ le gr. des isom, de $(V.b)$ et on l'appelle legroupe symplectique de (V, b).*

Remarque 16.16. Soit M la matrice de b dans une base de V. Alors on a

$$O(V, q) \cong \{U \in Gl_n(K) | {}^tUMU = M\}$$

Il s'ensuit que pour $u \in O(V, q)$ on a $\det(u)^2 \operatorname{dt} M = \det M$ et donc $\det(u) \in \{1, -1\}$.

Définition 16.17. Le groupe spécial orthogonal est $SO(V, q) = O(V, q) \cap Sl(V)$.

Théorème 16.18. *Supposons que b est symplectique. Alors $Sp(V, b) \subseteq Sl(V)$.*

Démonstration. Voir plus tard. □

16.0.4 Orthogonalité

Soit K un corps de $car(K) \neq 2$. Soient V un K-esp. vect. de dim. finie et $b : V \times V - K$ une forme bilinéaire symétrique ou alternée.

Définition 16.19. Deux vecteurs $u, v \in V$ sont orthogonaux si $b(v, w) = 0$ ($\Leftrightarrow b(w, v) = 0$).

L'orthogonal d'une partie $W \subseteq V$ est le ss-espace $W^\perp = \{v \in V | b(w, v) = 0\}$

Exemple 16.20. 1) $V^\perp = \ker(b)$

2) Si $V = K^2$ et $b(x, y) = x_1x_2 - y_1y_2$, alors $D = D^\perp$, où $D = K(e_1 + e_2)$.

Remarque 16.21. Donc si $W \subseteq V$ est un ss-espace, alors W et $W^\perp$ ne sont pas en somme directe en général.

Proposition 16.22. *Soit $W \subseteq V$ un ss-espace.*

a) Si b est non dégénérée , on a $\dim W + \dim W^\perp = \dim V$.

b) Si $b|_W := b|_{W\times W}$ est non dégénérée, on a $W \otimes W^\perp = V$.

Démonstration. a) Soit $r : V^\times \longrightarrow W^\times$ l'application de restriction $f \mapsto f|_W$. Elle est linéaire et surjective. Donc la composée $V \xrightarrow[\sim]{\hat{b}} V^\times \xrightarrow{r} \!\!\!\!\rightarrow\, W^\times$ est surjective. Or son noyau est $W^\perp$. Donc $\dim V = \dim W^\perp + \dim W^\times$

b) $b|_W$ est non dégénérée ssi $W \cap W^\perp = \{0\}$. On a $\dim W^\perp \geq \operatorname{codim} W$. Donc $V = W \oplus W^\perp$.

□

Lemme 16.23. *Pour des ss-espaces $W, W' \subseteq V$, on a*

a) $(W + W')^\perp = W^\perp \cap W'^\perp$ (pour tout b, mêmen si $\dim V = \infty$).

b) $(W^\perp)^\perp = W$ si b non dégénéré (et $\dim V \leq \infty$).

c) $(W \cap W')^\perp = W^\perp + W'^\perp$

Démonstration. a) $W^\perp \cap W'^\perp$ est l'ens. des solutions des équations $b(v, w) = 0$, $\forall w \in W$, et $b(v, w') = 0$, $\forall w' \in W'$.

$(W + W')^\perp$ est l'ens. des solutions des équations $b(v, w'') = 0$, pour $w'' = w + w'$, $w \in W$, $w' \in W'$.

b) On a clairement $W \subseteq (W^\perp)^\perp$. Par la Prop, on a $\dim W = \dim(W^\perp)^\perp$.

c) On a $(W^\perp + W'^\perp)^\perp = (W^\perp)^\perp \cap (W'^\perp)^\perp = W \cap W'$, ce qui donne c) par b).

□

Définition 16.24. Un vecteur vev est isotrope si $b(v, v) = 0$. Un ss-espace $W \subseteq V$ est totalement isotrope si $b|_W = 0$ ($\Leftrightarrow W \subseteq W^\perp$).

16.1 Décomposition en somme directe orthogonale

16.1.1 Cas d'un vecteur non isotrope

supposons que $\dim V \leq \infty$ et que $b : V \times V \longrightarrow K$ est symétrique.

Lemme 16.25 (réduction de Gauss)**.** *Il existe une base orthogonale $v_1, \ldots, v_r$ dans V, i.e. $b(v_i, v_j) = 0$, $\forall i \neq j$.*

Remarque 16.26. Si $x_1, x_2, \ldots, x_r$ sont les Il existe une base orthogonale $v_1, \ldots, v_n$, on a $q(v) = \alpha_1 x_1^2 + \ldots + a_r x_r^2$ où r est le rang de b et $\alpha_i = q(v_i) \neq 0$, $1 \leq i \leq r$.

Démonstration. Si $b = 0$, il n'y a rien à démontrer. Si non, par la formule de polarisation

$$b(x, y) = \frac{1}{2}(q_b(x + y) - q_b(x) - q_b(y)).$$

ildoit exister un vecteur non isotrope v_1. Alors $b|_{Kv_1}$ est non dégénérée et donc $V = Kv_1 \oplus v_1^{\perp}$. Par récurrence sur $\dim V$, il existe une base orthogonale $v_2, \ldots, v_r$ pour $v_1^{\perp}$ avec $b|_{v_1^{\perp}}$. Alors $v_1, \ldots, v_r$ est une base orthogonale dans V. □

Notation. *Pour $\alpha_1, \alpha_2, \ldots, \alpha_n \in K^{\times}$, on note $< \alpha_1, \alpha_2, \ldots, \alpha_n >$ la forme $(\alpha_1, \alpha_2, \ldots, \alpha_n) \longmapsto \alpha_1 x_1^2 + \ldots + a_n x_n^2$ sur K^n.*

Remarque 16.27. Si b est une forme bilin. sym. non dég. sur V de dim. n, on a donc une isométrie $< V, b > \cong < \alpha_1, \alpha_2, \ldots, \alpha_n >$ pour des $\alpha_i \in K^{\times}$. Clairement, pour $a_i \in K^{\times}$, on a une isométrie

$$< \alpha_1, \alpha_2, \ldots, \alpha_n > \cong < a_1^2\alpha_1, a_1^2\alpha_2, \ldots, a_n^2\alpha_n >, \quad e_i \longmapsto a_i e_i.$$

On a donc une surjection

$$\prod_{i=1}^{n} K^{\times}/(K^{\times})^2 \cong \{(V, b) | \dim V = n, \text{b non dég.}\}/\text{isom.}.$$

Le problème est de déterminer ses fibres : Quand est-ce qu'on a $< \alpha_1, \alpha_2, \ldots, \alpha_n > = < \alpha_1', \alpha_2', \ldots, \alpha_n' >$?

Une condition nécessaire est l'égalité des discriminants $\text{disc}(< \alpha_1, \alpha_2, \ldots, \alpha_n >) = \alpha_1\alpha_2 \ldots \alpha_n \in K^{\times}/(K^{\times})^2$. Mais elle n'est pas suffisante en général.

Exemple 16.28. 1) Si K est quadratiquement clos. (i.e. chaque élément de K est un carré, p.ex. si K est algébriquement clos), alors chaque forme quad. non dég. est isométrique à $< 1, \ldots, 1 >$.

On note $O_n(K)$ le groupe des isométries de $< 1, \ldots, 1 >$.

2) Si $K = \mathbb{R}$, alors $\{1, -1\} \cong K^\times/(K^\times)^2$. Donc chaque forme quad. non dég. q est isométrique à $< \underbrace{1, \ldots, 1}_{s}, \underbrace{-1, \ldots, -1}_{n-s} >$. Le couple $(s, n-s)$ est la signature de q. On verra qu'elle est indépendante du choix d'une base. On note $O_{n,n-s}(\mathbb{R})$ le groupe du isom'etries de $< \underbrace{1, \ldots, 1}_{s}, \underbrace{-1, \ldots, -1}_{n-s} >$. Le couple $(s, n-s)$. Comme q et $-q$ ont les mêmes groupes d'isométries, on a $O_{s,t}(\mathbb{R}) = O_{t,s}(\mathbb{R})$. Le discriminant de $< \underbrace{1, \ldots, 1}_{s}, \underbrace{-1, \ldots, -1}_{n-s} >$ est $(-1)^{n-s}$. Il ne suffit donc pas pour distinguer des formes non isométriques.

3) Supposons $K = \mathbb{F}_q$. Le noyau de $\mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times$, $x \longmapsto x^2$ est $\{1, -1\}$. Donc $\mathbb{F}^\times/(\mathbb{F}^\times)^2$ est d'ordre 2. Donc si $\alpha \in \mathbb{F}^\times/(\mathbb{F}^\times)^2$, alors toutes les formesquad. non dig. sont isométriques à $< \underbrace{1, \ldots, 1}_{s}, \underbrace{\alpha, \ldots, \alpha}_{t} >$ pour des $s, t \geq 0$. On peut faire mieux :

Proposition 16.29. *Soitq une forme quadratique non dégénérée sur $\mathbb{F}_q^n$, si $\alpha \in \mathbb{F}^\times/(\mathbb{F}^\times)^2$. Alors il existe une base dans laquelle q s'écrit sous l'une des formes suivantes*

(1) $q(x) = x_1^2 + \ldots + x_{n-1}^2 + x_n^2$

(2) $q(x) = x_1^2 + \ldots + x_{n-1}^2 + \alpha x_n^2$

Remarque 16.30. Notons que les deux formes ont des discriminants distincts. Donc les formes quadratiques non dégénérées sur $\mathbb{F}_q^n$ sont classifiées à isomorphisme près par leur discriminant.

Démonstration. On procède par récurrence sur n. On va montrer que si $n \geq 2$, il existe $v_1 \in \mathbb{F}_q^n$ t.q. $q(v_1) = 1$. On aura $\mathbb{F}_q^n = Kv_1 \oplus v_1^\perp$ et on obtient le résultat par l'hyp. de récurrence. Ecrivons q dans une base orthogonale : $q(x) = \alpha_1 x_1^2 + \ldots + \alpha_n x_n^2$. Le nombre de carrés dans $\mathbb{F}_q$ est $\frac{q+1}{2}$. Considérons $E = \{\alpha_1 x_1^2 | x_1 \in \mathbb{F}_1\}$ et $F = \{1 - \alpha_2 x_2^2 | x_2 \in \mathbb{F}_q\}$. Clairement, on a $|E| = |F| = \frac{q+1}{2}$. Comme on a $2 \cdot \frac{q+1}{2} \geq q$, on doit avoir $E \cap F \neq \emptyset$. Si $\alpha_1 x_1^2 = 1 - \alpha_2 x_2^2$, alors $1 = \alpha_1 x_1^2 + \alpha_2 x_2^2 = q(x_1, x_2, 0 \ldots, 0)$. □

Remarque 16.31. Notons $O(\alpha_1, \ldots, \alpha_n)$ le groupe des isométrie de la forme $\alpha_1 x_1^2 + \ldots + \alpha_n x_n^2$ sur $\mathbb{F}_q^n$. Alors on a

1) $O(1, \ldots, 1) = O(\alpha, \ldots, \alpha)$.

2) A isomorphisme près, $O(\alpha, \ldots, \alpha)$ ne dépend que de disc $< \alpha_1, \ldots, \alpha_n >= \alpha_1 \cdots \alpha_n$ modulo $K^{\times 2}$

   Si $n = 2m+1$ est impair, il résulte de 1) et 2) qu'à isomorphisme près, il n'existe qu'un seul groupe orthogonal en dimension $n = 2m + 1$. On le note $O_{2m+1}(\mathbb{F}_q)$.

   Si $n = 2m$ est pair, on note $O_{2m}^+(\mathbb{F}_q) = O(< 1, \ldots, 1)$ et $O_{2m}^-(\mathbb{F}_q) = O(< \alpha, \ldots, \alpha >)$ les deux groupes d'isométries possibles. On verra qu'ils sont d'ordres différents donc non isomorphes.

16.2 Réduction simultanée de formes quadratiques

Supposons que K est un corps alg. clos de caractéristique $\neq 2$, V un espace vectoriel de dimension $n \leq \infty$, $q : V \longrightarrow K$ une forme quadratique non dégénérée et $q' : V \longrightarrow K$ une forme quadratique.

Lemme 16.32. *Supposons que la matrice M' de q' dans une base orthonormale pour q (i.e. $b(v_i, v_j) = \delta_{ij}$, $q = q_b$) admet n valeurs propres distinctes 2 à 2 . Alors V admet une base qui est à la fois orthonormale pour q et orthogonale pour q.*

Remarque 16.33. On peut donc "réduire simultanément" q et q'.

Démonstration. Soit $v_1, v_2, \ldots, v_n$ une base orthonormale pour q comme dans l'énoncé. Soit M' la matrice de q' dans cette base et soient une $w_1, w_2, \ldots, w_n \in K^n$ des vecteurs propres de M' avec valeurs propres $\lambda_1, \lambda_2, \ldots, \lambda_n$. Alors pour $i \neq j$, on a

$$\begin{array}{ccccc} {}^t w_i M' w_j & = & {}^t w_i \lambda_j w_j & = & \lambda_j {}^t w_i w_j \\ \| & & & & \\ {}^t w_j M' w_i & = & {}^t w_j \lambda_i w_i & = & \lambda_i {}^t w_j w_i = \lambda_i {}^t w_i w_j \end{array}$$

(b' sym.)

□

Comme $\lambda_i \neq \lambda_j$, on a ${}^t w_i w_j = 0 = {}^t w_i M' w_j$ de façon que la base $w_1, w_2, \ldots, w_n$ est orthogonale à la fois pour q et q'. Comme q est non dégénérée. On a ${}^t w_i w_j \neq 0$, $\forall i$ et la base des $\frac{w_i}{\sqrt{{}^t w_i w_j}}$ est orthonormale pour q et orthogonalepour q'.

16.2.1 cas d'un vecteur isotrope

supposons que K est un corps de caractéristique $\neq 2$, V un espace vectoriel de dimension finie et $b : V \times V \longrightarrow K$ une forme non dégénérée symétrique ou alternée.

Lemme 16.34. *Si ve V est un vecteur isotrope non nul, il existe un vecteur isotrope w tel que $b(v, w) = 1$.*

Terminologie. *le couple (v, w) est un couple hyperbolique et $(P, b|_V) \subseteq (V, b)$ est un plan hyperbolique.*

Remarque 16.35. Soit $P \subseteq V$ le plan engendré par v et w. Alors la matrice de $b|_V$ dans la base v, w est $\begin{bmatrix} 0 & 1 \\ \epsilon & 0 \end{bmatrix}$, où $\epsilon = 1$ si b est symétrique et $\epsilon = -1$ si b est alternée.

Démonstration. comme b est non dégénérée et $v \neq 0$, il existe w' telque $b(v, w') = 1$. On prend alors $w = w' - \frac{1}{2}b(w, w')v$ pour obtenir $b(w, w) = 0$ dans le cas alterné et

$$b(w, w) = b(w', w') - 2 \cdot \frac{1}{2}b(w', w')b(w', v) = 0$$

dans le cas symétrique. □

Remarque 16.36. Soit $P \subseteq V$ un plan hyperbolique. Alors $b|_p$ est non dégénérée. On a donc une décomposition orthogonale $V = P \overset{\perp}{\oplus} P^\perp$ (on écrit $V = U \overset{\perp}{\oplus} W$ si $V = U \oplus W$ et $U \perp V$). La forme $b|_{P^\perp}$ est encore non dégénérée. Donc si $P^\perp$ contient un vecteur isotrope, on a $V = P \overset{\perp}{\oplus} P' \overset{\perp}{\oplus} (P \oplus P')^\perp$ etc.

Terminologie. *(V, b) est anisotrope si V ne contient aucun vecteur non nul isotrope.*

Un espace hyperbolique est une somme orthogonale de plans hyperboliques.

Corollaire 16.37. *(a) Si (V, b) est non dégénérée et alternée, alors (V, b) est isométrique à un espace hyperbolique, i.e. il existe une base $v_1, v_2, \ldots, v_{2m-1}, v_{2m}$ de V dans laquelle la matrice de b est*

$$\begin{bmatrix} 0 & 1 & & & & & \\ -1 & 0 & & & & & \\ & & 0 & 1 & & & \\ & & -1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & 1 \\ & & & & & -1 & 0 \end{bmatrix}$$

En particulier, $\dim V$ *est pair. On note $Sp_{2m}(K)$ le groupe des isométries et on l'appelle groupe symplectique.*

(b) Si (V,b) est non dégénéré et symétrique, alors (V, b) est isométrique à une somme orthogonale $H \overset{\perp}{\oplus} A$,où H est un espace hyperbolique et A un espace anisotrope .

Remarque 16.38. On verra que dans b), l'indice de la forme b , i.e. $\frac{1}{2}\dim H$, ne dépend que de (V, b).

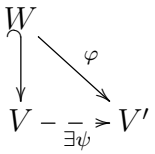
Exemple 16.39. (1) Toute forme quadratique $< \alpha, -\alpha >$ sur K^2 est un plan hyperbolique car on a le vecteur isotrope $e_1 + e_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$. Dans la base $e_1 + e_2$, $\frac{1}{2\alpha}(e_1 - e_2)$ sa matrice est $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

(2) Si $K = \mathbb{R}^n$, toute forme quadratique est isométrique à une forme $< \underbrace{1, \ldots, 1}_{s}, \underbrace{-1, \ldots, -1}_{t} >$.
Si $s \leq t$, on a $< \underbrace{1, \ldots, 1}_{s}, \underbrace{-1, \ldots, -1}_{t} > \cong P^s \oplus < \underbrace{-1, \ldots, -1}_{t-s} >$, où P est le plan hyperbolique $< 1, -1 >$ et $< \underbrace{-1, \ldots, -1}_{t-s} >$ est anisotrope (cas définie négative).

16.3 Le théorème de Witt

Supposons que K est un corps de $car(K) \neq 2$. Soient V,V' du K- espaces vectoriels de dimension finie.

Théorème 16.40 (Witt)**.** *soient (V, b) et (V', b') des espaces du même type isométriques et non dégénérés. Soit $W \subseteq V$ un ss-espace et $\varphi : W \longrightarrow V'$ une isométrie. Alors il existe une sométrie $\psi : V \longrightarrow V'$ telle que $\psi|_W = \varphi$.*



Définition 16.41. Soit $v \in V$ telque $q(v) \neq 0$ où $q = q_b$ (donc b est symétrique). On a la décomposition $V = Kv \oplus v^\perp$. La réflexion par rapport à $v^\perp$ est l'isométrie $s_v : V \xrightarrow{\sim} V$ donné par $S_v(v) = -v$ et $s_v(w) = w$, $\forall w \in v^\perp$.

Remarque 16.42. Explicitement, on a $s_v(x) = x - \frac{2b(v,x)}{b(v,v)} \cdot x$, $\forall x \in V$.

Lemme 16.43. *Soient $v, w \in V$ tels que $q(v) = q(w) \neq 0$. Alors il existe une isométrie $\alpha : (V, b) \xrightarrow{\sim} (V, b)$ telle que $\alpha(v) = w$.*

Remarque 16.44. e lemme implique le thm de Witt si $W = Kv$, $b(v, v) \neq 0$:

Démonstration. On a $q(v + w) + q(v - w) = 4q(v)$. Donc $v + w$ ou $v - w$ est non isotrope. Disons que $v + w$ est non isotrope . Alors on a $s_{v+w}(v) = s_{v+w}(\frac{1}{2}(v + w) + \frac{1}{2}(v - w)) = -\frac{1}{2}(v + w) + \frac{1}{2}(v - w) = -w$ et $\alpha = (-Id_V) \circ s_{v+w}$ envoie v sur w. □

Lemme 16.45. *Soit $W \subseteq V$ un ss-espace totalement isotrope avec une base $v_1, v_2, \ldots, v_r$. Alors il existe $v'_1, v'_2, \ldots, v'_r$ dans V tels que*

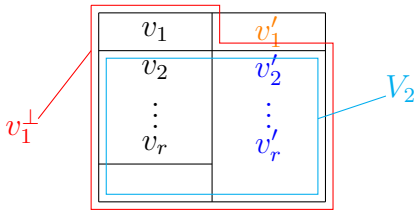
(1) v_i, v'_i est un couple hperbolique pour tout $1 \leq i \leq r$ et

(2) $P_1, P_2, \ldots, P_r$ sont en somme directe orthogonale, où $P_i = Kv_i + Kv'_i$.

En outre, toute isométrie $W \xrightarrow{\varphi} V'$ se prolonge en une isométrie $P_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} P_r \xrightarrow{\psi} V'$.

Démonstration. Supposons que $r = 1$. On sait qu'il existe $v' \in V$ isotrope tel que (v_1, v_1') est un couple hyperbolique . De même , il existe $v_1'' \in V$ isotrope tel que $\varphi(v_1)$, v_1'' est un couple hyperbolique de V'. Alors $\psi : v_1 \longmapsto \varphi(v_1)$, $v_1' \longmapsto v_2''$ définit une isométrie $P_1 \xrightarrow{\psi} V'$.

Supposons que $r \geq 2$. Posons $W_2 = Kv_2 + \ldots + Kv_r$. L' supposons hyperplan $v_1^\perp$ contien v_1 et W_2. Soit V_2 un supplémentaire de Kv_1, dans $v_1^\perp$ contenant W_2. La restriction de b à V_2 est non dégénérée. On applique l'hypothèse $V2$ de récurrence à son Ssespace totalement isotrope W_2.

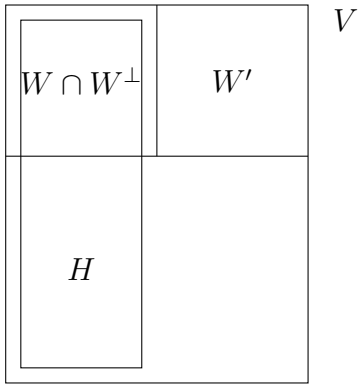


Il existe des vecteurs $v_1', v_2', \ldots, v_r'$ dans dans V_2 tq. v_i, v_i' soit un couple hyperbolique avec les propriétés de l'énoncé. La somme $P_2 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} P_r$ est orthogonale à v_1 et la restriction de b y est non dégénérée. Il existe donc v_1' dans $(P_2 \overset{\perp}{\oplus} \ldots \overset{\perp}{\oplus} P_r)^\perp$ qui forme avec v_1, un couple hyperbolique. On pose $P_1 = Kv_1 + Kv_1'$. On peut appliquer le même raisonnement à $\varphi(W) \subseteq V'$. Comme bert non dégénérée, φ est injective et $\varphi(W) = K\varphi(v_1) + \ldots + K\varphi(v_r)$ est totalement isotrope. On construit alors des paires hyperboliques $\varphi(v_i), v_i''$ et en prolonge φ en ψ en envoyant v_i' sur v_i''.

□

Dém du Thm de Witt. On commence par étendre φ à un ss-espace $\overline{W} \supseteq W$ tel que la restriction de b à $\overline{W}$ est non dégénérée . Soit W' un supplémentaire de $W \cap W^\perp = \ker(b|_W)$ dans W. La restriction de b à W' est non dégénérée donc aussi la restriction à $W'^\perp$. Le ss-espace $W'^\perp$ contient $W \cap W^\perp$ comme ss-espace totalement isotrope. Par le lemme précédent, on peut donc étendre $\varphi_{W \cap W^\perp}$ à un ss-espace hyperbolique H t.q. $W \cap W^\perp \subseteq H \subseteq W'^\perp$. On a ainsi étendu φ en $\overline{\varphi}$ défini sur $H \oplus W' = \overline{W}$ et la restriction de b à $\overline{W}$ est non dégénérée. La

restriction de b' à $\overline{\varphi}(\overline{W}) = \overline{\varphi}(H) \oplus \varphi(W')$ est aussi non dégénérée.



Si b est alternée, les restrictions non dég. de b à $\overline{W}^{\perp}$ et de b' à $\overline{\varphi}(\overline{W})^{\perp}$ sont isométriques(il n'existe qu'une seule classe d'isom. de formes symplectique sur un espace vectoriel de dimension paire). On a ainsi étendu φ à $\overleftarrow{W} \overleftarrow{\oplus} \overleftarrow{W}^{\perp} = V$.

Supposons donc b symétrique. Deplus, comme (V, b) et (V', b') sont isométriques, on peut supposer $(V, b) = (V', b')$. On raisonne par récurrence sur $\dim \overline{W}$. On a déjà traité le cas où $\dim \overline{W} = 1$ (à l'aide d'une réflexion resp. d'une complétion en couple hyperbolique). Supposons $\dim \overline{W} \geq 2$. Ecrivons $\overline{W} = W_1 \overleftarrow{\oplus} W_2$, où W_1 et W_2 sont non nuls et les restrictions de b à W_1 et W_2 sont non dégénérées. Par l'hypothèse de récurrence, $\varphi|_{W_2} : W_2 \longrightarrow \varphi(W_1)^{\perp}$ se prolonge en une isométrie $\varphi_2 : W_1^{\perp} \longrightarrow \varphi(W_1)^{\perp}$. On prend alors $\psi = \varphi|_{W_1} \oplus \varphi_2 : W_1 \oplus W_1^{\perp} \longrightarrow \varphi(W_1) \oplus \varphi(W_1)^{\perp}$. □

Corollaire 16.46. *(a) Si W et W' sont des ss-espaces isométriques de V, les ss-espaces $W^{\perp}$ et $W'^{\perp}$ sont isométriques.*

(b) Tous les ss-espaces totalement isotropes maximaux ont même dimension v appelée l'indice v de b.

(c) Tous les ss-espaces hyperboliques maximaux ont même dimension $2v$.

(d) Si H est un ss-espace hyperbolique maximal, on peut écrire $V = H \overleftarrow{\oplus} W$, ou W est anisotrope (ne contient pas de vecteur isotrope non nul).

Démonstration. (a) Une isométrie $\varphi : W \xrightarrow{\sim} W'$ s'étend en une isométrie $\psi : V \xrightarrow{\sim} V$ qui induit une isométrie de $W^{\perp}$t sur $W' \perp$.

(b) Si W et W' sont totalement isotropes et $\dim W \leq \dim W'$, toute application linéaire injective $\varphi : W \longrightarrow W'$ est une isométrie, qui s'étend en une isométrie $\psi : V \longrightarrow V'$. Alors $\varphi^{-1}(W')$ contient W et est aussi totalement isotrope. Donc $W = \varphi^{-1}(W')$ si W est maximal.

(c) Tout ss-espace totalement isotrope de dimension d est contenu dans un ss-espace hyperbolique de dimension $2d$ et réciproquement. Donc (c) résulte de (b).

(d) Déjà vu.

□

Exemple 16.47. (a) Si K est un corps quadratiquement clos, une forme quadratique non dégénérée est d'indice $\lfloor n/2 \rfloor$.

(b) Si q est une forme quadratique non dégénérée sur $\mathbb{R}^n$ de signature (s,t), alors l'indice de q est $min(s,t)$. Si $H \subseteq \mathbb{R}^n$ est un ss-espace hyperbolique maximal et $H \neq V$, la forme induite sur $H^\perp \subseteq V$ est ou bien définie positive ou bien définie nég. . La doimention de H et le signe de la forme sur $H^\perp$ déterminent la signature de (V,b), qui est donc bien un invariant de la classe d'isométrie de (V,b).

(c) Soit $K = \mathbb{F}_q$, q impair. Rappelons que les formes quadratiques non dégénérées sur $\mathbb{F}_q^n$ sont isométriques ou bien à $< 1, \ldots, 1 >$ ou bien à $< 1, \ldots, 1, \alpha >$, où $\alpha \in \mathbb{F}_q^\times$ n' estpas un carré. On a vu que toute forme quad. non dég. q sur K^n, $n \geq 2$, admet un vecteur x t.q. $q(x) = 1$. Le même argument montre que pour $\alpha_1, \alpha_2, \alpha_3 \in K^\times$, l'équation $\alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2 = 0$ admet une solution $x \neq 0$. Donc toute forme quad. non dég. sur K^n, $n \geq 3$, admet un vecteur isotrope. Si on écrit $< \alpha_1, \ldots, \alpha_n > \cong H \oplus W$, où H est un espace hyperbolique et W est anisotrope, on a donc $\dim W \leq 2$. En dimension 2,

— la forme $< 1, -1 >$ admet le vecteur isotrope $x = e_1 + e_2$,

— la forme $< 1, -\alpha >$ n'admet pas de vecteur isotrope nonnul (carl'équation $x_1^2 = \alpha x_2^2$ n' admet pas de solution $x \neq 0$ si α n'est pas un carré).

Si on a une forme quad. non dégénérée sur

— K^{2m+1}, $m \in \mathbb{N}$, alors elle est isométrique à $H \oplus W$, où $\dim W = 1$ et H est un espace hyperbolique. Alors l'indice de la forme est $v = m$. On rappelle qu'il n' y a qu'un seul groupe d'isométries (à isom. près) noté $O_{2m+1}(\mathbb{F}_q)$.

— K^{2m}, $m \in \mathbb{N}$, alors ou bien l'espace est hyperbolique ($W = 0$) et l'indice vaut m, ou bien l'indice vaut $m-1$ et $W =< 1, -\alpha >$. Rappelons que les deux groupes d'isométries correspondants sont noté $O_{2m}^+(\mathbb{F}_q)$ et $O_{2m}^-(\mathbb{F}_q)$.

16.4 Le groupe de Witt

Soit K un corps.

Définition 16.48. Le monoïde de Witt (ou semi-groupe de Witt) est l'ensemble $MW(K)$ des classes d'isométrie $[(V,q)]$ de couples (V,q), où V est un espace vectoriel de dimension finie et q une forme quadratique sur V. On le munit de l'addition définie par

$$[(V,q)] + [(V',q')] = [(V \oplus V', q \overset{\perp}{\oplus} q')],$$

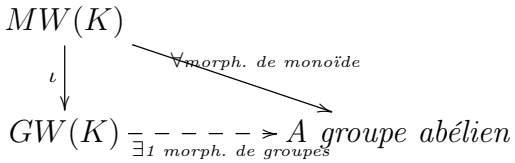
où $(q \overset{\perp}{\oplus} q')(v,v') = q(v) + q'(v')$.

Remarques 16.49. *(1) Le monoïde de Witt est associatif et admet l'élément neutre* $(V = \{0\}, q = 0)$. *Par contre aucun élément non nul* $[(V,q)]$ *admet un inverse* $[(V',q')]$ *car si* $[(V,q)] + [(V',q')] = [(0,0)]$, *alors* $\dim V + \dim V' = 0$.

(2) Abrégeons $[(V,q)]$ *par* $[q]$. *Si on a* $[q]+[r] = [q]+[s]$ *dans* $MW(K)$, *alprs par le théorème de Witt, on a* $[r] = [s]$.

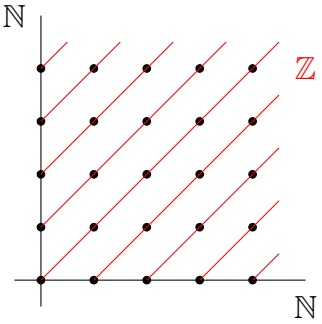
Lemme 16.50 (Lemme et déf.)**.** *IL existe un morphisme de monoïdes universel* $MW(K) \xrightarrow{\iota} GW(K)$ *vers un groupe abélien* $GW(K)$ *appelé groupe de Grothendieck-Witt de K. Il est injectif.*

Universalité :



Démonstration. On définit $GW(K) = MW(K) \times MW(K)/\sim$, où

$$([q_1],[q_2]) \sim ([r_1],[r_2]) \Leftrightarrow [q_1] + [r_2] = [q_2] + [r_1]$$



L'addition est induite par l'addition composante par composante . L'injectivité du morphisme $MW(K) \longrightarrow GW(K)$, $[q] \longmapsto$ classe de ([q],0) résulte du thm de Witt. □

Remarques 16.51. *(1) Par la propriété universelle , on obtient des morphismes de groupes (surjectifs)* $\dim : GW(K) \longrightarrow \mathbb{Z}$ *t.q.* $\dim \iota([V,q]) = \dim V$ *et* $\mathrm{disc} : GW(K) \longrightarrow K^\times/(K^\times)^2$ *t.q.* $\mathrm{disc}\,\iota([V,q]) = \mathrm{disc}(q)$.

(2) On sait que $< \alpha, -\alpha >$ *est isométrique au plan hyperbolique P,* $\forall \alpha \in K^\times$. *Il s'ensuit-qu'on a* $\iota([q]) + \iota([-q]) = \dim(q) \cdot \iota([P])$ *dans* $GW(K)$ *pour toute forme quadratique non dégénérée q.*

Définition 16.52. le groupe de Witt $W(K)$ est le quotient de $GW(K)$ par le ss-groupe engendré par le plan hyperbolique $\iota([P])$.

Remarques 16.53. *(1) Dans* $W(K)$, *on a* $[q] + [-q] = 0$ *et donc* $-[q] = [-q]$.
Abus de notation : on écrit $[q]$ *au lieu de "classe de* $\iota([q])$ *dans* $W(K)$*".*

(2) On a un isomorphisme de monoïdes $MW(K)/(\text{ss-monoïde eng. par } [P]) \xrightarrow{\sim} W(K)$. *C'est la définition originelle de* $W(K)$ *par Witt.*

(3) Dans $W(K)$, *on a les relations suivantes :*

$$[< \alpha_1, \ldots, \alpha_m >] = [\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(m)}] \quad \text{pour tout } \sigma \in \mathfrak{A}_m.$$

$$[< \alpha_1, \ldots, \alpha_m >] + [< \beta_1, \ldots, \beta_n >] = [< \alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n >], \quad \forall \alpha_i, \beta_j \in K^\times.$$

$$-[< \alpha_1, \ldots, \alpha_m >] = [< -\alpha_1, \ldots, -\alpha_m >].$$

$$[< \alpha, -\alpha >] = 0.$$

(4) $\dim : GW(K) \longrightarrow \mathbb{Z}$ *induit un morphisme* $W(K) \longrightarrow \mathbb{Z}/2\mathbb{Z}$ *mais* $\mathrm{disc} : GW(K) \longrightarrow K^\times/(K^\times)^2$ *n'induit pas de morphisme défini sur* $W(K)$ *sauf si* $-1- = disc(P)$ *est un carré dans K.*

(5) On sait que tout $[q] \in MW(K)$ *s'écrit* $[H] + [W]$, *où H est hyperbolique et W est anisotrope. Avec la remarque (2), cela implique que tout élément de W(K) est de la forme [q] pour une forme anisotrope. Plus précisément, on a une bijection*

$$\{\text{formes quad. anisotropes}\}/\text{isométrie} \xrightarrow{\sim} W(K).$$

Montrons l'injectivité : si q_1 *et* q_2 *sont anisotropes et* $[q_1] = [q_2]$ *dans W(K), alors on a une isométrie*

$$q_1 \oplus P^{\oplus n_1} \cong q_2 \oplus P^{\oplus n_2}$$

(par la remarque (2)). Alors on a $n_1 = n_2$ *(l'indice ne dépend que de la classe d'isométrie) et* $q_1 \cong q_2$ *(thm de Witt).*

Exemple 16.54. (1) Si K est un corps quadratiquement clos, alors $W(K) \longrightarrow \mathbb{Z}/2\mathbb{Z}$ est un isomorphisme (exercice !).

(2) Si -1 est un carré dans K, on a $[g] = [-q] = -[q]$dans $W(K)$. Donc tout élément de $W(K)$ est d'ordre ≤ 2.

(3) Toute forme quad. réelle anisotrope est isométrique à $< 1, \ldots, 1 >$ ou $< -1, \ldots, -1 >$ et $< -1 >= - < 1 >$ dans $W(K)$. Donc $\mathbb{Z} \cong W(\mathbb{R})$.
Exercice : Montrer qu'on a un isomorphisme $\begin{bmatrix} \dim \\ s \end{bmatrix} : GW(\mathbb{R}) \xrightarrow{\sim} \mathbb{Z} \oplus \mathbb{Z}$, où $s : GW(K) \longrightarrow \mathbb{Z}$ envoie $< \underbrace{1, \ldots, 1}_{s}, \underbrace{-1, \ldots, -1}_{t} >$ sur s. Plus simple : On a un isomorphisme de monoïdes $\mathbb{N} \times \mathbb{N} \xrightarrow{\sim} MW(\mathbb{R})$, $(s,t) \longmapsto < \underbrace{1, \ldots, 1}_{s}, \underbrace{-1, \ldots, -1}_{t} >$!

(4) Soit $K = \mathbb{F}_q$, q impair, Alors

$$W(K) = \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & si \ -1 \in K^{\times 2} \\ \mathbb{Z}/4\mathbb{Z} & si \ -1 \notin K^{\times 2} \end{cases}$$

Démonstration. Soit $\alpha \in K^\times / K^{\times 2}$. On a quatre classes d'isométrie de formes anisotropes : $0, < 1 >, < \alpha >$ et $< 1, -\alpha >$. Donc $W(K)$ est d'ordre 4 et isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Si -1 est un carré dans K, on sait que tout élément de $W(K)$ est d'ordre ≤ 2 et $W(K) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Si -1 n'est pas un carré, on peut prendre $\alpha = -1$ et on a $[< 1 >] + [< 1 >] = [< 1, 1 >] = [< 1, -\alpha >]$ de façon que $[< 1 >]$ est d'ordre 4 et $W(K) = \mathbb{Z}/4\mathbb{Z}$. □

(5) On peut montrer qu'on a une suite exacte

$$0 \longrightarrow \mathbb{Z} \cdot < 1 > \longrightarrow W(\mathbb{Q}) \longrightarrow \bigoplus_{p \ premier} W(\mathbb{F}_p) \longrightarrow 0$$

17 Groupe symplectique

Soient K un corps de caractéristique $\neq 2$ et soit V un espace vectoriel de dimension finie paire 2n. Soit b une forme symplectique sur V, c'est-à-dire une forme alternée non dégénérée. Rappelons que dans une base bien choisie, la matrice de b est de la forme $J_{2n} = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$. Dans une telle base $v_1, v_2, \ldots, v_{2n}$ les v_i, v_{i+n} forment des couples hyperboliques orthogonaux 2 à 2.

On va étudier le groupe symplectique $Sp(V,b)$.

Par le choix d'une base comme ci-dessus il s'identifie avec le groupe $Sp_{2n}(K) = \{U \in Gl_n(K) | {}^tUJ_{2n}U = J_{2n}\}$.

Si on écrit $U = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$, on a $U \in Sp_{2n}(K) \Leftrightarrow \begin{cases} {}^tAC = {}^tCA, {}^tBD = {}^tDB \\ {}^tAD - {}^tCB = I_n \end{cases}$. Pour $n = 1$, on obtient $Sp_2(K) = Sl_2(K)$(même ss-groupe de $Gl_2(K)$!).

17.1 Générateurs

Définition 17.1. Soit $l : V \to K$ une forme linéaire. Soit $a \in \ker(l)$. La transvection associée avec l et a est l'application linéaire $\tau_{l,a} : V \longrightarrow V$, $x \longmapsto \tau(x) = x + l(x)a$.

Remarques 17.2. *1) On a $\tau_{l,a} \circ \tau_{l,-a} = Id_V$ de façon que $\tau_{l,a}$ est inversible.*

2) Avec $\tau \circ \tau_{l,a}$, on a

$$b(\tau(x), \tau(y)) = b(x + l(x)a, y + l(y)a) = b(x,y) + l(y)b(x,a) + l(x)b(a,y).$$

On voit que pour $l = \lambda b(a, ?)$,$\lambda \in K$,l'automorphisme $\tau_{l,a}$ est symplectique (i.e. $\tau_{l,a} \in Sp(V,b)$). On dit alors que $\tau_{l,a}$ est une transvection symplectique.

Notons qu'en dimension 2, toutes les transvection sont symplectique, car $\hat{b} : V \longrightarrow V^\times$ est un isomorphisme et $\ker b(a, ?) = K_a$ si $a \neq 0$. Autre raison dét$(\tau_{l,a}) = 1$ et $Sl(V) = Sp(V,b)$ si $\dim V = 2$.

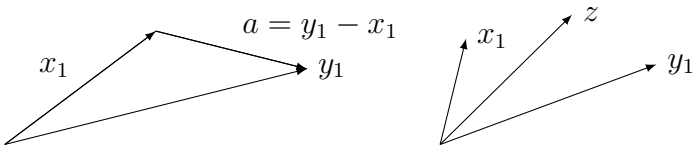
Théorème 17.3. *$Sp(b,V)$ est engendrépar les transvection symplectique.*

Corollaire 17.4. *Le groupe symplectique est un sous-groupe de $Sl(V)$.*

Dém du Cor. Toute transvection est de déterminant 1. □

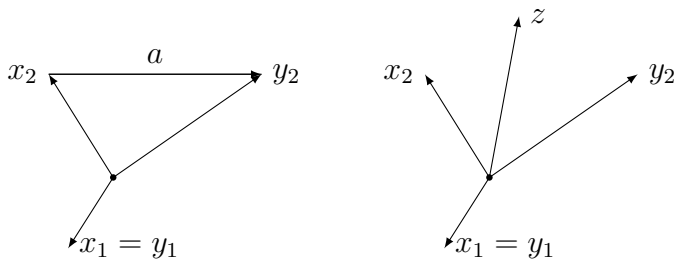
Lemme 17.5. *Si x_1, x_2 et y_1, y_2 sont des couples hyperboliques , il existe un produit d'au plus quatre transvection hyperboliques q tel que $\varphi(x_1) = y_1$ et $\varphi(x_2) = y_2$.*

Démonstration. Si $b(x,y) \neq 0$, onpeut envoyer x, suey, par la transvection symplectique $\tau_{l,a}$ associée à $l = \frac{1}{b(x_1,y_1)} b(y_1 - x_1, \cdot)$ et $a = y_1 - x_1$.



Sinon on peut trouver z tel que $b(x_1, z) \neq 0$ et $b(z, y_1) \neq 0$ (car V n'est pas la réunion des hyperplans $x^\perp$ et $y^\perp$!) et on peut envoyer successivement x_1 sur z puis z sur y_1. On est ainsi ramené au cas où $x_1 = y_1$, et on veut envoyer x_2 sur y_2 tout en laissant x_1 fixe. Si $b(x_2, y_2) \neq 0$, la transvection symplectique associée à $l = \frac{1}{b(x_2,y_2)} b(y_2 - x_2, \cdot)$ et $a = y_2 - x_2$ convient car

$$b(y_2 - x_2, x_1) = b(y_2, y_1) - b(x_2, x_1) = 0.$$



Si $b(x_2, y_2) = 0$, on cherche un z tel que

— $b(x_2, z) \neq 0$ et $b(z, y_2) \neq 0$ et

— $b(z - x_2, x_1) = 0$ et $b(y_2 - z, x_1) = 0$, i.e. $b(x, z) = 1$.

Or $z = x_1 + y_2$ vérifie toutes conditions. □

Dém. du Thm. On peut supposer que $\dim V = 2n \geq 2$, où $V = K^{2n}$. V contient un plan hyperbolique P engendrépar un couple hyperbolique x_1, x_2. Soit $\psi \in Sp(V, b)$. Alors $Q = \psi(P)$ est encore unplan hyperbolique. Par le lemme, il existe un produit φ d' au plus quatre transvection, symplectique tel que $\varphi(x_1) = \psi(x_1)$ et $\varphi(x_2) = \psi(x_2)$. Alors $\varphi^{-1}\psi$ nduit l'identité dans P et induit un élément du $Sp(P^\perp, b|_{P^\perp})$ dans $P^\perp$, i.e. on a $\varphi^{-1}\psi = Id_P \oplus \psi' : P \oplus P^\perp \longrightarrow P \oplus P^\perp = V$ pour un $\psi' \in Sp(P^\perp, b|_{P^\perp})$. Par récurrence sur $\dim V$ est un produit d'au plus $4(n-1)$ transrections symplectique $\tau_1, \ldots, \tau_m$ de $P^\perp$. Les τ_i sont aussi des transrections symplectique, de V qui induisent l'identité dans P car $\tau_i = \tau_{l_i, a_i}$ où $a_i \in P^\perp$ et $l_i = \lambda_i b(a_i, \cdot)$. On a donc $\psi = \varphi \circ \tau_1 \circ \ldots \circ \tau_m$ et ψ est produit d'au plus $4n$ transrections symplectique . □

17.2 Centre

soit u un élément du centre de $Sp(V,b)$. Soient $0 \neq a \in V$, $l = b(a,\cdot)$ et $\tau = \tau_{l,a}$.Alors

$$u \circ \tau_{l,a}(x) = u(x + b(a,x)a) = u(x) + b(a,x)u(a)$$
$$\tau_{l,a} \circ u(x) = \tau_{l,a}(u(x)) = u(x) + b(a,u(x)) \cdot a$$

On peut trouver x t.q. $b(a,x) \neq 0$ et on déduit que $u(a)$ est proportionnel à a pour tout $a \in V$. Donc u est une homothétie de rapport de $\lambda \in K^\times$. On a donc pour tous $x, y \in V$. Donc $\lambda^2 b = b$ et $\lambda^2 = 1$ et $\lambda \in \{1, -1\}$. Donc le centre de $Sp(V,b)$ est réduit à $\{\pm Id_V\}$.

Le groupe symplectiqueprojectif associé est $PSp(V,b) = Sp(V,b)/\{\pm Id_V\}$. C'est un sous groupe de $PSl(V)$. Il agit donc fidèlement dans $\mathbb{P}(V)$.

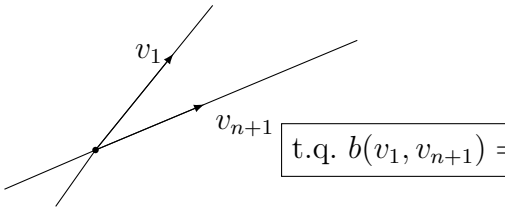
17.3 Ordres des groupes symplectique finis

Soit q une puissance d'un nombre premier impair. Soit $K = \mathbb{F}_q$. Les éléments de $Sp_{2n}(K))$ sont en bijection avec les bases hyperboliques de K^n, i.e. les bases $v_1, v_2, \ldots, v_{2n}$ telles que $v_i.v_{n+i}$ est un couple hyperbolique pour tout $1 \leq i \leq n$ et $K^{2n} = P_1 \overset{\perp}{\oplus} \ldots \overset{\perp}{\oplus} P_n$, où $P_i = Kv_i \oplus Kv_{n+i}$. Il s'ensuit qu'on a

$$\begin{aligned}
|Sp_{2n}(K)| &= (q^{2n}-1) \cdot \frac{q^{2n} - q^{2n-1}}{q-1} \cdot |Sp_{2n-1}(K)| \\
&= (q^{2n}-1) \cdot \frac{q^{2n} - q^{2n-1}}{q-1} \cdot (q^{2n-2}-1) \cdot \frac{q^{2n-2} - q^{2n-3}}{q-1} \cdot \ldots \cdot (q^2-1) \cdot \frac{q^2-q}{q-1} \\
&= q^{(2n+1)+(2n+3)+\cdots+3+1}(q^{2n}-1)(q^{2n}-1)(q^{2n-2}-1)\cdots(q^2-1).
\end{aligned}$$

$$|Sp_{2n}(\mathbb{F}_q)| = q^{n^2}(q^{2n}-1)(q^{2n-2}-1)\cdots(q^2-1).$$

$$|PSp_{2n}(\mathbb{F}_q)| = \tfrac{1}{2}|Sp_{2n}(\mathbb{F}_q)| = q^{n^2}(q^{2n}-1)(q^{2n-2}-1)\cdots(q^2-1).$$



17.4 Groupe dérivé

Soit K un corps de caractéristique $\neq 2$.

Théorème 17.6. *Pour $n \geq 2$, le groupe symplectique $Sp_{2n}(K)$ est égal à son groupe dérivé.*

Démonstration. Comme $Sp_{2n}(K)$ est engendré par les transvection
symplectiques, il suffit de montrer que chaque transvection symplectique est un commutateur. Notons $V = K^{2n}$. Soient $0 \neq v \in V$, $\lambda \in K$ et $l = \lambda b(v, \cdot)$. Montrer que $\tau_{l,v}$ est un commutateur. Rappelons que

$$\tau_{l,v}(x) = x + \lambda b(v, x) \cdot v.$$

On saitqu'onpeutcompléter v en un couple hyperbolique v, w. Soit $P = Kv \oplus Kw$ leplan hyperbolique engendrépar v et w. Comme $2n \geq 4$, on a $V = P \overset{\perp}{\oplus} Q \overset{\perp}{\oplus} W$, où Q est le plan hyperbolique engendré par un couple hyperbolique v', w'. Complétons v, w, v', w' en une base hyperbolique de V. Dans cette base la transvection $\tau = \tau_{l,v}$ a pour matrice $\left[\begin{array}{c|c} N(\lambda) & 0 \\ \hline 0 & I_{2n-4} \end{array}\right]$, où $N(\lambda) = \left[\begin{array}{cc|cc} 1 & 0 & \lambda & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right]$. Il suffit d'exprimer $N(\lambda)$ comme un commutateur d'éléments du groupe $Sp_4(K) = \{U \in Gl_4(K) | {}^tUJ_4U = J_4\}$. Or les matrices

$$U_1 = \begin{bmatrix} A_1 & 0 \\ 0 & {}^tA_1^{-1} \end{bmatrix}, \quad U_2 = \begin{bmatrix} I_2 & A_2 \\ 0 & I_2 \end{bmatrix}$$

sont symplectique si A_1 est inversible et A_2 symétrique. Si on prend $A_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ et $A_2 = \lambda \cdot \frac{1}{2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, alors on vérifie qu'on a $U_1U_2U_1^{-1}U_2^{-1} = N(\lambda)$. □

17.5 Simplicité

Théorème 17.7. *Supposons que $car(k) \neq 2$ et que $n \geq 2$. Alors $Sp_{2n}(K)$ est simple.*

Pour la démonstration, on a besoin de quelques rappels et compléments : Soit G un groupe. un ss-groupe $H \leq G$ est maximal si $H \neq G$ et si $H \leq K \leq G$, alors $H = K$ ou $K = G$. Soit X un G-ensemble. L'action de G sur X est transitive si, $\forall x, y \in X$, il existe $g \in G$ t.q. $gx = y$. L'action est primitive si elle est transitive et les stabilisateurs $G_x = \{g \in G | gx = x\}$ sont des ss-groupes maximaux.

Exemple 17.8. l'action de $PSl_n(K)$ sur $\mathbb{P}^{n-1}(K)$ est primitive car elle est fidèle et deux fois transitive (i.e. transitive et transitive sur l'ensemble des couples d'élément distinct). Voir la première partie du cours.

Proposition 17.9. *Supposons que l'action de G sur X est primitive. Supposons que pour tout $x \in X$, on a un ss-groupe $T_x \leq G$ t.q.*

1) T_x est abélien, $\forall x \in X$,

2) $T_{gx} = gT_xg^{-1}$, $\forall x \in X$, $\forall g \in G$,

3) G est engendrépar la réunion des T_x, $x \in X$.

Alors tout ss-groupe distingué H de G qui agit non sur X contient le groupe dérivé $\mathcal{D}(G)$.

Démonstration. Soit H un ss-groupe distingué qui agit non trivialement sur X. Soit $x \in X$. Comme G_x est maximal, le ss-groupe HG_x (ss-gr. car H est distingué !) est égal à G_x ou à G. 1^{er} cas : $HG_x = G_X$. Alors $H \subseteq G_x$. Mais alors, pour tout $g \in G$, on a $H = hHh^{-1} \subseteq gG_xg^{-1} = G_{g.x}$. Comme l'action est transitive $H \subseteq G_y$, $\forall y \in X$. Donc H agit trivialement sur X.↯

2^e cas : $HG_x = G$. Comme l'action de G sur X est transitive, on a $X = G.x = HG_x = H.x$. Donc H aussi agit transitivement sur X. Je dis que $G = H \cdot T_x$. En effet, pour $h \in H$, on a

$$T_{h.x} = hT_xh^{-1} \subseteq HT_xH = HT_x.$$

Comme l'action de H sur X est transitive, on a $T_y \subseteq HT_x$ pour tout $y \in X$. Or les T_y, $y \in X$, engendrent G. Donc $G = HT_x$. Le quotient $G/H = HT_x/H \xleftarrow{\sim} T_x/T_x \cap H$ st abélien car T_x est abélien. Donc H contient $\mathcal{D}(G)$.

□

Exemple 17.10. soient $G = PSl_n(K)$, $X = \mathbb{P}^{n-1}(K)$ et T_x le ss-groupe des transvections $\tau_{l,a}$ où a est un vecteur de la droite x. Alors l'action est primitive et 1), 2), 3) sont vérifiés.

Donc tout ss-gr. distingué H de $PSl_n(K)$ qui agit non trivialement sur $\mathbb{P}^{n-1}(K)$ contient le groupe dérivé de $PSl_n(K)$. On en déduit que $PSl_n(K)$ est simple si on n'a pas né et $K \in \{\mathbb{F}_2, \mathbb{F}_3\}$.

Dém. du Thm de simplicité. On fait agit $G = PSp_{2n}(K)$sur $X = \mathbb{P}^{2n-1}(K)$ si $x \in X$ est une droite de K^n, on pose

$$T_x = \{\tau_{l,a} | a \in x, l = \lambda b(a, \cdot)\}.$$

Notons que les T_x vérifient 1),2),3) de la Prop. . Soit $H \trianglelefteq Sp_{2n}(K)$ un ss-groupe distingué. Si H agit trivialement dans $\mathbb{P}^{n-1}(K)$, alors $H = \{e\}$ car $PSp_{2n}(K)$ agit fidèlement sur $\mathbb{P}^{n-1}(K)$. On peut donc supposer que H agit non trivialement dans X. La Prop. donnera que H contient $\mathcal{D}(Sp_{2n}(K)) = Sp_{2n}(K)$ si l'action de $G = PSp_{2n}(K)$ sur $X = \mathbb{P}^{2n-1}(K)$ est primitive. Il s'agit demontrer que

a) $Sp_{2n}(K)$ agit transitivement sur X et

b) le stabilisateur G_x de chaque droite $x \in X$ est un ss-groupe maximal.

Le point a) résulte du Thm de Witt car toutes les droits sont anisotropes. Si l'action était deux fois transitive, on aurait immédiatement le point b). Malheureusement, l'action n'est pas deux fois transitive. En fait, l'action diagonale de G sur $\{(x, y) \in X \times X | x \neq y\}$ a deux orbites : en effet, si P est un plan de V, alors ou bien

1) $b|_P \neq 0$ et alors P est hyperboliques ou bien

2) $b|_P = 0$ et alors P est totalement isotrope.

Donc par le thm de Witt on a 2 orbites

(1) L'orbite O_1 des couples de droites (x, y) qui engendrent un plan hyperbolique et

(2) l'orbite O_2 des couples de droites (x, y) qui engendrent un plan totalement isotrope.

Montrons directement que le stabilisateur G_x d'un point $x \in X$ est maximal dans $G = Sp_{2n}(K)$. Supposons que $G_x \leq H \leq G$. Montrons que $H = G$. Comme $G_x \leq H$, l'orbite Hx n'est pas réduite à $\{x\}$. Considérons les translatés gHx, $g \in G$, de l'orbite Hx. Leur réunion contient tous les gHx et est donc égale à X. Montrons que les gHx, $g \in G$ forment une partition de X. Supposons qu'on a $gHx \cap g'Hx \neq \emptyset$. Alors il existe $h, h' \in H$ tels que $ghx = g'h'x$. Donc

$$h^{-1}g^{-1}g'h' \in G_x \subseteq H.$$

Mais alors on a $g^{-1}g' \subseteq H$ et donc $gHx = gH'x$. Posons

$$\Sigma = \{(y, z) \in X \times X | y \neq z \text{ et y et z sont dans la même partie } gHx\} \subseteq X \times X$$

Comme $Hx \neq \{x\}$ l'ensemble Σ est non vide. Clairement il est stable sous l'action diagonale de G. Donc il est réunion d'orbites de G dans $X \times X \setminus \underbrace{\{(x, x) | x \in X\}}_{\stackrel{\text{def}}{=} \Delta}$. Mais ce n'a que deux orbites O_1 et O_2 dans $X \times X \setminus \Delta$.

1^{er}cas : Supposons que $\Sigma = O_1$. Alors pour tous $y \neq z$, on a

$$\boxed{\begin{array}{c} y \text{ et } z \text{ sont dans la même} \\ \text{partie } gHx \end{array}} \Leftrightarrow \boxed{y \text{ et } z \text{ engendrent un plan hyperbolique.}}$$

Or pour toutes droites distinctes y et z il existe $t \in X$ qui n'est orthogonal ni à y ni à z (car $V = K^{2n}$ n'est pas la réunion des hyperplans $y^\perp$ et $z^\perp$). Mais alors x et t engendrent un plan hyperbolique et t et z engendrent un plan hyperbolique. Donc y et z sont dans la même partie gHx. Comme y et z sont distinctes mais sinon arbitraires cela implique qu'il n'y a qu'une seule orbite O_1.$\frac{1}{4}$

2^e cas : $\Sigma = O_2$. On exclut ce cas de façon similaire. Seule possibilité qui reste : $\Sigma = O_1 \cup O_2$. Alors toutes les droites sont dans une même partie gHx. Comme $x \in Hx$, toutes les droites sont dans Hx. Donc si $g' \in G$ on a ou bien $g'x = x$ et $g' \in G_x \subset H$, ou bien $g'x = hx$ pour un $h \in H$. Mais alors $h^{-1}g'$iG_x et $g' \in hG_x \in H$. Il s'ensuit que $H = G$. □

Remarque 17.11. (cas de la caractéristique 2) : Pour un corps K de caractéristique quelconque, on peut toujours définir $Sp_{2n}(K) = \{U \in Gl_n(K) | {}^tUJ_{2n}U = J_{2n}\}$. Les résultats suivants restent vrais :

- $Sp_2(K) = Sl_2(K)$
- $Sp_{2n}(K) \subseteq Sl_{2n}(K)$
- $\mathcal{Z}(Sp_{2n}(K)) = \{\pm I_{2n}\}$
- la formule pour l'ordre
- pour $n \geq 2$, on a $\mathcal{D}(Sp_{2n}(K)) = Sp_{2n}(K)$
- $PSp_{2n}(K)$ est simple sauf si $n = 2$ et $K = \mathbb{F}_2$: on a $Sp_4(\mathbb{F}_2) = |PSp_4(\mathbb{F}_2) \cong \mathfrak{S}_6$ de roupe dérivé $\mathfrak{A}_6$.

17.6 groupe orthogonal quelques résultats

Soient K un corps de caractéristique $\neq 2$, V un espace vectoriel de dimension finie et q : $V \longrightarrow K$ une forme quadratique non dégénérée.

Proposition 17.12. *a) Le centre de $O(V,q)$ est $\{\pm Id_V\}$ sauf si $K = \mathbb{F}_3$ et V est un plan hyperbolique. Dans ce cas, le centre est d'ordre 4.*

b) Si $\dim \geq 3$*, le centre de $SO(V,q)$ est trivial si* $\dim V$ *est impair et égal à $\{\pm Id_V\}$ si* $\dim V$ *est pair.*

Théorème 17.13. *a) les réflexions engendrent $O(V,q)$.*

b) (Cartan - Dieudonné) Tout élément de $O(V,q)$ est produit de $\leq \dim V$ *réflexions.*

Définition 17.14. soit $P \subseteq V$ un plan tel que $q|_P$ est non dégénérée de façon que $V = P \overset{\perp}{\oplus} P^\perp$. Le renversement par rapport à P est $r_P = (-Id_P) \oplus Id_{P^\perp}$.

Remarque 17.15. On a $r_P \in SO(V,q)$.

Théorème 17.16. *Si* $\dim V \geq 3$*, les renversements engendrent* $SO(V,q)$.