ECOLE POLYTECHNIQUE

Recueil

Modules et groupes finis

Textes de contrôles
des connaissances proposés
les années antérieures

Département de Mathématiques

Promotion 2014
Année 3
Période 1
MAT556

Modules et groupes finis

Textes de contrôles des connaissances proposés les années antérieures

Édition 2016

Examen 2015/2016
MAT556 'Modules et groupes finis'
Anna Cadoret

Avertissement.

Sont autorisés: le polycopié du cours, les notes manuscrites du cours et des exercices traités en cours, les dictionnaires de langues papier.

Les réponses peuvent être rédigées en français ou *en anglais*. L'examen est long; le barême sera adapté en conséquence.

Exercice 1 (Quelques remarques sur les groupes d'ordre 8)

On rappelle que si G est un groupe fini et p un nombre premier, on note $\mathcal{S}_p(G)$ l'ensemble des p-Sylow de G.

(1) Déterminer - à isomorphisme près - tous les groupes abéliens d'ordre 8.

(2) L'objectif de cette question est de déterminer tous les groupes non-abéliens d'ordre 8. Soit G un groupe non-abélien d'ordre 8.

(a) Montrer que $|Z(G)| = 2$ et que $G/Z(G) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$. On notera $z \in Z(G)$ le générateur de $Z(G)$.

(b) Montrer que G contient un élément d'ordre 4 - disons a. Notons $C := \langle a \rangle \subset G$ le sous-groupe engendré par a. Montrez que C est normal dans G et que $a^2 = z$.

(c) D'après (2.b), G est donc une extension de la forme

$$(*) \quad 1 \to C \to G \to \mathbb{Z}/2 \to 1$$

(i) Si $(*)$ se scinde, montrer qu'il n'y a qu'un seule classe d'isomorphisme pour G. Fixons $b \in G \setminus C$ d'ordre 2. On peut écrire

$$G = \{b^i a^j,\ i = 0, 1,\ j = 0, 1, 2, 3\}.$$

En particulier, on doit avoir $b^i a^j b^k a^l = b^{f(i,j,k,l)} a^{g(i,j,k,l)}$. Déterminer les fonctions f, g et lister les éléments de G en fonction de leur ordre.

(ii) Supposons maintenant que $(*)$ ne se scinde pas. Fixons $b \in G \setminus C$. Quel est l'ordre de b? Montrer que $bab^{-1} = za$. En notant $c := ab$, montrer que G est exactement l'ensemble

$$\{1, z, a, b, c, az, bz, cz\}.$$

Construire la table de multiplication de G et lister les éléments de G en fonction de leur ordre.

(3) (Plongement des groupes non-abéliens d'ordre 8 dans un groupe symétrique). On note D_8 et $\mathbb{H}_8$ les groupe construits dans les questions (2.c.i) et (2.c.ii) respectivement.

(a) Montrer que $|\mathcal{S}_2(\mathcal{A}_4)| = 1$ et donner la structure du 2-Sylow V de $\mathcal{A}_4$.

(b) Soit $S \in \mathcal{S}_2(\mathcal{S}_4)$. Expliquer pourquoi $V \subset S$. En déduire la structure des 2-Sylow de $\mathcal{S}_4$.

(c) Peut-on plonger $\mathbb{H}_8$ dans $\mathcal{S}_4$? Déterminer le plus petit entier $n \geq 1$ tel que l'on peut plonger $\mathbb{H}_8$ dans $\mathcal{S}_n$.

Exercice 2 (Table des caractères de $\mathcal{A}_5$)

(1) (Classes de conjugaison)

(a) Montrer que les doubles transpositions (resp. les 3-cycles) sont conjuguées dans $\mathcal{A}_5$.

(b) Montrer qu'il y a deux classes de conjugaison de 5-cycles dans $\mathcal{A}_5$.

(c) Montrer que si $c \in \mathcal{A}_5$ est un 5-cycle alors c et c^2 ne sont pas conjugués mais que c et c^{-1} le sont.

(d) Lister les classes de conjugaison de $\mathcal{A}_5$ et pour chaque classe, donner son cardinal et un représentant.

(e) Déterminer le nombre de représentations irréductibles de $\mathcal{A}_5$.

(2) On considère la représentation de $\mathcal{A}_5$ sur $V = \mathbb{C}^{\oplus 5}$ par permutation des coordonnées. Montrer que

$$V = \mathbb{I} \oplus V_{std},$$

où $\mathbb{I}$ désigne la représentation triviale. Vérifer, en calculant le caractère χ_{std} de V_{std}, que V_{std} est irréductible.

(3) Notons X l'ensemble des parties à deux éléments de $\{1, 2, 3, 4, 5\}$. On considère la représentation de $\mathcal{A}_5$ sur

$$V = \bigoplus_{x \in X} \mathbb{C}x \simeq \mathbb{C}^{\oplus 10}$$

définie par $\sigma \cdot \{x, y\} = \{\sigma(x), \sigma(y)\}$. Vérifer, en calculant le caractère χ_5 de V, que $V = \mathbb{I} \oplus V_{std} \oplus V_5$ et que V_5 est irréductible.

(4) Déterminer les dimensions des représentations irréductibles de $\mathcal{A}_5$.

(5) Compléter la table des caractères de $\mathcal{A}_5$ en exploitant les relations d'orthogonalité (lignes et colonnes).

(6) Notons V l'une des deux représentations irréductibles autre que $\mathbb{I}$, V_{std} et V_5. Déterminer la dimension de la représentation produit tensoriel $V_5 \otimes V$ et sa décomposition en somme directe de sous-représentations irréductibles.

Exercice 3 (Lemme de Brauer-Nesbitt)

Soit k un corps et A une k-algèbre (associative unitaire). Pour tout $a \in A$ et A-module M, on note $a_M \in \mathrm{End}_k(M)$ l'endomorphisme de k-espace vectoriel défini par $a_M(m) = a \cdot m$, $m \in M$. On note également $A'_M := \mathrm{End}_A(M)$, $A''_M := \mathrm{End}_{A'_M}(M)$.
Soit M, N deux A-modules *semisimples* de k-dimension finie. L'objectif de cet exercice est de montrer que les conditions suivantes sont équivalentes:

(i) pour tout $a \in A$, a_M et a_N ont même polynôme caractéristique
(ii) M et N sont isomorphes comme A-modules.

Ecrivons

$$M = \bigoplus_{P \in \widehat{A}} P^{\oplus \mu_P}, \quad N = \bigoplus_{P \in \widehat{A}} P^{\oplus \nu_P}$$

pour les décompositions en somme directe de sous-Amodules simples de M et N (ici, $\widehat{A}$ désigne un système de représentants des classes d'isomorphismes de A-modules simples). Notons également $V := M \oplus N$.

(1) Rappeler pourquoi le morphisme canonique de k-algèbres

$$\begin{array}{ccc} A & \to & A''_V \\ a & \to & a_V \end{array}$$

est bien défini et surjectif.

(2) En déduire que pour tout $P \in \widehat{A}$ il existe $e_P \in A$ tel que $(e_P)_V \in \mathrm{End}_k(V)$ est la projection sur $P^{\oplus \mu_P + \nu_P}$ parallèlement à

$$\bigoplus_{P \neq Q \in \widehat{A}} Q^{\oplus \mu_Q + \nu_Q}.$$

(3) Calculer les polynômes caractéristiques de $(e_P)_M$ et $(e_P)_N$.

(4) Conclure.

(5) On considère l'action du groupe symétrique $\mathcal{S}_n$ sur la k-algèbre des polynômes à n indéterminées $k[X_1, \ldots, X_n]$ définie par $\sigma \cdot P(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$ et on note $k[X_1, \ldots, X_n]^{\mathcal{S}_n} \subset k[X_1, \ldots, X_n]$ la sous-k-algèbre des polynômes symétriques *i.e.* tels que $\sigma \cdot P = P$, $\sigma \in \mathcal{S}_n$. Supposons que k est de *caractéristique* 0. On admettra que les polynômes de Newton:

$$\Sigma_k := \sum_{1 \leq i \leq n} X_i^k, \ k = 1 \ldots, n$$

forment une base de transcendance de la k-algèbre $k[X_1, \ldots, X_n]^{\mathcal{S}_n}$. Cela signifie que pour tout $P \in k[X_1, \ldots, X_n]^{\mathcal{S}_n}$ il existe un unique polynôme $Q_P \in k[T_1, \ldots, T_n]$ vérifiant

$$P = Q_P(\Sigma_1, \ldots, \Sigma_n).$$

En utilisant cela, montrer que les conditions suivantes sont équivalentes:

(i) pour tout $a \in A$, a_M et a_N ont même trace
(ii) M et N sont isomorphes comme A-modules.

ENGLISH VERSION

Exercise 1 (A few remarks about groups of order 8)

We recall that for a finite group G and a prime p we let $\mathcal{S}_p(G)$ denote the set of p-Sylow of G.

(1) List - up to isomorphism - all the abelian groups of order 8.

(2) Let G be a non-abelian group of order 8.

(a) Show that $|Z(G)| = 2$ and that $G/Z(G) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$. Let $z \in Z(G)$ denote the generator of $Z(G)$.

(b) Show that G contains an element of orderc4 - say a. Let $C := \langle a \rangle \subset G$ denote the subgroup generated by a. Show that C is normal in G and that $a^2 = z$.

(c) According to (2.b), G is an extension of the form

$$(*)\ \ 1 \to C \to G \to \mathbb{Z}/2 \to 1$$

(i) If $(*)$ splits, show that G is unique up to isomorphism. Fix $b \in G \setminus C$ of order 2. One can write

$$G = \{b^i a^j,\ i = 0, 1,\ j = 0, 1, 2, 3\}.$$

In particular, one should have $b^i a^j b^k a^l = b^{f(i,j,k,l)} a^{g(i,j,k,l)}$. Determine the maps f, g and list the elements of G according to their order.

(ii) Suppose now that $(*)$ does not split. Fix $b \in G \setminus C$. What is the order of b? Show that $bab^{-1} = za$. Writing $c := ab$, show that G is the set

$$\{1, z, a, b, c, az, bz, cz\}.$$

Construct the multiplication table of G and list the elements of G according to their order.

(3) (Embedding non-abelian groups of order 8 into a symmetric group). Let D_8 and $\mathbb{H}_8$ denote the groups constructed in questions (2.c.i) et (2.c.ii) respectively.

(a) Show that $|\mathcal{S}_2(\mathcal{A}_4)| = 1$ and give the structure of the 2-Sylow V of $\mathcal{A}_4$.

(b) Let $S \in \mathcal{S}_2(\mathcal{S}_4)$. Explain why $V \subset S$. Deduce from this the isomorphism class of the 2-Sylow of $\mathcal{S}_4$.

(c) Can we embed $\mathbb{H}_8$ in $\mathcal{S}_4$? Determine the smallest integer $n \geq 1$ such that $\mathbb{H}_8$ can be embedded into $\mathcal{S}_n$.

Exercise 2 (Character table of $\mathcal{A}_5$)

(1) (Conjugacy classes)

(a) Show that the double transpositions (resp. the 3-cycles) are conjuguated in $\mathcal{A}_5$.

(b) Show that there exists two conjugacy classes of 5-cycles in $\mathcal{A}_5$.

(c) Show that if $c \in \mathcal{A}_5$ is a 5-cycle then c and c^2 are not conjugated but c and c^{-1} are.

(d) Give the list of conjugacy classes in $\mathcal{A}_5$ and for each class, give its cardinality and a representative.

(e) Give the number of irreducible representations of $\mathcal{A}_5$.

(2) Consider the representation $V = \mathbb{C}^{\oplus 5}$ of $\mathcal{A}_5$ by permutation of the coordinates. Show that

$$V = \mathbb{I} \oplus V_{std},$$

where $\mathbb{I}$ denotes the trivial representation. Compute the character χ_{std} of V_{std} and check that V_{std} is irreducible.

(3) Let X denote the set of (unordered) pairs in $\{1, 2, 3, 4, 5\}$ and consider the representation of $\mathcal{A}_5$ on

$$V = \bigoplus_{x \in X} \mathbb{C}x \simeq \mathbb{C}^{\oplus 10}$$

defined by $\sigma \cdot \{x, y\} = \{\sigma(x), \sigma(y)\}$. Compute the character χ_5 of V and check that $V = \mathbb{I} \oplus V_{std} \oplus V_5$ with V_5 irreducible.

(4) Give the dimensions of the irreducible representations of $\mathcal{A}_5$.

(5) Using the orthogonality relations (lines and columns), complete the character table of $\mathcal{A}_5$.

(6) Let V denote one of the two irreducible representations other than $\mathbb{I}$, V_{std} and V_5. Give the dimension of the tensor product representation $V_5 \otimes V$ as well as its decomposition into direct sum of irreducible subrepresentations.

Exercise 3 (Brauer-Nesbitt Lemma)

Let k be a field and A a k-algebra (associative, with unit). For every $a \in A$ and A-module M, let $a_M \in \mathrm{End}_k(M)$ denote the endomorphism of k-vector space defined by $a_M(m) = a \cdot m$, $m \in M$. Set also $A'_M := \mathrm{End}_A(M)$, $A''_M := \mathrm{End}_{A'_M}(M)$.
Let M, N be two A-modules *semisimples* of finie k-dimension. The aim of this exercise is two show that the following two conditions are equivalent.

(i) for every $a \in A$, a_M and a_N have the same characteristic polynomial
(ii) M and N are isomorphic as A-modules.

Write

$$M = \bigoplus_{P \in \widehat{A}} P^{\oplus \mu_P}, \quad N = \bigoplus_{P \in \widehat{A}} P^{\oplus \nu_P}$$

for the decompositions into direct sum of simple A-submodules of M and N (here, $\widehat{A}$ denotes as usual a system of representatives of the isomorphism classes of simple A-modules). Set also $V := M \oplus N$.

(1) Recall why the canonical morphism of k-algebras

$$\begin{array}{ccc} A & \to & A''_V \\ a & \to & a_V \end{array}$$

is well-defined and surjective.

(2) Deduce from (1) that for every $P \in \widehat{A}$ there exists $e_P \in A$ such that $(e_P)_V \in \mathrm{End}_k(V)$ is the projection onto $P^{\oplus \mu_P + \nu_P}$ with respect to the direct sum decomposition

$$V = (P^{\oplus \mu_P + \nu_P}) \bigoplus (\bigoplus_{P \neq Q \in \widehat{A}} Q^{\oplus \mu_Q + \nu_Q}).$$

(3) Compute the characteristic polynomials of $(e_P)_M$ and $(e_P)_N$.

(4) Conclude.

(5) Consider the action of the symmetric group $\mathcal{S}_n$ on the k-algebra $k[X_1, \ldots, X_n]$ of polynomial with n indeterminates defined by $\sigma \cdot P(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$ and write $k[X_1, \ldots, X_n]^{\mathcal{S}_n} \subset k[X_1, \ldots, X_n]$ for the k-subalgebra of symmetric polynomials *i.e.* those satisfying $\sigma \cdot P = P$, $\sigma \in \mathcal{S}_n$. Assume k has *caracteristic* 0. We will admit that the Newton polynomials:

$$\Sigma_k := \sum_{1 \leq i \leq n} X_i^k, \ k = 1 \ldots, n$$

are a transcdence basis for the k-algebra $k[X_1, \ldots, X_n]^{\mathcal{S}_n}$. This means that for every $P \in k[X_1, \ldots, X_n]^{\mathcal{S}_n}$ there exists a unique polynomial $Q_P \in k[T_1, \ldots, T_n]$ such that

$$P = Q_P(\Sigma_1, \ldots, \Sigma_n).$$

Using this result, show that the following two conditions are equivalent.

(i) for every $a \in A$, a_M and a_N have the same trace
(ii) M and N are isomorphic as A-modules.

anna.cadoret@polytechnique.edu
Centre de Mathématiques Laurent Schwartz - Ecole Polytechnique,
91128 PALAISEAU, FRANCE.

Examen 2015/2016 - Correction
MAT556 'Modules et groupes finis'
Anna Cadoret

Exercice 1 (Quelques remarques sur les groupes d'ordre 8)

(1) Par le théorème de structure, il n'y a à isomorphisme près que 3 groupes abéliens d'ordre 8:

$$\mathbb{Z}/8,\ \mathbb{Z}/2\times\mathbb{Z}/4,\ \ \mathbb{Z}/2\times\mathbb{Z}/2\times\mathbb{Z}/2.$$

(2) (a) On sait que $|Z(G)||8$, $|Z(G)|<8$ (G n'est pas commutatif), $|Z(G)|\geq 2$ (G 2-groupe) et $|Z(G)|\neq 4$ ($G/Z(G)$ ne peut être cyclique)... Il ne reste donc que $|Z(G)|=2$. Comme $G/Z(G)$ est d'ordre 4 non cyclique, c'est forcément $\mathbb{Z}/2\times\mathbb{Z}/2$.

(b) G contient au moins un élément d'ordre 4 sinon tous ses éléments seraient d'ordre 1 ou 2 donc G serait abélien ($ab=(ab^{-1}=b^{-1}a^{-1}=ba)$). Notons a un élément d'ordre 4 et $C:=\langle a\rangle\subset G$ le sous-groupe engendré par a. Comme C est d'indice 2, il est normal dans G. Si $a^2\neq z$ on aurait $Z(G)\cap C=1$ donc $G=Z(G)\times C$ serait un produit direct (car $Z(G)$ et C sont tous deux normaux dans G) de deux groupes abéliens donc abélien.

(c) D'après (2.b), G est donc une extension de la forme

$$(*)\ \ 1\to C\to G\to\mathbb{Z}/2\to 1$$

(i) Si $(*)$ se scinde, la structure de produit semi-direct est déterminée par un morphisme de groupes

$$\phi:\mathbb{Z}/2\to \mathrm{Aut}_{Grp}(C)\simeq(\mathbb{Z}/4)^\times=\{Id,-Id\}.$$

il n'y a donc que deux possibilités: $\phi=Id$, correspondant au produit direct, qui serait abélien donc exclu et $\phi:1\to -Id$, qui correspond à un produit semidirect non-abélien. Fixons $b\in G\setminus C$ d'ordre 2. On a la règle

$$bab=bab^{-1}b=\phi(b)(a)=a^{-1}.$$

D'où $b^ia^jb^ka^l=b^ia^{j+l}$ si $k=0$ et $b^ia^jb^ka^l=b^{i+1}a^{l-j}$ si $k=1$. Enfin, on peut classer les éléments de G en fonction de leur ordre:
- Ordre 1: 1;
- Ordre 2: ba^i, $i=0,\dots,3$, a^2 (5 éléments);
- Ordre 4: a,a^3 (2 éléments).

(ii) Supposons maintenant que $(*)$ ne se scinde pas. Fixons $b\in G\setminus C$. Si b était d'ordre 2, $1\to b$ fournirait un scindage de $(*)$ donc b est forcément d'ordre 4. Comme bab^{-1} et a ont la même image par $p_{Z(G)}:G\twoheadrightarrow G/Z(G)$, on a $bab^{-1}\in\{a,za\}$. Mais on ne peut pas avoir $bab^{-1}=a$. Sinon a et b cpmmuteraient or, comme ils enegendrent G, cela imposerait à G d'être abélien. On a

$$G=p^{-1}(0)\sqcup p^{-1}(1)=C\sqcup Cb$$

et, en notant $c:=ab$, on a

$$p^{-1}(0)=C=\{1,z,a,az\}$$

et

$$p^{-1}(1)=Cb=\{b,zb,c,zc\}.$$

Avec ces notations, on peut construire la table de multiplication de G.

	1	z	a	za	b	zb	c	zc
1	1	z	a	za	b	zb	c	zc
z	z	1	za	a	zb	b	zc	c
a	a	za	z	1	c	zc	zb	b
za	za	a	1	z	zc	c	b	zb
b	b	zb	zc	c	z	1	a	za
zb	zb	b	c	zc	1	z	za	a
c	c	zc	b	zb	za	a	z	1
zc	zc	c	zb	b	a	za	1	z

Enfin, on peut classer les éléments de G en fonction de leur ordre:
- Ordre 1: 1;
- Ordre 2: z (1 éléments);
- Ordre 4: a, za, b, zb, c, zc (6 éléments).

(3) (2-Sylow de $\mathcal{S}_4$)

(a) Soit V un 2-Sylow de $\mathcal{A}_4$. On a $|V| = 4$. Par ailleurs, $\mathcal{A}_4$ ne contient que 4 éléments d'ordre une puissance de 2: Id et l'ensemble $C_{2,2}$ des doubles transpositions. Donc, nécessairement $V = \{Id, C_{2,2}\}$. En particulier, l'ensemble $\{Id, C_{2,2}\}$ est un groupe et $|\mathcal{S}_2(\mathcal{A}_4)| = 1$ et S est normal dans $\mathcal{A}_4$. Comme tous les éléments de V sont d'ordre 1, 2 on a forcément $V = \mathbb{Z}/2 \times \mathbb{Z}/2$.

(b) On notera que V est normal dans $\mathcal{S}_4$. Par ailleurs, V est un 2-groupe donc il existe $S \in \mathcal{S}_2(\mathcal{S}_4)$ tel que $V \subset S$. Mais alors, pour tout $\sigma \in \mathcal{S}_4$ on a

$$V = \sigma V \sigma^{-1} \subset \sigma S \sigma^{-1}.$$

Comme les 2-Sylow de $\mathcal{S}_4$ sont tous conjugués, cela montre bien que V est contenu dans tous les 2-Sylow de $\mathcal{S}_4$. Donc les 2-Sylow de $\mathcal{S}_4$ - étant d'ordre 8 et contenant V sont engendrés par un 4-cycle et V. En particulier, ils sont non abéliens et contiennent 3 éléments d'ordre exactement 2; il s'agit donc de groupes isomorphes à D_8.

(c) On ne peut plonger $\mathbb{H}_8$ dans $\mathcal{S}_4$ sinon on aurait $\mathbb{H}_8$ isomorphe à D_8. Par contre, en faisant agir $\mathbb{H}_8$ par translation à gauche sur lui-même, on peut toujours le plonger dans $\mathcal{S}(\mathbb{H}_8) \simeq \mathcal{S}_8$. Reste à savoir si l'on peut plonger $\mathbb{H}_8$ dans $\mathcal{S}_n$ pour $n = 5, 6, 7$. Cela revient à déterminer si pour $n = 5, 6, 7$ les 2-Sylow de $\mathcal{S}_n$ contiennent un sous-groupe isomorphe à $\mathbb{H}_8$. En observant que

$$\mathcal{S}_n \simeq \mathrm{Stab}_{\mathcal{S}_{n+1}}(n+1) \subset \mathcal{S}_{n+1},$$

on voit que les 2-Sylow de $\mathcal{S}_n$ s'injectent dans ceux de $\mathcal{S}_{n+1}$. En particulier, les 2-Sylow de $\mathcal{S}_5$ sont encore isomorphes à D_8 et ceux de $\mathcal{S}_7$ sont isomorphes à ceux de $\mathcal{S}_6$. Enfin, les 2-Sylow de $\mathcal{S}_6$ sont d'ordre 16. Or on peut facilement exhiber un sous-groupe de $\mathcal{S}_6$ d'ordre 16 sous la forme

$$D_8 \times \mathbb{Z}/2$$

En prenant pour copie de D_8 le 2-Sylow de $\mathrm{Stab}_{\mathcal{S}_6}(\{1, 2, 3, 4\}) \simeq \mathcal{S}_4$ et pour copie de $\mathbb{Z}/2$ le sous-groupe engendré par la permutation $(5, 6)$. Donc les 2-Sylow de $\mathcal{S}_6$ ne contient que 4 éléments d'ordre 4: $(c, 1)$, (c, τ), $(c^3, 1)$, (c^3, τ) où c est un élément d'ordre 4 dans D_8 et τ un élément d'ordre 2 dans $\mathbb{Z}/2$. Ils ne peuvent donc contenir $\mathbb{H}_8$ qui, lui, contient 6 éléments d'ordre 4.

Exercice 2 (table des caractères de $\mathcal{A}_5$)

(1) (Classes de conjugaison)

(a) On sait que les doubles transpositions (resp. les 3-cycles) sont conjuguées dans $\mathcal{S}_5$ donc si σ, σ' sont deux doubles transpositions (resp. les 3-cycles) on peut toujours trouver $\tau \in \mathcal{S}_5$ tel que $\sigma' = \tau\sigma\tau^{-1}$. Si $\tau \in \mathcal{A}_5$, il n'y a rien à faire. Sinon, on peut essayer de modifier τ en le composant avec une permutation $c \in \mathcal{S}_5 \setminus \mathcal{A}_5$ qui centralise σ.
- Si $\sigma = c_1 \circ c_2$ avec c_1, c_2 deux transpositions à supports disjoints, on peut prendre $c = c_1$ par exemple;
- Si σ est un 3-cycle, on peut prendre pour c la transposition dont le support est disjoint de celui de σ.

(b) L'argument de la question précédente ne marche plus pour les 5-cycles dans $\mathcal{A}_5$. Il dit cependant qu'il y a au plus deux classes de conjugaison de 5-cycles. On sait qu'il y a $4! = 24$ 5-cycles dans $\mathcal{A}_5$. Comme les 5-cycles sont conjugués dans $\mathcal{S}_5$, on voit que le cardinal du centralisateur $C_{\mathcal{S}_5}(c)$ d'un 5-cycle c dans $\mathcal{S}_5$ est $\frac{120}{24} = 5$ donc est réduit à $\langle c\rangle$. Comme $C_{\mathcal{A}_5}(c) = C_{\mathcal{S}_5}(c) \cap \mathcal{A}_5 = \langle c\rangle$, on en déduit que la classe de conjugaison de c dans $\mathcal{A}_5$ est de cardinal $\frac{60}{5} = 12$. Il y a donc exactement deux classes de conjugaison de 5-cycles dans $\mathcal{A}_5$: celle des éléments de la forme $\sigma c\sigma^{-1}$ avec $\sigma \in \mathcal{A}_5$ et celle des éléments de la forme $\sigma c\sigma^{-1}$ avec $\sigma \in \mathcal{S}_5 \setminus \mathcal{A}_5$. En effet, si c est un 5-cycle et $\sigma \in \mathcal{S}_5 \setminus \mathcal{A}_5$, c et $\sigma c\sigma^{-1}$ ne peuvent être conjugués dans $\mathcal{A}_5$ sinon il existerait $\tau \in \mathcal{A}_5$ tel que $\tau^{-1}\sigma \in C_{\mathcal{A}_5}(c) = \langle c\rangle$: une contradiction.

(c) Prenons par exemple $c = (1,2,3,4,5)$. On a donc $c^2 = (1,3,5,2,4)$ et en utilisant la formule $\sigma(1,2,3,4,5)\sigma^{-1} = (\sigma(1),\sigma(2),\sigma(3),\sigma(4),\sigma(5))$, on en déduit que c et c^2 sont conjugués par $(2,4,5,3) \in \mathcal{S}_5 \setminus \mathcal{A}_5$. Ils ne sont donc pas dans la même classe de conjugaison de $\mathcal{A}_5$. De même $c^{-1} = (1,5,4,3,2)$ est conjugué à c par $(2,5)(3,4) \in \mathcal{A}_5$.

(d) - C_1, 1, $|C_1| = 1$;
- $C_{2,2}$, $(1,2)(3,4)$, $|C_{2,2}| = 15$;
- C_3, $(1,2,3)$, $|C_3| = 20$;
- C_5^1, $(1,2,3,4,5)$, $|C_5^1| = 12$;
- C_5^2, $(1,3,5,2,4)$, $|C_5^2| = 12$.

(e) $|\widehat{\mathcal{A}_5}| = |Cl(\mathcal{A}_5)| = 5$.

(f) On fait agir $\mathcal{A}_5$ sur $V := \oplus_{1\leq i\leq 5}\mathbb{C}e_i$ par $\sigma \cdot e_i = e_{\sigma(i)}$. L'application $\mathbb{C}$-linéaire

$$\epsilon : V \to \mathbb{I},\ \sum_{1\leq i\leq 5} x_i e_i \to \sum_{1\leq i\leq 5} x_i$$

est un morphisme de $\mathbb{C}[\mathcal{A}_5]$-modules, donc $V_{std} := \ker(\epsilon) \subset V$ est un sous-$\mathbb{C}[\mathcal{A}_5]$-module et comme $\mathbb{C}[\mathcal{A}_5]$ est semisimple, on a

$$V = \mathbb{I} \oplus V_{std}.$$

En particulier, pour $\sigma \in \mathcal{A}_5$ on a

$$\chi_{std}(\sigma) = \chi_V(\sigma) - \chi_{\mathbb{I}}(\sigma) = |\{1,\dots,5\}^\sigma| - 1,$$

où $\{1,\dots,5\}^\sigma$ est l'ensemble des points fixes de σ. On a donc:

$$\chi_{std}(C_1) = 4,\ \chi_{std}(C_{2,2}) = 0,\ \chi_{std}(C_3) = 1,\ \chi_{std}(C_5^1) = \chi_{std}(C_5^2) = -1.$$

Et

$$(\chi_{std},\chi_{std})_{\mathcal{A}_5} = \frac{1}{60}(4^2 + 15\times 0 + 20\times 1 + 12\times 1 + 12\times 1) = 1,$$

ce qui montre que V_{std} est irréductible.

(g) Notons X l'ensemble des parties à deux éléments de $\{1,2,3,4,5\}$. On considère la représentation de $\mathcal{A}_5$ sur

$$V = \bigoplus_{x\in X} \mathbb{C}x \simeq \mathbb{C}^{\oplus 10}$$

définie par $\sigma \cdot \{x,y\} = \{\sigma(x),\sigma(y)\}$. Par construction, on a

$$\chi_V(\sigma) = |X^\sigma|$$

soit

$$\chi(C_1) = 10,\ \chi(C_{2,2}) = 2,\ \chi(C_3) = 1,\ \chi(C_5^1) = \chi_{std}(C_5^2) = 0.$$

On a également

$$(\chi_V,\chi_{\mathbb{I}})_{\mathcal{A}_5} = \frac{1}{60}(10 + 15\times 2 + 20\times 1) = 1,\ (\chi_V,\chi_{std})_{\mathcal{A}_5} = \frac{1}{60}(10\times 4 + 20\times 1) = 1.$$

Comme $\mathbb{C}[\mathcal{A}_5]$ est semisimple, on en déduit que V se décompose comme $\mathbb{C}[\mathcal{A}_5]$-module sous la forme

$$V = \mathbb{I} \oplus V_{std} \oplus V_5,$$

où V_5 est de dimension 5 et $\chi_{V_5} = \chi_V - \chi_{\mathbb{I}} - \chi_{std}$ soit

$$\chi(C_1) = 5,\ \chi(C_{2,2}) = 1,\ \chi(C_3) = -1,\ \chi(C_5^1) = \chi_{std}(C_5^2) = 0.$$

On a donc

$$(\chi_5,\chi_5)_{\mathcal{A}_5}=\frac{1}{60}(5^2+15\times 1+20\times 1+12\times 0+12\times 0)=1,$$

ce qui montre que V_5 est irréductible.

(h) On a $60=|\mathcal{A}_5|=n_1^2+n_{std}^2+n_5^2+a^2+b^2=1+4^2+5^2+a^2+b^2$ donc $18=a^2+b^2$. La seule possibilité est $a=b=3$. Il reste donc 2 représentations irréductibles de dimension 3.

(i) On a déjà

	C_1	$C_{2,2}$	C_3	C_5^1	C_5^2
$\chi_{\mathbb{I}}$	1	1	1	1	1
χ_{std}	4	0	1	-1	-1
χ_5	5	1	-1	0	0
χ_3^1	3	$a=-1$	$b=0$	$c=\frac{1-\sqrt{5}}{2}$	$d=\frac{1+\sqrt{5}}{2}$
χ_3^2	3	$e=-1$	$f=0$	$g=\frac{1+\sqrt{5}}{2}$	$h=\frac{1-\sqrt{5}}{2}$

Et on peut compléter en utilisant l'orthogonalité selon les lignes et les colonnes.

- L'orthogonalité de la 1ère et 2ème colonne donne: $a+e=-2$. Par ailleurs, on sait que a et e sont somme de 3 racines carrée de 1, donc ne peuvent valoir que $-3,-1,1,3$. D'un autre coté, orthogonalité de la 2ème colonne avec elle-même donne $a^2+e^2=2$. Donc on a forcément $a=b=-1$.
- L'orthogonalité de la 3ème colonne avec elle-même donne $b^2+f^2=0$. Donc on a forcément $b=f=0$.
- L'orthogonalité de la 1ère et 4ème (resp. 5ème) ligne donne $c+d=1$ (resp. $g+h=1$) et l'orthogonalité de la 4ème (resp. 5ème) ligne avec elle-même donne $c^2+d^2=3$ (resp. $g^2+h^2=3$). Donc $c^2-c-1=0$ (resp. $g^2-g-1=0$). On en déduit $c=\frac{1-\sqrt{5}}{2}$, $d=\frac{1+\sqrt{5}}{2}$ puis $g=\frac{+\sqrt{5}}{2}$, $h=\frac{1-\sqrt{5}}{2}$.

(j) En utilisant que $\chi_{V_5\otimes V_3^2}=\chi_5\chi_3^2$ et en calculant $(\chi_5\chi_3^2,\chi)_{\mathcal{A}_5}$ pour $\chi\in\widehat{\mathcal{A}_5}$, on obtient

$$V_5\otimes V_3^2=V_{std}\oplus V_5\oplus V_3^1\oplus V_3^2.$$

Exercice 3 (Lemme de Brauer-Nesbitt)

(1) C'est l'exercice 3.1.4 du cours. On rappelle l'argument. Soit $f\in A_V''$. Montrons d'abord que pour tout $v\in V$ il existe $a\in A$ tel que $f(v)=av$. Comme V est semi-simple, il existe un sous-A-module $W\subset V$ tel que $V=Av\oplus W$. Notons $\pi:V\twoheadrightarrow Av$ la projection sur Av parallèlement à W; c'est un morphisme de A-modules. Et

$$V\overset{\pi}{\twoheadrightarrow}Av\hookrightarrow V\in A_V'$$

donc $f\circ\pi=\pi\circ f$. En particulier, $f(v)=f(\pi(v))=\pi(f(v))\in Av$. On applique ensuite ce qui précèdeà $V^{\oplus r}$ et $f^{\oplus r}:V^{\oplus r}\to V^{\oplus r}$, $(v_1,\dots,v_r)\to(f(v_1),\dots,f(v_r))$ pour en déduire qu'il existe $a\in A$ tel que $f(v_i)=av_i$, $i=1,\dots,r$. On conclut en invoquant que V est un A-module de type fini.

(2) D'après la question (1), il suffit de montrer que la projection $p:V\to P^{\oplus\mu_P+\nu_P}$ parallèlement à

$$\bigoplus_{P\neq Q\in\widehat{A}}Q^{\oplus\mu_Q+\nu_Q}$$

est dans A_V'', *i.e.* que pour tout $f\in A_V'$ on a $pf=fp$. Mais si $f\in A_V'$, par le lemme de Schur, on a $f(Q^{\oplus\mu_Q+\nu_Q})\subset Q^{\oplus\mu_Q+\nu_Q}$. Notons $f_Q:Q^{\oplus\mu_Q+\nu_Q}\to Q^{\oplus\mu_Q+\nu_Q}$ la restriction de f à $Q^{\oplus\mu_Q+\nu_Q}$. Alors pour tout $v=\sum_{Q\in\widehat{A}}v_Q\in V=\oplus_{Q\in\widehat{A}}Q^{\oplus\mu_Q+\nu_Q}$ on a

$$f(v)=\sum_{Q\in\widehat{A}}f_Q(v_Q)$$

donc $pf(v)=f_P(v_P)$ et $fp(v)=f(v_P)=f_P(v_P)$.

(3) Par définition, $(e_P)_M$ (resp. $(e_P)_N$) est la projection sur $P^{\oplus \mu_P}$ parallèlement à $\oplus_{P\neq Q\in \widehat{A}} Q^{\oplus \mu_Q}$ (resp. $P^{\oplus \nu_P}$ parallèlement à $\bigoplus_{P\neq Q\in \widehat{A}} Q^{\oplus \nu_Q}$). Son polynôme caractéristique est donc $\chi_{P,M} = (T-1)^{p\mu_P} T^{m-p\mu_P}$ (resp. $\chi_{P,N} = (T-1)^{p\nu_P} T^{n-d_P\nu_P}$), où p, m, n sont les k-dimensions de P, M et N respectivement.

(4) $\chi_{P,M} = \chi_{P,N}$ pour tout $P \in \widehat{A}$ si et seulement si $\mu_P = \nu_P$ pour tout $P \in \widehat{A}$, ce qui équivaut à $M \simeq N$.

(5) D'après ce qui précède, la question revient à montrer que les conditions suivantes sont équivalentes:

(i) pour tout $a \in A$, a_M et a_N ont même trace
(i') pour tout $a \in A$, a_M et a_N ont même polynôme caractéristique.

Déjà (i') $\Rightarrow$ (i). Pour l'implication inverse, notons $\chi_{a_M} := \prod_{1\leq i\leq n}(T-\mu_i)$ et $\chi_{a_N} := \prod_{1\leq i\leq n}(T-\nu_i)$ les polynômes caractéristiques de a_M et a_N vus dans $\overline{k}[T]$. En les développant, on obtient

$$\chi_{a_M} = T^n + \sum_{1\leq i\leq n} \sigma_n^i(\mu_1,\dots,\mu_n)T^{n-i},\ \chi_{a_N} = T^n + \sum_{1\leq i\leq n} \sigma_n^i(\nu_1,\dots,\nu_n)T^{n-i},$$

avec $\sigma_n^i(X_1,\dots,X_n) \in k[X_1,\dots,X_n]^{\mathcal{S}_n}$, $i=1,\dots,n$. Par le théorème de structure de $k[X_1,\dots,X_n]^{\mathcal{S}_n}$ donné dans l'énoncé on peut donc écrire

$$\sigma_n^i(X_1,\dots,X_n) = Q_i(\Sigma_1(X_1,\dots,X_n),\dots,\Sigma_n(X_1,\dots,X_n))$$

pour des polynômes $Q_1,\dots,Q_n \in k[U_1,\dots,U_n]$ Mais comme

$$\Sigma_r(\mu_1,\dots,\mu_n) = \sum_{1\leq i\leq n} \mu_i^r = Tr(a_M^r) = Tr(a_N^r) = \sum_{1\leq i\leq d} \nu_i^r = \Sigma_r(\nu_1,\dots,\nu_n),\ r\geq 0,$$

on en déduit

$$\sigma_n^i(\mu_1,\dots,\mu_n) = \sigma_n^i(\nu_1,\dots,\nu_n),\ i=1,\dots,n$$

soit $\chi_{a_M} = \chi_{a_N}$.

anna.cadoret@polytechnique.edu
Centre de Mathématiques Laurent Schwartz - Ecole Polytechnique,
91128 PALAISEAU, FRANCE.

Examen 2014/2015
MAT556 'Modules et groupes finis'
Anna Cadoret

Avertissement.

Sont autorisés: le polycopié du cours, les notes manuscrites du cours et des exercices traités en cours, les dictionnaires de langues papier.

Les réponses peuvent être rédigées en français ou *en anglais*.

Les deux exercices et le problème sont indépendants. Le problème porte sur la théorie des représentations des groupes finis et utilise les techniques standard vues au chapite 3. Ll'exercice 1 discute le problème de la semisimplicité des $k[G]$-modules lorsque la caractéristique de k divise l'ordre de G et est donc plutôt à rattacher au chapitre 1. L'exercice 2 donne deux applications élémentaires de la théorie des Sylow à l'étude de la (non-)simplicité des groupes finis. Chacun des deux exercices est divisé en deux parties indépendantes.

Le sujet est peut-être long. Le barême sera adapté en conséquence.

Exercice 1 ('transfert' de semisimplicité) Soit A un anneau associatif unitaire. On a vu en cours que tout sous-A-module et tout A-module quotient d'un A-module semisimple était encore un A-module semisimple. Donc la semisimplicité se transfère aux sous-A-modules et aux A-modules quotients. Pour d'autres types de construction, en général, les choses sont assez compliquées même si on peut quand-même parfois faire des observations intéressantes. Voici deux exemples dans le cas où $A = k[G]$ avec G un groupe fini et k un corps de caractéristique $p > 0$ *divisant* l'ordre de G.

(1) Transferts aux sous-groupes normaux: Soit $N \subset G$ un sous-groupe normal et V un $k[G]$-module de k-dimension finie.
   (a) Expliquer pourquoi V contient toujours un sous-$k[G]$-module simple.
   (b) Montrer que si V est semisimple comme $k[G]$-module alors il est semisimple comme $k[N]$-module. On observera qu'il suffit de traiter le cas où V est un $k[G]$-module simple et on pourra essayer de montrer que dans ce cas, V est somme de sous-$k[N]$-modules simples.
   (c) Montrer que la réciproque est vraie si p ne divise pas $[G : N]$. (Indication: penser à la preuve de la semisimplicité de $k[G]$ lorsque la caractéristique de k est 0 ou ne divise pas $|G|$).

(2) Transfert au produit tensoriel: Supposons $p = 2$, k fini et $G = SL_2(k) \subset GL_2(k)$ le groupe des matrices 2×2 inversibles sur k de déterminant 1. On note $V(d)$ le k-espace vectoriel des polynomes homogènes de degré d en X, Y sur k. C'est donc un k-espace vectoriel de k-base $X^i Y^{d-i}$, $i = 0, \dots, d$ et de k-dimension $d + 1$. On munit $V(d)$ de la structure de $k[G]$-module induite par

$$\begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} X = aX + bY, \ \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} Y = cX + dY.$$

   (a) Montrer que $V(1)$ est un $k[G]$-module simple.
   (b) Montrer que $V'(2) = kX^2 \oplus kY^2$ est un sous-$k[G]$-module de $V(2)$.

(c) Montrer que $V(2)/V'(2) \simeq k$ est le $k[G]$-module trivial. En déduire que si $|k| \geq 4$ la suite exacte courte de $k[G]$-modules

$$0 \to V'(2) \to V(2) \to V(2)/V'(2) \to 0$$

n'est pas scindée. En particulier, $V(2)$ n'est pas un $k[G]$-module semisimple.

(d) Construire un morphisme surjectif (naturel) de $k[G]$-modules

$$V(1) \otimes_k V(1) \twoheadrightarrow V(2).$$

(e) Déduire de ce qui précède que $V(1) \otimes_k V(1)$ n'est pas un $k[G]$-module semisimple.

Remarque: La construction ci-dessus s'étend à un corps k fini de caractéristique $p > 0$ comme suit: $V(d)$ est un $k[G]$-module simple si $d < p$, $V'(p) = kX^p \oplus kY^p \subset V(p)$ est un sous-$k[G]$-module, $V(p)/V'(p) \simeq V(p-2)$ mais sauf si $k = \mathbb{F}_2$, la suite exacte courte de $k[G]$-modules

$$0 \to V'(p) \to V(p) \to V(p)/V'(p) \to 0$$

n'est jamais scindée. Par contre, on a toujours des morphismes surjectifs de $k[G]$-modules

$$V(d_1) \otimes_k \cdots \otimes_k V(d_m) \twoheadrightarrow V(p)$$

pour $1 \leq d_i \leq p-1$ tels que $d_1 + \cdots + d_m = p$. En fait, Serre a montré (Inventiones Math. 116, p. 513-530, 1994) que si $V_1, \ldots V_m$ sont des $k[G]$-modules semisimples tels que $\sum_{1 \leq i \leq m} dim_k(V_i) < p$ alors $V_1 \otimes_k \cdots \otimes_k V_m$ est encore un $k[G]$-module semisimple.

Exercice 2 (simplicité et Sylow) Soit G un groupe fini. Si X est un ensemble fini, on note $\mathcal{S}(X)$ le groupe des permutations de X et $\mathcal{A}(X) \subset \mathcal{S}(X)$ le sous-groupe alterné (*i.e.* le groupe des permutations paires).

(1) (Simplicité et 2-Sylow)

(a) En utilisant le morphisme injectif de G induit par l'action à gauche de G sur lui-même par translation

$$\begin{array}{rccc} L: & G & \hookrightarrow & \mathcal{S}(G) \\ & g & \to & h \to gh \end{array}$$

montrer que, si G est simple distinct de $\mathbb{Z}/2$ alors $L(G) \subset \mathcal{A}(G)$.

(b) En déduire que, si G est simple distinct de $\mathbb{Z}/2$ alors les 2-Sylow de G ne peuvent être cycliques.

(c) Vérifier que pour $n \geq 5$, les 2-Sylow du groupe alterné $\mathcal{A}_n$ ne sont pas cycliques. Sont-ils abéliens?

(d) Montrer qu'un groupe G d'ordre pair tel que $\frac{|G|}{2}$ est impair n'est jamais simple.

(2) (Simplicité et nombre de p-Sylow)

(a) Supposons G simple non abélien. Soit p un nombre premier divisant l'ordre de G et s_p le nombre de p-Sylow de G. Montrer que $|G|$ divise $s_p!$.

(b) Montrer qu'un groupe d'ordre 10000000 ne peut pas être simple.

Problème (caractères irréductibles des groupes non abéliens d'ordre pq)

Soit $p \neq q$ deux nombres premiers distincts avec $p < q$. Soit G un groupe non abélien d'ordre pq.

(1) Rappeler rapidement pourquoi, à isomorphisme près, il y a au plus un groupe non abélien G d'ordre pq - que l'on notera donc $G_{p,q}$ dans la suite - et rappeler quelle est sa structure.

Dans la suite, pour fixer les notations, on se donnera $z_p \in G_{p,q}$ un élément d'ordre p, $z_q \in G_{p,q}$ un élément d'ordre q et on posera $C_p := \langle z_p \rangle$, $C_q := \langle z_q \rangle$.

(2) Déterminer le groupe dérivé et l'abélianisé de $G_{p,q}$; en déduire les représentations de dimensions 1 de $G_{p,q}$.
(3) Calculer le nombre et la dimension des représentations irréductibles de $G_{p,q}$.
(4) L'objectif de cette question est de déterminer les classes de conjugaison de $G_{p,q}$.
   (a) Déterminer le nombre de classes de conjugaison de $G_{p,q}$.
   (b) Expliquer pourquoi les éléments z_p^k, $k = 0, \ldots, p-1$ sont deux à deux non conjugués. Déterminer le cardinal de leurs classes de conjugaison.
   (c) Montrer que C_q est réunion disjointe de classes de conjugaison de $G_{p,q}$. Montrer que l'action par conjugaison de $G_{p,q}$ sur C_q se factorise *via* $G_{p,q} \twoheadrightarrow G_{p,q}/C_q \simeq C_p$. En déduire que C_q est réunion disjointe de $1 + \frac{q-1}{p}$ classes de conjugaison dont on déterminera le cardinal.
   (d) Conclure.
(5) On considère l'action de C_p sur $\widehat{C}_q$ définie par

$$\begin{array}{lll} C_p \times \widehat{C}_q & \to & \widehat{C}_q \\ (z, \chi) & \to & z \cdot \chi = \chi(z^{-1} - z). \end{array}$$

   Déterminer le nombre d'orbites.
(6) Soit $\chi \in \widehat{C}_q$ et $\tilde{\chi} := \mathrm{Ind}_{C_q}^{G_{p,q}}$ son induite.
   (a) Montrer que le caractère de $\tilde{\chi}$ ne dépend que de la C_p-orbite de χ (pour l'action définie à la question précédente).
   (b) Montrer que si χ n'est pas le caractère trivial alors $\tilde{\chi}$ est irréductible et que $\tilde{\chi} \simeq \tilde{\chi}'$ si et seulement si χ et χ' sont dans la même C_q-orbite.
(7) Conclure en dressant la liste des représentations irréductibles de $G_{p,q}$.
(8) Tracer la table des caractères du groupe non-abélien d'ordre 14.
(9) Tracer la table des caractères du groupe non-abélien d'ordre 21.

Examen 2014/2015 - Correction
MAT556 'Modules et groupes finis'
Anna Cadoret

Exercice 1 ('transfert' de semisimplicité) Soit A un anneau associatif unitaire. On a vu en cours que tout sous-A-module et tout A-module quotient d'un A-module semisimple était encore un A-module semisimple. Donc la semisimplicité se transfère aux sous-A-modules et aux A-modules quotients. Pour d'autres types de construction, en général, les choses sont assez compliquées même si on peut quand-même parfois faire des observations intéressantes. Voici deux exemples dans le cas où $A = k[G]$ avec G un groupe fini et k un corps de caractéristique $p > 0$ *divisant* l'ordre de G.

(1) (a) Tout sous $k[G]$-module de V de k-dimension minimale et > 0 est nécessairement simple.
(b) Il suffit de traiter le cas où V est un $k[G]$-module simple. En particulier, V contient un sous-$k[N]$ -module simple non trivial. Soit $W \subset V$ la somme de tous les $k[N]$-sous-modules simple de V; c'est un sous-$k[N]$-module semisimple non trivial de V. De plus, comme N est normal dans G, pour tout $V' \subset V$ sous-$k[N]$-module et pout tout $g \in G$ l'application $g\cdot : V' \tilde{\to} gV'$, $v' \to g \cdot v'$ est un isomorphimse de $k[N]$-modules. Cela montre que W est un sous-$k[G]$-module de V donc, comme V est un $k[G]$-module simple, on a $W = V$ donc V est un $k[N]$-module semisimple.
(c) Soit $W \subset V$ un sous-$k[G]$-module. C'est *a fortiori* un sous-$k[N]$-module. Mais comme V est un $k[N]$-module semisimple, il existe un sous-$k[N]$-module $U \subset V$ tel que

$$V = W \oplus U.$$

Notons $p : V \to W$ la projection sur W parallèlement à U; c'est un morphisme de $k[N]$-modules. Posons

$$\tilde{p} := \frac{1}{[G : N]} \sum_{\overline{g} \in G/N} g^{-1} p(g \cdot -).$$

Notons que c'est bien défini car pour tout $g \in G, n \in N$ on a $(ng)^{-1}p(ngv) = g^{-1}n^{-1}np(gv) = g^{-1}p(gv)$, la première égalité résultant du fait que p est un morphisme de $k[N]$-modules. On vérifie alors que $\tilde{p}$ est un projecteur d'image W et un morphisme de $k[G]$-module; $\ker(\tilde{p})$ est donc un sous-$k[G]$-module de V et $V = W \oplus \ker(\tilde{p})$.

(2) (a) $V(1) = kX \oplus kY$ et la matrice dans la base (X, Y) d'un élément

$$M = \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} \in G$$

opérant sur $V(1)$ est M elle-même. En particulier, $V(1)$ est simple (sinon G serait conjugué à un sous-groupe de $SL_2(k)$ de la forme

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix},$$

ce qui est impossible, par exemple ici pour des raisons de cardinalité.
(b) Il suffit d'observer que pour

$$M = \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} \in G$$

on a $MX^2 = (aX + bY)^2 = a^2X^2 + b^2Y^2 \in V'(2)$ et $MY^2 = (cX + dY)^2 = c^2X^2 + d^2Y^2 \in V'(2)$.
(c) Avec les notations de la question précédente, on a

$$MXY = (aX + bY)(cX + dY) = acX^2 + (ad + bc)XY + bdY^2 \equiv XY \ [V'(2)]$$

(noter que $ad + bc = ad - bc = 1$). Supposons que $|k| \geq 4$. Si la suite exacte courte de $k[G]$-modules

$$0 \to V'(2) \to V(2) \to V(2)/V'(2) \to 0$$

était scindée, $V(2)$ contiendrait un vecteur fixé par G, que l'on peut toujours supposer de la forme $w = \alpha X^2 + \beta Y^2 + XY$. Donc, pour tout

$$M = \begin{pmatrix} \text{a} & \text{b} \\ \text{c} & \text{d} \end{pmatrix} \in G$$

on devrait avoir

$$\begin{pmatrix} a^2 & b^2 \\ c^2 & d^2 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} + \begin{pmatrix} ac \\ bd \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

En particulier, si $b = c = 0$ et $d = a^{-1}$ avec $a^2 \neq 1$ (c'est ici qu'on utilise $|k| \geq 4$:)), on doit avoir $(a^2 - 1)\alpha = 0$, $(a^{-2} - 1)\beta = 0$ donc $\alpha = \beta = 0$. Mais XY n'est clairement pas fixé par G non plus (voir calcul dans la question précédente).

(d) Il suffit de considérer l'application k-biliéaire surjective $f : V(1) \times V(1) \to V(2)$ définie par $f(X_1X_2) = X^2$, $f(X_1, Y_2) = f(Y_1, X_2) = XY$, $f(Y_1, Y_2) = Y^2$. Elle se factorise en une application k-linéaire surjective $V(1) \otimes_k V(1) \twoheadrightarrow V(2)$, dont on vérifie immédiatement que c'est un morphisme de $k[G]$-modules.

(e) Si $V(1) \otimes_k V(1)$ était un $k[G]$-module semisimple alors tous ses $k[G]$-modules quotients le seraient aussi. Or ce n'est pas le cas de $V(2)$ comme on l'a vu dans la question (2) (c).

Exercice 2 (simplicité et Sylow)

(1) (a) Comme $\mathcal{A}(G)$ est normal dans $\mathcal{S}(G)$, $L(G) \cap \mathcal{A}(G)$ est normal dans $L(G)$. Comme G donc $L(G)$ est simple, on a donc $L(G) \cap \mathcal{A}(G) = 1$ ou $L(G) \cap \mathcal{A}(G) = L(G)$. Dans le premier cas, on aurait alors $G \tilde{\to} L(G) \subset \mathcal{S}(G) \xrightarrow{\epsilon} \mathbb{Z}/2$ injectif (ici, $\epsilon : \mathcal{S}(G) \to \mathbb{Z}/2$ dsigne la signature), ce qui contredit l'hypothèse sur G. Donc $L(G) \cap \mathcal{A}(G) = L(G)$ ou encore $L(G) \subset \mathcal{A}(G)$.

(b) Ecrivons $|G| = 2^r m$ avec m impair. Soit S un 2-Sylow de G. Supposons S cyclique de générateur s. Alors $L(s)$ est un produit de m cycles de longueur 2^r à support deux à deux disjoints. En particulier, $\epsilon(L(s)) = (-1)^m = -1$, ce qui contredit le fait que $L(s) \in \mathcal{A}(G)$.

(c) Supposons $n \geq 4$. Un 2-Sylow S de $\mathcal{A}_n$ est d'ordre 2^r avec $r \geq \frac{n}{2}$ (si n pair) ou $\frac{n-1}{2}$ (si n impair). Si S était cyclique, $\mathcal{A}_n$ contiendrait donc un élément d'ordre $2^{\frac{n}{2}}$ ou $2^{\frac{n-1}{2}}$ selon le cas. Mais en considérant la décomposition en produit de cycles à supports deux à deux disjoints d'un élément d'ordre une puissance de 2 dans $\mathcal{S}_n$, on voit que celui-ci est d'ordre $\leq n$ (le cas dégalité n'étant possible que si n est lui-même une puissance de 2). Pour $n \geq 4$, on a toujours $2^{\frac{n-1}{2}} > n$. En fait, les 2-Sylow de $\mathcal{A}_n$ ne sont pas non plus abéliens dès que $n \geq 6$ (pour $n = 5$, on a $s_5 = 4$ donc les 2-Sylow sont de la forme $(\mathbb{Z}/2)^2$). Il suffit de le montrer pour $n = 6$ (puisque pour $n \geq 6$, $\mathcal{A}_n$ contient des copies de $\mathcal{A}_6$ donc les 2-Sylow de $\mathcal{A}_n$ contiennent des copies des 2-Sylow de $\mathcal{A}_6$ comme on l'a vu en cours). Dans ce cas $s_2 = 8$. Soit S un 2-Sylow de $\mathcal{A}_6$. Comme S est un 2-groupe, les orbites de S opérant sur $\{1, \ldots, 6\}$ sont de longueur 2 ou 4. De plus S opère sans point fixe sinon S serait contenu dans une copie de $\mathcal{A}_5$. Or les 2-Sylow de $\mathcal{A}_5$ sont d'ordre 4. Les orbites ne peuvent pas non plus toutes être de longueur 2 sinon les éléments de S seraient tous d'ordre 2. Mais $\mathcal{A}_6$ contient des éléments d'ordre 4 (les produits d'une transposition et d'un 4-cycle à supports disjoints). Donc S a une orbite de longueur 2 - que l'on peut toujours supposer être $\{1, 2\}$ quitte à renuméroter et une orbite de longueur 4 - $\{3, 4, 5, 6\}$. Comme S contient des éléments d'ordre 4, S contient forcément $(12)(3456)$ et son inverse $(12)(3654)$ et ce sont les seuls éléments d'ordre 4 que S peut contenir. De plus, le centralisateur de $(12)(3456)$ dans $\mathcal{A}_6$ est $\langle (12)(3456) \rangle \subsetneq S$ (en effet, si $\sigma \in \mathcal{A}_6$ centralise $(12)(3456)$, il stabilise forcément $\{1, 2\}$ et $\{3, 4, 5, 6\}$ donc σ s'écrit $\sigma = (12)^a(3456)^b$ car le stabilisateur d'un n-cycle c_n dans $\mathcal{S}_n$ est $\langle c_n \rangle$), ce qui montre que S n'est pas abélien (en fait $S = D_8$ puisque des deux groupes non-abéliens d'ordre 8, c'est celui qui n'a que 2 éléments d'ordre 4).

(d) Si G est un groupe fini d'ordre pair tel que $\frac{|G|}{2}$ est impair alors ses 2-Sylow sont d'ordre 2 donc cycliques. D'après la question (1) (b) G ne peut être simple.

(2) (a) Soit p un nombre premier divisant l'ordre de G, $\mathcal{S}_p(G)$ l'ensemble des p-Sylow de G et $s_p := |\mathcal{S}_p(G)|$. On sait que G agit transitivement par conjugaison sur $\mathcal{S}_p(G)$ d'où un

morphisme de groupes non trivial

$$G \to \mathcal{S}(\mathcal{S}_p(G)) \simeq \mathcal{S}_{s_p}.$$

Si on suppose G simple non abélien, ce morphisme est nécessairement injectif donc G s'identifie à un sous-groupe de $\mathcal{S}_{s_p}$ et on a bien $|G||s_p!$.

(b) $|G| = 10^7 = 2^7 5^7$. Si G était simple, on aurait $10^7 | s_5!$. Mais $s_5 \equiv 1[5]$ et $s_5 | 2^7$. Cela impose $s_5 = 16 = 2^4$. Mais 10^7 ne divise pas 16! car la puissance de 5 dans la décomposition de 16! en produit de nombres premiers est 3 (seuls 5, 10 et 15 contribuent).

Problème (caractères irréductibles des groupes non abéliens d'ordre pq)

Soit $p \neq q$ deux nombres premiers distincts avec $p < q$. Soit G un groupe non abélien d'ordre pq.

(1) *Cf.* Cours.

(2) Comme $G_{p,q} = C_q \rtimes C_p \twoheadrightarrow C_p$, on a déjà $DG_{p,q} \subset C_q$. Mais comme C_q est simple, on a soit $DG_{p,q} = C_q$ soit $DG_{p,q} = 1$ mais comme $G_{p,q}$ n'est pas abélien, on a forcément $1 \subsetneq DG_{p,q}$. Donc $DG_{p,q} = C_q$ et $G_{p,q}^{ab} \simeq C_p$. Les représentations irréductibles de dimension 1 de $G_{p,q}$ sont donc les morphismes

$$\phi_k \circ \pi : G_{p,q} \to \mathbb{C}^\times,\ k = 0, \dots, p-1,$$

où $\pi : G_{p,q} \twoheadrightarrow G_{p,q}/C_q \simeq C_p$ est la projection canonique et, si on se fixe un générateur z_p de C_p, $\phi_k : C_p \to \mathbb{C}^\times$ est la représentation définie par $\phi_k(z_p) = e^{\frac{k2i\pi}{p}}$, $k = 0, \dots, p-1$.

(3) On a déjà p représentations irréductibles de dimension 1. Notons pour l'instant r le nombre de représentations irréductibles de G de dimension > 1 et $n_1, \dots, n_r$ la dimension de ces représentations. On a

$$pq = p + n_1^2 + \cdots + n_r^2$$

ou encore $p(q-1) = n_1^2 + \cdots + n_r^2$. On sait aussi que les n_i divisent $|G_{p,q}| = pq$; les seules possibilités sont donc $n_i = p, q$ ou pq. Mais comme $p < q$, on a $p(q-1) < q(q-1) < q^2 < (pq)^2$. Donc, finalement, la seule possibilité est $n_i = p$, $r = \frac{q-1}{p}$ (où l'on retrouve que p divise $q-1$ ...).

(4) (a) On a $|\widehat{G_{p,q}}| = |Cl(G_{p,q})| = p + \frac{q-1}{p}$. On peut isoler comme d'habitude la classe de conjugaison de 1. Il reste donc $p - 1 + \frac{q-1}{p}$ autres classes de conjugaison à déterminer.

(b) Si z_p^k et z_p^l étaient conjugués dans $G_{p,q}$ alors leurs images $\bar{z}_p^k$, $\bar{z}_p^l$ seraient conjuguées dans $G_{p,q}/C_q$. Mais comme $G_{p,q}/C_q \simeq C_p$ est abélien, cela signifierait que $\bar{z}_p^k = \bar{z}_p^l$ donc $z_p^k = z_p^l$ (puisque $C_p \subset G_{p,q} \twoheadrightarrow G_{p,q}/C_q$ est un isomorphisme). Notons B_k la classe de conjugaison de z_p^k, $k = 1, \dots, p-1$. On peut la calculer explicitement. On sait que $z_p^{-1} z_q z_p = z_q^u$ pour un certain $1 \neq u \in (\mathbb{Z}/q)^\times$ donc

$$(z_q^i z_p^j) z_p^k (z_q^i z_p^j)^{-1} = z_q^i z_p^k z_q^{-i} = z_p^k z_p^{-k} z_q^i z_p^k z_q^{-i} = z_p^k z_q^{u^k i - i}.$$

Or comme $1 \neq u$, on a encore $u^k - 1 \in (\mathbb{Z}/q)^\times$ donc l'application $i \to u^k i - i$ est un automorphisme de $\mathbb{Z}/q$. D'où:

$$B_k = \{z_p^k z_q^l \mid l = 0, \dots, q-1\}$$

et B_k est de cardinal q.

(c) Comme C_p est normal dans $G_{p,q}$, C_p est réunion (disjointe) de classes de conjugaison. Fixons un générateur z_q de C_q et un générateur z_p de C_p. Tout élément de $G_{p,q}$ s'écrit alors de façon unique sous la forme $z_q^l z_p^k$, $k = 0, \dots, p-1$, $l = 0, \dots, q-1$. En particulier, on voit que les classes de conjugaison des éléments de C_q dans $G_{p,q}$ sont en fait les orbites de C_p agissant par conjugaison sur C_q. De telles orbites sont de longueur 1 ou p. Mais un élément $1 \neq z \in C_q$ est un générateur de C_q donc ne peut commuter avec z_p (sinon $G_{p,q}$ serait abélien); son orbite sous l'action par conjugaison de C_p est donc de longueur p. En conclusion, C_q est réunion de (disjointe) la classe $I := \{1\}$ et de $\frac{q-1}{p}$ classes de conjugaison $A_1, \dots, A_{\frac{q-1}{p}}$ de cardinal p.

(d) On a donc la classe de 1, $p-1$ classes $B_1, \dots, B_{p-1}$ de cardinal q et $\frac{q-1}{p}$ classes $A_1, \dots, A_{\frac{q-1}{p}}$ de cardinal p. Le compte y est puisque

$$1 + (p-1)q + \frac{q-1}{p}p = pq.$$

(5) Rappelons que comme C_q est abélien, $|\widehat{C}_q| = |C_q| = q$. La encore, comme p est premier, une orbite de C_p agissant sur $\widehat{C}_q$ est de longueur 1 ou p. Soit $\chi \in \widehat{C}_q$ tel que $C_p \cdot \chi = \{\chi\}$. Comme C_q est abélien, χ est de la forme $\chi(z_q^k) = \omega_q^k$ pour une certaine racine q-ième de l'unité ω_q. Donc $C_p \cdot \chi = \{\chi\}$ signifie que $\omega_q^u \chi(z_q^u) = \chi(z_p^{-1} z_q z_p) = \chi(z_q) = \omega_q$ *i.e.* $\omega_q^{u-1} = 1$ mais comme $1 \neq u$, cela impose $\omega_q = 1$ donc χ est le caractère trivial. En conclusion, on a une seule orbite de longueur 1, celle du caractère trivial et $\frac{q-1}{p}$ orbite de longueur p.

(6) Soit $\chi \in \widehat{C}_q$ et

$$\tilde{\chi} := \mathrm{Ind}_{C_q}^{G_{p,q}} = \bigoplus_{0 \leq i \leq p-1} z_p^i \otimes_{\mathbb{C}[C_q]} \chi$$

son induite. Par abus de notation, on note encore $\tilde{\chi}$ le caractère de $\tilde{\chi}$.

(a) On a

$$z_q^k z_p^l z_p^i = z_p^{l+i} z_p^{-(l+i)} z_q^k z_p^{l+i} = z_p^{l+i} z_q^{u^{l+i}k}$$

donc

$$\begin{array}{lll} \tilde{\chi}(z_q^k z_p^l) & = p & \text{si } k = l = 0; \\ & = 0 & \text{si } l \neq 0; \\ & = \sum_{0 \leq i \leq p-1} z_p^i \cdot \chi(z_q^k) = \sum_{\phi \in C_p \cdot \chi} \phi(z_q^k) & \text{si } l = 0,\ k \neq 0. \end{array}$$

En particulier, $\tilde{\chi}$ ne dépend que de $C_p \cdot \chi$.

(b) Supposons χ et χ' distincts du caractère trivial. Calculons

$$\begin{aligned} (\tilde{\chi}, \tilde{\chi}')_{G_{p,q}} &= \frac{1}{pq}(p^2 + \sum_{1 \leq k \leq q-1} \tilde{\chi}(z_q^k)\tilde{\chi}'(z_q^{-k})) \\ &= \frac{1}{pq}(p^2 + \sum_{1 \leq k \leq q-1} \sum_{\phi \in C_p \cdot \chi, \phi' \in \mathbb{C}_p \cdot \chi'} \phi(z_q^k)\phi'(z_q^{-k})) \\ &= \frac{1}{pq}(p^2 + \sum_{\phi \in C_p \cdot \chi, \phi' \in \mathbb{C}_p \cdot \chi'} \sum_{1 \leq k \leq q-1} \phi(z_q^k)\phi'(z_q^{-k})) \\ &= \frac{1}{pq}(p^2 + \sum_{\phi \in C_p \cdot \chi, \phi' \in \mathbb{C}_p \cdot \chi'} (q(\phi, \phi')_{C_q} - 1) \end{aligned}$$

Or $(\phi, \phi')_{C_q} = \delta_{\phi,\phi'}$ donc si χ et χ' ne sont pas dans la même C_p-orbite, on a $(\tilde{\chi}, \tilde{\chi}')_{G_{p,q}} = \frac{1}{pq}(p^2 - p^2) = 0$, si χ et χ' sont dans la même C_p-orbite, on a $(\tilde{\chi}, \tilde{\chi}')_{G_{p,q}} = \frac{1}{pq}(p^2 + p(q-1) - (p^2 - p)) = 1$.

(7) On a trouvé p représentations irréductibles de dimension 1 (question (2)) et $\frac{q-1}{p}$ représentations irréductibles de dimension p (question (6)). On les a donc toutes d'après la question (3).

(8)

	1	B_1	A_1	A_2	A_3
$\mathbb{I}$	1	1	1	1	1
χ_2	1	-1	1	1	1
χ_3	2	0	$2cos(\frac{2\pi}{7})$	$2cos(\frac{4\pi}{7})$	$2cos(\frac{8\pi}{7})$
χ_4	2	0	$2cos(\frac{8\pi}{7})$	$2cos(\frac{2\pi}{7})$	$2cos(\frac{4\pi}{7})$
χ_5	2	0	$2cos(\frac{4\pi}{7})$	$2cos(\frac{8\pi}{7})$	$2cos(\frac{2\pi}{7})$

(9)

	1	B_1	B_2	A_1	A_2
$\mathbb{I}$	1	1	1	1	1
χ_2	j	j^2	1	1	1
χ_3	1	j^2	j	1	1
χ_4	3	0	0	ω	$1-\omega$
χ_5	3	0	0	$1-\omega$	ω

où $\omega = \zeta_7 + \zeta_7^2 + \zeta_7^4$ et $1 - \omega = \zeta_7^3 + \zeta_7^5 + \zeta_7^6$ avec $\zeta_7 = e^{\frac{2i\pi}{7}}$.

anna.cadoret@math.polytechnique.fr
Centre de Mathématiques Laurent Schwartz - Ecole Polytechnique,
91128 PALAISEAU, FRANCE.

MAT 556 EXAMEN 2013/2014
GROUPE ET REPRÉSENTATIONS

BENOIT STROH

La durée est de 3 heures. Toutes les réponses doivent être soigneusement justifiées.
Sont autorisés : le poly de cours, les notes de cours et d'exercices, les dictionnaires papiers.
Les réponses peuvent être rédigées en français ou en anglais.

1. Exercice

1.1. Soit K un corps algébriquement clos de caractéristique $\neq 2$. Soit V un espace vectoriel de dimension n sur K et $(e_1, \cdots, e_n)$ une K-base de V. Soit ι l'endomorphisme K-linéaire de $V \otimes_K V$ défini par $\iota(e_i \otimes e_j) = e_j \otimes e_i$. Montrer qu'il existe une décomposition canonique

$$V \otimes_K V \ = \ \Lambda^2(V) \ \oplus \ \mathrm{Sym}^2(V)$$

avec $\Lambda^2(V) = \{x \in V \otimes_K V \mid \iota(x) = -x\}$ et $\mathrm{Sym}^2(V) = \{x \in V \otimes_K V \mid \iota(x) = x\}$. Calculer la dimension de $\Lambda^2(V)$ et de $\mathrm{Sym}^2(V)$ et donner une base de ces espaces.

1.2. Soit G un groupe fini de cardinal premier à la caractéristique de K et $\theta : G \to \mathrm{GL}_K(V)$ une représentation linéaire de G sur V. Notons χ le caractère de θ. Montrer que $\Lambda^2(V)$ et $\mathrm{Sym}^2(V)$ sont naturellement des représentations de G de caractères respectifs

$$\chi_{\Lambda^2(V)}(g) \ = \ \frac{\chi(g)^2 - \chi(g^2)}{2}$$

et

$$\chi_{\mathrm{Sym}^2(V)}(g) \ = \ \frac{\chi(g)^2 + \chi(g^2)}{2}$$

1.3. Dresser la table des caractères du groupe symétrique $\mathfrak{S}_5$. On pourra utiliser la question précédente pour construire explicitement le caractère d'une représentation irréductible de dimension 6.

2. Exercice

2.1. Soit A un anneau commutatif et M un A-module. Soit $n \geq 1$ un entier, $(x_1, \cdots, x_n) \in M^n$ et $P \in \mathrm{Mat}_{n\times n}(A)$. Notons

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \ = \ P \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

avec donc $(y_1, \cdots, y_n) \in M^n$. Notons $M' = Ax_1 + \cdots + Ax_n \subset M$ et $M'' = Ay_1 + \cdots + Ay_n \subset M$. Montrer que

$$(\det(P)) \cdot M' \ \subset \ M'' \ \subset \ M'.$$

Indication : on pourra utiliser les formules de Cramer qui disent que $\det(P) \cdot x_j = \det(P_j)$ *pour tout* $1 \leq j \leq n$ *où la matrice* $P_j \in \mathrm{Mat}_{n\times n}(M)$ *est obtenue à partir de* P *en remplaçant la* j*-ième colonne de* P *par*

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

En particulier $\det(P_j) \in M$ *a un sens et est donné par la formule sommatoire usuelle avec* $\mathfrak{S}_n$.

2.2. Soit A un anneau commutatif qui admet un unique idéal maximal $\mathfrak{m}$. On dit que A est local. Notons $A^\times = \{x \in A \mid \exists y \in A \,\mathrm{tq}\, xy = 1_A\}$. Montrer que $A^\times = A - \mathfrak{m}$.

2.3. (*Lemme de Nakayama*) Supposons toujours A commutatif local. Soit M un A-module de type fini tel que $\mathfrak{m} \cdot M = M$. Montrer que $M = 0$. *Indication : on pourra utiliser la question 2.1 pour montrer qu'il existe* $a \in \mathfrak{m}$ *tel que* $(1 + a)M = 0$.

2.4. Supposons toujours A commutatif local. Soit M un A-module de type fini et $N \subset M$ un sous-A-module tel que $M = \mathfrak{m}M + N$. Montrer que $N = M$.

2.5. Supposons A commutatif local intègre. Notons K le corps des fractions de A et $k = A/\mathfrak{m}$. Soit M un A-module de type fini. Montrer que $\dim_K(M \otimes_A K) \leq \dim_k(M \otimes_A k)$.

3. Exercice

3.1. Soit p un nombre premier. Montrer que tout groupe de cardinal p est abélien.

3.2. Soit p un nombre premier. Montrer que tout groupe G de cardinal p^2 est abélien. *Indication : On pourra expliquer pourquoi le centre* Z *de* G *est non trivial, puis raisonner par l'absurde en supposant que* G *est non-abélien et en considérant* $x \in G - Z$ *et son stabilisateur* $\mathrm{Stab}_G(x)$ *pour l'action par conjugaison de* G *sur lui-même.*

3.3. (*Réciproque au théorème de Lagrange pour les p-groupes*) Soit p un nombre premier, α un entier et G un groupe de cardinal p^α. Montrer que G admet un sous-groupe distingué de cardinal p^β pour tout $\beta \leq \alpha$. *Indication : montrer qu'il existe un sous-groupe central de cardinal* p *dans* G *puis raisonner par récurrence sur* α.

3.4. Soit p un nombre premier, α un entier et G un groupe de cardinal p^α. À quelle condition le groupe G admet-il des éléments d'ordre p^β pour tout $\beta \leq \alpha$?

3.5. (*Réciproque au théorème de Lagrange pour les groupes nilpotents*) Soit G un groupe fini de cardinal n. Montrer que G est nilpotent si et seulement si il admet un sous-groupe distingué de cardinal r pour tout diviseur r de n.

4. Exercice

4.1. Soit G un groupe fini de centre Z et (V, θ) une représentation irréductible de G sur un $\mathbb{C}$-espace vectoriel de dimension finie. Soit $z \in Z$. Expliquer pourquoi $\theta(z)$ est une homothétie de facteur noté $\lambda(z)$ et pourquoi l'application $\lambda : Z \to \mathbb{C}^*, z \mapsto \lambda(z)$ ainsi obtenue est un morphisme de groupe.

4.2. Soit $m \geq 0$ un entier. Notons $\theta^{\otimes m} : G^m \to \mathrm{GL}_{\mathbb{C}}(V^{\otimes m})$ la représentation de $G^m = G \times \cdots \times G$ sur $V^{\otimes m} = V \otimes_{\mathbb{C}} \cdots \otimes_{\mathbb{C}} V$ obtenue par m produits tensoriels successifs. Soit H l'ensemble des $(z_1, \cdots, z_m) \in Z^m$ tels que $z_1 \times \cdots \times z_m = 1$. Montrer que $\theta^{\otimes m}$ se factorise par G^m/H.

4.3. En déduire que $\dim_{\mathbb{C}}(V)$ divise $\mathrm{Card}(G/Z)$.

CORRIGÉ DE L'EXAMEN 2013/2014
GROUPE ET REPRÉSENTATIONS

BENOIT STROH

1. Exercice

1.1. Comme $\iota\circ\iota = \mathrm{Id}_{V\otimes_K V}$ il suffit de décomposer $V\otimes_K V$ en sous-espaces propres pour ι. La dimension de $\Lambda^2(V)$ est $n(n-1)/2$ et une base est formée des $e_i\otimes e_j - e_j\otimes e_i$ avec $i<j$. La dimension de $\mathrm{Sym}^2(V)$ est $n(n+1)/2$ et une base est formée des $e_i\otimes e_j + e_j\otimes e_i$ avec $i\leq j$.

1.2. Le groupe G agit sur $V\otimes_K V$ par la formule $g\cdot(v\otimes w) = (g\cdot v)\otimes(g\cdot w)$. L'action de G préserve ι donc aussi les sous-espaces $\Lambda^2(V)$ et $\mathrm{Sym}^2(V)$. Soit $g\in G$ et $\lambda_1,\cdots,\lambda_n$ les valeurs propres de $\theta(g)$ sur V. Les valeurs propres de g agissant sur $\Lambda^2(V)$ sont alors les $\lambda_i\lambda_j$ avec $i<j$ car si $(f_1,\cdots,f_n)$ est une base de diagonalisation de $\theta(g)$ – qui est bien diagonalisable – alors une base de diagonalisation de $\theta_{\Lambda^2(V)}(g)$ est formée des $f_i\otimes f_j - f_j\otimes f_i$ avec $i<j$. On a alors

$$\chi_{\Lambda^2(V)} = \sum_{i<j}\lambda_i\lambda_j = \frac{(\sum_i\lambda_i)^2 - \sum_i\lambda_i^2}{2} = \frac{\chi(g)^2-\chi(g^2)}{2}$$

De même pour $\mathrm{Sym}^2(V)$.

1.3. Le groupe $\mathfrak{S}_5$ est de cardinal 120 et a 7 classes de conjugaison : $C_1 =< (1) >$, $C_2 =< (12) >$, $C_3 =< (123) >$, $C_4 =< (12)(34) >$, $C_5 =< (1234) >$, $C_6 =< (12)(345) >$ et $C_7 =< (12345) >$. Il y a donc 7 caractères irréductibles $\chi_1,\cdots,\chi_7$ de dimensions $n_1,\cdots,n_7$. Quitte à réordonner on peut supposer que $\chi_1 = 1$ et que χ_2 est la signature $\varepsilon:\mathfrak{S}_5\to\{\pm1\}$. Ainsi les deux premières lignes de la table sont remplies.

On dispose de la représentation standard V_0 sur l'hyperplan de trace nulle de K^5. On sait qu'elle est irréductible de dimension 4. Notons χ_3 son charactère, qui est facile à calculer explicitement car c'est $\sigma\mapsto \sharp\mathrm{Fix}_{\{1,\cdots,n\}}(\sigma)-1$. On peut alors introduire $\chi_4 = \chi_2\chi_3$ qui est le caractère de la représentation irréductible $V_0\otimes\varepsilon$. On constate numériquement que $\chi_4\neq\chi_3$ donc V_0 n'est pas isomorphe à $V_0\otimes\varepsilon$.

On a donc $n_1 = n_2 = 1$ et $n_3 = n_4 = 4$. On obtient alors $n_5 = n_6 = 5$ et $n_7 = 6$ car $\sum_i n_i^2 = 120$. Introduisons alors $\Lambda^2(V_0)$ (de dimension 6) dont on calcule le caractère $\chi_{\Lambda^2(V_0)}$ en fonction de χ_3. On trouve $(\chi_{\Lambda^2(V_0)},\chi_{\Lambda^2(V_0)})_{\mathfrak{S}_5} = 1$ donc $\Lambda^2(V_0)$ est irréductible et $\chi_{\Lambda^2(V_0)} = \chi_7$ qui est connu.

Il ne reste plus qu'à trouver χ_5 et χ_6. On utilise les relations d'orthogonalité et on a même $\chi_6 = \chi_5\chi_2$ donc il n'y a qu'à introduire 6 inconnues et à résoudre. On trouve finalement la table suivante où on écrit $\chi_i(C_j)$ en position (i,j) :

1	1	1	1	1	1	1
1	-1	1	1	-1	-1	1
4	2	1	0	0	-1	-1
4	-2	1	0	0	1	-1
5	1	-1	1	-1	1	0
5	-1	-1	1	1	-1	0
6	0	0	-2	0	0	1

2. Exercice

2.1. Comme $y_i = \sum_j a_{ij}x_i$ pour tout $1\leq i\leq n$ (où les $a_{ij}\in A$ sont les coefficients de P) il est clair que $M''\subset M'$. Puis $(\det(P))M'$ est engendré par $(\det(P))x_1,\cdots,(\det(P))x_n$ donc il suffit de montrer que $(\det(P))x_i\in M''$ pour tout $1\leq i\leq n$. C'est un corollaire immédiat de la formule de Cramer.

2.2. Tout $x \in A$ est inversible si et seulement si $xA = A$. Mais si $xA \subset A$ est un idéal strict si et seulement si il est inclus dans un idéal maximal strict de A donc si et seulement si $xA \subset \mathfrak{m}$ soit $x \in \mathfrak{m}$.

2.3. Montrons qu'il existe $a \in \mathfrak{m}$ tel que $(1+a)M = 0$. Soit $x_1, \cdots, x_n$ un système générateur de M sur A. Comme $\mathfrak{m}M = M$, il existe $a_{ij} \in \mathfrak{m}$ tels que $x_i = \sum_{j=1}^n a_{ij}x_j$ pour tout tout $1 \leq i \leq n$. Introduisons $P = \mathrm{Mat}(a_{ij}) - I_n$. En utilisant les notations de la question 2.1 on a donc $M' = M$ et $M'' = 0$ donc $\det(P)M = 0$. Mais il est clair que $\det(P)$ est de la forme $1 + a$ avec $a \in A$.

On a $1 + a \notin \mathfrak{m}$ donc $1 + a$ est inversible grâce à la question 2.2. On en déduit finalement que $M = 0$.

2.4. Appliquer la question précédente à M/N.

2.5. Soit $n = \dim_k(M \otimes_A k)$ et $(e_1, \cdots, e_n)$ une k-base de $M \otimes_A k$. Soit $f_i \in M$ qui relève e_i pour tout $1 \leq i \leq n$. Notons $N \subset M$ le sous-A-module engendré par $f_1, \cdots, f_n$. D'après la question précédente, on a $N = M$ donc $M \otimes_A K$ est engendré par n éléments, d'où l'inégalité voulue.

3. Exercice

3.1. Tout groupe de cardinal p est cyclique donc abélien par le théorème de Lagrange.

3.2. Soit G un groupe de cardinal p^2. C'est un p-groupe donc son centre Z n'est pas trivial. Le cardinal de Z est donc p ou p^2. Si c'est p^2 c'est fini. Sinon soit $x \in G \setminus Z$ et H le stabilisateur de x pour l'action de G sur lui-même par conjugaison. On a $Z \subset H$ et $x \in H$ donc H est de cardinal p^2 donc x est central dans G, ce qui est absurde.

3.3. Si $\alpha = 0$ c'est clair. Sinon on raisonne par récurrence sur α. Comme G est un p-groupe son centre est non-trivial donc admet un élément d'ordre p d'après le théorème de classification des groupes abéliens finis. Notons W le sous-groupe engendré, il est central de cardinal p dans G. Par hypothèse de récurrence, il existe un sous-groupe distingué $\bar{H} \subset G/W$ de cardinal $p^{\beta-1}$. Son image inverse H dans G est distinguée de cardinal p^β, ce qu'il fallait démontrer.

3.4. Si G admet un élément d'ordre p^α il est cyclique. L'inverse est vraie.

3.5. Commençons par montrer que si G est nilpotent, il admet des sous-groupes distingués de tout ordre. On sait que G est un produit de p-groupes où p parcourt les nombres premiers. Il suffit alors d'appliquer la question 3.3 et de construire le sous-groupe distingué de G comme produit de sous-groupes distingués dans chacun des facteurs de G.

Si G admet des sous-groupes distingués de tout ordre, montrons qu'il est nilpotent. On obtient en effet que les p-Sylow de G sont distingués, ce qui est une caractérisation des groupes nilpotents.

4. Exercice

4.1. C'est le lemme de Schur.

4.2. On remarque que H est bien un sous-groupe car Z est abélien. Pour tout $(z_1, \cdots, z_m) \in Z^m$, le morphisme $\theta^{\otimes m}(z_1, \cdots, z_m)$ est une homothétie de facteur $\lambda(z_1 \times \cdots \times z_m)$ d'où la réponse.

4.3. Notons c le cardinal de Z, g celui de G et d la dimension de V. La dimension de $V^{\otimes m}$ est d^m. D'après un résultat du cours, $V^{\otimes m}$ est une représentation irréductible de G^m donc aussi de G^m/H. D'après un autre résultat du cours, on en déduit que d^m divise g^m/c^{m-1} car g^m est le cardinal de G et c^{m-1} celui de H. Donc $(\frac{g}{cd})^m \in \frac{1}{c}\mathbb{Z}$ pour tout $m \geq 0$. On en déduit $g/cd \in \mathbb{Z}$ ce qu'il fallait démontrer.

Examen 2012/2013
MAT556 'Groupes et Représentations'
Anna Cadoret

Avertissement.

Sont autorisés: le polycopié du cours, les notes manuscrites du cours et des exercices traités en cours, les dictionnaires de langues papier.

Les réponses peuvent être rédigées en français ou *en anglais*.

Le sujet est *long* (il n'est clairement pas possible de le traiter correctement dans les 3 heures imparties) mais *le barême sera adapté en conséquence*. Il vaut donc mieux traiter moins de questions mais en rédiger soigneusement et rigoureusement les réponses.

Les deux exercices et le problème sont indépendants mais les questions à l'intérieur de chaque exercice et du problème s'enchainent. Si vous ne savez pas répondre à une question, il faut donc, quand c'est possible, essayer d'en deviner la réponse pour passer à la suivante. Le problème porte sur la théorie de groupes finis (Cours 4-5) et les deux exercices sur la théorie des représentations des groupes finis (Cours 6-9).

Problème (groupes simples d'ordre 168)

(1) On note $\mathbb{P}^1(\mathbb{F}_7)$ l'ensemble des droites vectorielles de $\mathbb{F}_7^{\oplus 2}$. Montrer qu'on a des bijections naturelles
$$\{(i,1)\}_{0\leq i\leq 6}\cup\{(1,0)\}\tilde{\to}\mathbb{P}^1(\mathbb{F}_7)\tilde{\to}s(\mathbb{F}_7^{\oplus 2}\setminus\{0\})/\mathbb{F}_7^\times.$$
On notera $\infty := (1,0)(" = \frac{1}{0}")$, $i := (i,1)(" = \frac{i}{1}")$, $i = 0,\dots,6$ et $\mathbb{P}(\mathbb{F}_7) := \mathbb{P}^1(\mathbb{F}_7)\setminus\{\infty\} = \{1,\dots,i\}$.

(2) On fait agir le groupe $\mathrm{SL}_2(\mathbb{F}_7)$ sur l'ensemble $\mathbb{P}^1(\mathbb{F}_7)$ des droites vectorielles de $\mathbb{F}_7^2$. Montrer que le noyau du morphisme induit $\varphi : \mathrm{SL}_2(\mathbb{F}_7)\to\mathfrak{S}(\mathbb{P}^1(\mathbb{F}_7))$ est $\{\pm Id\}$.

Dans la suite, on notera
$$\mathrm{PSL}_2(\mathbb{F}_7) := \mathrm{SL}_2(\mathbb{F}_7)/\{\pm Id\}$$

(3) (Description de l'image). On appelle homographie toute application
$$\begin{array}{rccc} h: & \mathbb{P}^1(\mathbb{F}_7) & \tilde{\to} & \mathbb{P}^1(\mathbb{F}_7) \\ & i & \to & \frac{ai+b}{ci+d} \end{array}$$
avec $a,b,c,d\in\mathbb{F}_7$, $ad-bc=1$ et les conventions
$$\begin{array}{l} 1/\infty = 0; \\ 1/0 = \infty; \\ a\infty/b\infty = a/b. \end{array}$$
Justifier que l'ensemble $\mathcal{H}(\mathbb{F}_7)$ des homographies est exactement l'image de φ et, en particulier, forme un sous-groupe de $\mathfrak{S}(\mathbb{P}^1(\mathbb{F}_7))$.

(4) Justifier que $|\mathrm{PSL}_2(\mathbb{F}_7)| = 168$.

Dans la suite, on admettra que $\mathrm{PSL}_2(\mathbb{F}_7)$ est un groupe simple. Nous allons montrer que tout groupe simple d'ordre 168 est isomorphe à $\mathrm{PSL}_2(\mathbb{F}_7)$. Soit donc G un groupe simple d'ordre 168. On notera $\mathcal{S}_p(G)$ l'ensemble de ses p-Sylow.

(5) Montrer que $|\mathcal{S}_7(G)| = 8$.

Soit $S\in\mathcal{S}_7(G)$. Posons $\mathbb{P}^1 := \mathcal{S}_7(G)$, $\infty := S$ et $\mathbb{P} := \mathbb{P}^1\setminus\{\infty\}$. On fait agir G par conjugaison sur $\mathbb{P}^1$, cela induit un morphisme de groupes
$$\psi : G\to\mathfrak{S}(\mathbb{P}^1).$$

(6) Montrer que $\psi : G\to\mathfrak{S}(\mathbb{P}^1)$ est injectif. En déduire que les éléments de G sont d'ordre ≤ 15.

La principale difficulté est donc de montrer que l'image de ψ s'identifie au sous-groupe des homographies de $\mathfrak{S}(\mathbb{P}^1)$. La fin du problème y est consacrée. La stratégie consiste à choisir une identification *ad-hoc* entre $\mathbb{P}^1$ et $\mathbb{P}^1(\mathbb{F}_7)$ et à exhiber trois éléments $\alpha,\beta,\gamma\in G$ tels que $\psi(\alpha),\psi(\beta),\psi(\gamma)$ sont des homographies et $G = \langle\alpha,\beta,\gamma\rangle$.

(7) Soit $N := \mathrm{Nor}_G(S)$ le normalisateur de S dans G. Calculer $[G:N]$.

(8) Calculer $|\mathcal{S}_7(N)|$. En déduire que N est produit semidirect non direct d'un groupe cyclique d'ordre 7 par un groupe cyclique d'ordre 3. En déduire qu'il existe $\alpha,\beta\in N$ avec α d'ordre 7, β d'ordre 3,
$$N = \langle\alpha\rangle\rtimes\langle\beta\rangle,$$

et qu'on peut toujours supposer que la structure de produit semi-direct est donnée par $\beta\alpha\beta^{-1} = \alpha^2$.

Par définition, les éléments de N fixent ∞ donc N agit par conjugaison sur $\mathbb{P}$, ce qui définit un morphisme de groupes

$$N \to \mathfrak{S}(\mathbb{P})$$

(8) Montrer que α agit simplement transitivement sur $\mathbb{P}$;

(9) Montrer qu'il existe un unique $x_0 \in \mathbb{P}$ tel que $\beta \cdot x_0 = x_0$.

(10) En déduire qu'on peut écrire

$$\mathbb{P} = \{x_0, \alpha \cdot x_0, \alpha^2 \cdot x_0, \ldots, \alpha^6 \cdot x_0\}.$$

Dans la suite, on identifie

$$\begin{array}{ccc} \mathbb{P}^1(\mathbb{F}_7) & \tilde{\to} & \mathbb{P}^1 \\ \infty & \to & \infty \\ i & \to & \alpha^i \cdot x_0 \end{array} .$$

(11) Modulo l'identification ci-dessus, montrer que $\psi(\alpha)$, $\psi(\beta)$ sont respectivement les homographies $i \to i+1$, $i \to \frac{i}{2}$.

(12) Calculer $|\mathcal{S}_3(N)|$.

(13) Notons $S' := \langle\beta\rangle$ et $N' := \mathrm{Nor}_G(S')$. En utilisant (11), montrer que $|\mathcal{S}_3(G) > 7|$. En déduire que $|N'| = 6$.

(14) En déduire que $N' = \mathbb{Z}/6$ ou qu'il existe $\gamma \in N'$ d'ordre 2 tel que

$$N' = \langle\beta\rangle \rtimes \langle\gamma\rangle,$$

et qu'on peut toujours supposer que la structure de produit semi-direct est donné par $\gamma\beta\gamma^{-1} = \beta^{-1}$.

On souhaite éliminer le cas $N' = \mathbb{Z}/6$. Pour cela, on va montrer que G ne contient pas d'éléments d'ordre 6. Notons respectivement U_6 et U_3 l'ensemble des éléments d'ordre 6 et d'ordre 3 de G. Supposons $U_6 \neq \emptyset$. On va montrer que cette hypothèse implique que G a trop d'éléments.

(15) Calculer le nombre d'éléments d'ordre 7 (*cf.* (5)) et d'ordre 3 (*cf.* (14)) de G.

(16) Montrer que l'application

$$\begin{array}{ccc} U_6 & \to & \mathcal{S}_3(G) \\ u & \to & \langle u^2 \rangle \end{array}$$

est surjective.

(17) En déduire que l'application

$$\begin{array}{ccc} U_6 & \to & U_3 \\ u & \to & u^2 \end{array}$$

est surjective et que G a au moins 56 éléments d'ordre 6.

(18) Montrer qu'on obtient ainsi une contradiction et donc que N' n'est pas cyclique.

(19) Montrer que $\gamma \notin N$.

(20) Montrer qu'un sous-groupe $N \subsetneq H \subset G$ est nécessairement d'indice 1 ou 4 dans G. Un tel sous-groupe d'indice 4 peut-il exister? En déduire que

$$G = \langle N, \gamma \rangle = \langle \alpha, \beta, \gamma \rangle.$$

(21) Il reste à voir que $\psi(\gamma)$ est une homographie.

(a) Montrer que $\gamma(\infty) = 0$ et $\gamma(0) = \infty$.

(b) Montrer que γ échange les deux orbites $\{1, 2, 4\}$ et $\{3, 6, 5\}$ de β agissant sur $\mathbb{P}$.

(c) Montrer que $\gamma(i) = \frac{\gamma(1)}{i}$.

(d) Notons $\lambda := \gamma(1)$. Montrer que $-\lambda \in (\mathbb{F}_7^\times)^2$. Ecrivons $-\lambda = \mu^2$ avec $\mu \in \mathbb{F}_7^\times$. Déduire de ce qui précède que $\psi(\gamma)$ est l'homographie $i \to -\frac{\mu}{\mu^{-1} i}$.

Exercice 1

Soit $p > 2$ un nombre premier, $q := p^r$ (avec $r \geq 1$). Rappelons qu'on désigne par $\mathbb{F}_q$ le corps à q éléments (*i.e.* le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$ ou, plus concrètement, l'ensemble des solutions de l'équation $x^q - x = 0$ dans une cloture algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$). Notons $V := \mathbb{F}_q^{\oplus 2}$. On considère le groupe des similitudes affines de V

$$G := \left\{ \begin{array}{ccc} V & \to & V \\ v & \to & av + b \end{array} \ , \ a \in \mathbb{F}_q^\times, \ b \in \mathbb{F}_q \right\}$$

(1) On note $N := (\mathbb{F}_q, +)$ et $Q := (\mathbb{F}_q^\times, \times)$. Montrer que G est canoniquement isomorphe à un produit semi-direct $N \rtimes_\phi Q$ dont on décrira explicitement la loi de composition interne.

(2) Montrer que N est isomorphe à $(\mathbb{Z}/p)^{\oplus r}$.

(3) Montrer que tout Sylow de Q est cyclique. En déduire que Q lui-même est cyclique.

(4) Calculer l'abélianisé de G et en déduire les représentations irréductibles de $\mathbb{C}$-dimension 1 de G.

(5) Déterminer les représentations irréductibles de N et calculer le caractère des représentations induites $\mathrm{Ind}_N^G(\mathbb{C}, \chi)$, $(\mathbb{C}, \chi) \in \widehat{\mathbb{C}[N]}$.

(6) En déduire la table des caractères de G.

Exercice 2

Soit G un groupe fini et (V, θ) une $\mathbb{C}$-représentation *fidèle*, de dimension finie n de G. On se fixe une base $e_1, \ldots, e_n$ de V de base duale $e_1^\vee, \ldots, e_n^\vee$ (*i.e.* $e_i^\vee(e_j) = \delta_{i,j}$) et on considère la $\mathbb{C}$-algèbre de polynômes en les indéterminées $e_1^\vee, \ldots, e_n^\vee$

$$S(V^\vee) := \mathbb{C}[e_1^\vee, \ldots, e_n^\vee] = \bigoplus_{d \geq 0} S_d(V^\vee),$$

où on note

$$S_d(V^\vee) = \bigoplus_{|\underline{\alpha}| = d} \mathbb{C} e_1^{\vee \alpha_1} \cdots e_n^{\vee \alpha_n}$$

le sous-$\mathbb{C}$-espace vectoriel des polynômes homogènes de degré d. On fait agir G sur chacun des $S_d(V^\vee)$ par

$$\theta_d^\vee(g)(e_1^{\vee \alpha_1} \cdots e_n^{\vee \alpha_n}) = \theta^\vee(g)(e_1^\vee)^{\alpha_1} \cdots \theta^\vee(g)(e_n^\vee)^{\alpha_n} = e_1^\vee(g^{-1} -)^{\alpha_1} \cdots e_n^\vee(g^{-1} -)^{\alpha_n}.$$

L'objectif de cet exercice est de montrer que toute représentation irréductible de G est une sous-représentation de $S_d(V^\vee)$ pour un certain $d \geq 0$.

(1) Montrer qu'un $\mathbb{C}$-espace vectoriel V de $\mathbb{C}$-dimension finie ne peut s'écrire comme réunion d'un nombre fini de sous-$\mathbb{C}$-espaces vectoriels stricts (Ind.: on pourra observer qu'il suffit de montrer qu'un $\mathbb{C}$-espace vectoriel V de $\mathbb{C}$-dimension finie ne peut s'écrire comme réunion d'un nombre fini d'*hyperplans*, écrire l'équation de la réunion finie d'hyperplans dans une base de V, observer qu'il s'agit d'une équation polynomiale en n variables, se ramener à une variable (en substituant X^j à X_j) et obtenir une contradiction en utilisant que $\mathbb{C}$ est infini).

(2) Déduire de (1) qu'il existe $v \in V$ tel que $\mathrm{Stab}_G(v) = \{e_G\}$.

(3) On choisit $v \in V$ comme en (2). On introduit le morphisme de $\mathbb{C}$-espaces vectoriels

$$\begin{array}{rccc} \Phi_v\colon & S(V^\vee) & \to & \mathbb{C}[G] \\ & e_1^{\vee\alpha_1}\cdots e_n^{\vee\alpha_n} & \to & \sum_{g\in G}(e_1^{\vee\alpha_1}\cdots e_n^{\vee\alpha_n})(gv)g \end{array}$$

(a) Montrer que $\Phi_v : S(V^\vee) \to \mathbb{C}[G]$ est un morphisme de $\mathbb{C}[G]$-modules (où l'on munit $\mathbb{C}[G]$ de sa structure de $\mathbb{C}[G]$-module régulier, comme d'habitude).

(b) Montrer que $\Phi_v : S(V^\vee) \to \mathbb{C}[G]$ est surjectif (Ind: Il suffit de montrer que les éléments $g \in \mathbb{C}[G]$ sont dans l'image de Φ_v).

(4) Déduire de (3) que pour toute représentation irréductible $(W, \tau) \in \mathbb{C}[G]$ il existe $d_\tau \geq 0$ et un morphisme surjectif de $\mathbb{C}[G]$-modules

$$\Phi_{v,\tau} : S_{d_\tau}(V^\vee) \twoheadrightarrow W.$$

(5) Conclure.

anna.cadoret@math.polytechnique.fr
Centre de Mathématiques Laurent Schwartz - Ecole Polytechnique,
91128 PALAISEAU, FRANCE.

Examen 2012/2013 - Correction
MAT556 'Groupes et Représentations'
Anna Cadoret

Problème (groupes simples d'ordre 168)

(1) La première bijection est juste l'application qui à un vecteur v de coordonnées $(i,1)$, $0 \leq i \leq 6$ ou $(1,0)$ associe la droite $\mathbb{F}_7 v$. La seconde bijection s'obtient en considérant l'application surjective $(\mathbb{F}_7^{\oplus 2} \setminus \{0\}) \twoheadrightarrow \mathbb{P}^1(\mathbb{F}_7)$ qui envoie un vecteur $0 \neq v \in \mathbb{F}_7^{\oplus 2}$ sur la droite $\mathbb{F}_7 v$ et en observant que deux vecteurs $0 \neq v, v' \in \mathbb{F}_7^{\oplus 2}$ engendrent la même droite si et seulement si il existe $\lambda \in \mathbb{F}_7^\times$ tel que $v' = \lambda v$ donc l'application surjective $(\mathbb{F}_7^{\oplus 2} \setminus \{0\}) \twoheadrightarrow \mathbb{P}^1(\mathbb{F}_7)$ se factorise en une bijection

$$(\mathbb{F}_7^{\oplus 2} \setminus \{0\})/\mathbb{F}_7^\times \twoheadrightarrow \mathbb{P}^1(\mathbb{F}_7)$$

.

(2) $\ker(\phi)$ est l'ensemble des matrices $M \in \mathrm{SL}_2(\mathbb{F}_7)$ qui fixent toutes les droites du plan. En particulier si $v, v' \in (\mathbb{F}_7^{\oplus 2}$ sont deux vecteurs linéairement indépendants on doit avoir $Mv = \lambda v$, $Mv' = \lambda v'$, $\lambda v + \lambda v' = M(v+v') = \mu(v+v')$ donc $\lambda = \lambda' = \mu$. Ce qui montre déjà que M est une matrice scalaire $M = \lambda Id$. En outre $\det(M) = \lambda^2 = 1$ impose $\lambda = \pm 1$.

(3) (Description de l'image). Une matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ envoie la droite de vecteur directeur $(i,1)$ (resp. $(1,0)$) sur la droite de vecteur directeur $(ai+b, ci+d)$ (resp. (a,c)) donc, modulo l'identification $\mathbb{P}^1(\mathbb{F}_7)$ à $0, 1, \ldots, 6, \infty$, $\varphi(M)$ est exactement l'homographie $i \to \frac{ai+b}{ci+d}$.

(4) On a les suites exactes courtes

$$1 \to \mathrm{SL}_2(\mathbb{F}_7) \to \mathrm{GL}_2(\mathbb{F}_7) \stackrel{\det}{\to} \mathbb{F}_7^\times \to 1$$

et

$$1 \to \{\pm 1\} \to \mathrm{SL}_2(\mathbb{F}_7) \to \mathrm{PSL}_2(\mathbb{F}_7) \to 1.$$

De la première on déduit $|\mathrm{SL}_2(\mathbb{F}_7)| = \frac{|\mathrm{GL}_2(\mathbb{F}_7)|}{\mathbb{F}_7^\times} = \frac{(7^2-1)(7^2-7)}{7-1} = 7(7^2-1)$ et de la seconde $|\mathrm{PSL}_2(\mathbb{F}_7)| = \frac{|\mathrm{SL}_2(\mathbb{F}_7)|}{|\{\pm 1\}|} = \frac{7(7^2-1)}{2} = 168$.

(5) On a $|\mathcal{S}_7(G)||24$ et $|\mathcal{S}_7(G)| \equiv 1 \bmod 7$. Comme G est simple, on a aussi $|\mathcal{S}_7(G)| > 1$. Le seul cas possible est donc $|\mathcal{S}_7(G)| = 8$.

(6) Comme G agit transitivement par conjugaison sur $\mathcal{S}_7(G)$, ϕ n'est pas le morphisme trivial. Son noyau est donc un sous-groupe normal strict de G. Comme G est simple, c'est forcément $\{1\}$. En particulier G se plonge dans $\mathfrak{S}(\mathbb{P}^1) \simeq \mathfrak{S}_8$. Or les éléments du groupe de permutation $\mathfrak{S}_8$ sont d'ordre au plus 15 (produits d'un 3-cycle et d'un 5-cycle à supports disjoints).

(7) Comme G agit transitivement sur $\mathcal{S}_7(G)$ on a

$$[G : N] = |G \cdot S| = |\mathcal{S}_7(G)| = 8.$$

(8) D'après (7) on a $|N| = 21 = 3 \cdot 7$. En outre $|\mathcal{S}_7(G)||3$ et $|\mathcal{S}_7(G)| \equiv 1 \bmod 7$ donc la seule possibilité est $|\mathcal{S}_7(G)| = 1$ *i.e.* N ne possède qu'un seul 7-Sylow C et celui-ci est normal dans N. On a donc une suite exacte courte

$$1 \to C \to N \to N/C \to 1.$$

De plus $|C| = 7$ et $N/C = 3$ donc C est le groupe cyclique $\mathbb{Z}/7$ et N/C le groupe cyclique $\mathbb{Z}/3$. Par Schur-Zassenhauss, la suite exacte courte ci-dessus se scinde donc $N = C \rtimes N/C$. En outre, ce produit semidirect n'est pas direct sinon N serait cyclique (lemme Chinois), ce

qui contredirait (6). Choisissons $\alpha \in C$ un générateur de C et $\beta \in N$ un élément d'ordre 3 relevant un générateur de N/C. On a $\beta\alpha\beta^{-1} = \alpha^k$ avec $k = 2, 4$ (les deux éléments d'ordre 3 de $\mathbb{F}_7^\times$). Si $k = 4$, on remplace β par β^2.

(9) Déjà α agit non trivialement sur $\mathbb{P}$ puisque ψ est injectif. Comme α est d'ordre 7 son image dans $\mathfrak{S}(\mathbb{P}) \simeq \mathfrak{S}_7$ est également d'ordre 7. Mais les seuls éléments d'ordre 7 dans $\mathfrak{S}_7$ sont les 7-cycles, qui agissent simplement transitivement sur $\{1, \ldots, 7\}$.

(10) Le même raisonnement appliqué à β montre que l'image de β est soit un 3-cycle soit un produit de deux 3-cycles à supports disjoints. Dans les deux cas ces permutations ont au moins un point fixe. Donc il existe bien $x_0 \in \mathbb{P}$ tel que $\beta \cdot x_0 = x_0$. Si β avait deux point fixe, par (9) il existerait $1 \leq k \leq 6$ tel que $\beta\alpha^k x_0 = \alpha^k x_0$. Mais $\beta\alpha^k x_0 = \beta\alpha^k\beta^{-1}x_0 = \alpha^{2k}x_0$. D'où $\alpha^k x_0 = x_0$, ce qui contredit le fait que α agit simplement sur $\mathbb{P}$.

(11) Cela résulte immédiatement de (8).

(12) Faisons le calcul: $\psi(\alpha)(\infty) = \psi(\beta)(\infty) = \infty$ par définition de N et $\psi(\alpha)(i) = \alpha \cdot \alpha^i x_0 = \alpha^{i+1}x_0 = i + 1 \bmod 7$,. $\psi(\beta)(i) = \beta \cdot \alpha^i x_0 = \beta\alpha^i\beta^{-1}x_0 = \alpha^{2i}x_0 = 2i \bmod 7$.

(13) On a $|\mathcal{S}_3(N)||7$ et, comme N est non abélien, $|\mathcal{S}_3(N)| > 1$ donc $|\mathcal{S}_3(N)| = 7$.

(14) Comme $168 = 7 \cdot 3 \cdot 2^3$, S' est aussi un 3-Sylow de G donc $|N'| = \frac{|G|}{|\mathcal{S}_3(G)|}$ avec $|\mathcal{S}_3(G)||56$ et $|\mathcal{S}_3(G)| \equiv 1 \bmod 3$, $|\mathcal{S}_3(G)| \geq 7$. En fait $|\mathcal{S}_3(G)| > 7$ sinon on aurait $\mathcal{S}_3(G) = \mathcal{S}_3(N)$ donc le sous-groupe (normal!) engendré par les 3-Sylow de G serait contenu dans N, contredisant la simplicité de G. La seule possibilité est donc $|\mathcal{S}_3(G)| = 28$ et $|N'| = 6$.

(15) Si N' est abélien, on a $N' = \mathbb{Z}/6$ (lemme Chinois) sinon, comme par définition de N' le groupe $\langle\beta\rangle$ est normal dans N' on a une suite exacte courte

$$1 \to \langle\beta\rangle \to N' \to N'/\langle\beta\rangle \to 1,$$

qui se scinde par Schur-Zassenhauss donc il existe $\gamma \in N'$ d'ordre 2 tel que

$$N' = \langle\beta\rangle \rtimes \langle\gamma\rangle,$$

et comme ce produit n'est pas direct, on a forcément $\gamma\beta\gamma^{-1} = \beta^{-1}$ (γ est d'ordre 2).

(16) Qu'il s'agisse de 3 ou 7 les Sylow correspondant sont cycliques d'ordre premier donc d'intersection deux à deux trivial. On en déduit qu'il y a $(7-1)|\mathcal{S}_7(G)| = 48$ éléments d'ordre 7 et $(3-1)|\mathcal{S}_3(G)| = 56$ éléments d'ordre 3. $|\mathcal{S}_2(G)||21$, $|\mathcal{S}_2(G)| \equiv 1 \bmod 2$ et $|\mathcal{S}_2(G)| > 1$ donc $|\mathcal{S}_2(G)| \geq 3$.

(17) Comme G agit transitivement sur ses 3-Sylow, pour tout $T \in \mathcal{S}_3(G)$ il existe $g \in G$ tel que $T = g^{-1}S'g$ donc $\mathrm{Nor}_G(T) = g^{-1}\mathrm{Nor}_G(S')g = g^{-1}N'g$. En particulier $\mathrm{Nor}_G(T)$ est cyclique d'ordre 6 avec pour unique 3-Sylow T. Donc si $u \in \mathrm{Nor}_G(T)$ est un générateur de $\mathrm{Nor}_G(T)$, u^2 est un générateur de T.

(18) D'après (16), pour tout $v \in U^3$ il existe $u \in U_6$ tel que $\langle v\rangle = \langle u^2\rangle$ *i.e.* $v = u^2$ ou $v = u^{-2} = (u^{-1})^2$. Donc $|U_6| \geq |U_3| = 56$.

(19) Les questions précédentes montrent qu'on a déjà au moins $48 + 56 + 56 = 160$ éléments d'ordre $3, 6$ ou 7. Comme G a au moins deux 2-Sylow dont l'intersection est un groupe d'ordre au plus 4, on a au moins 11 éléments d'ordre une puissance de 2. Ce qui contredit $|G| = 168$.

(20) Si $\gamma \in N$ on aurait $N' \subset N$ donc $6|21$, ce qui n'est pas possible.

(21) On aurait alors $21||H||168$ et $|H| > 21$. Les seules possibilités sont $|H| = 42$, 84 ou 168. Si $|H| = 42$, N serqit d'indice 2 donc normal dans H. Mais cela impliquerait que H agit par

conjugaison sur les 7-Sylow de N. Comme N a pour unique 7-Sylow S, cela impliquerait que H normalise S donc $H \subset N$: c'est impossible. Donc $|H| = 84$ ou 168. Mais si H est d'indice 4 en faisant agir G par translation sur G/H et en invoquant la simplicité de G, on obtiendrait un plongement $G \hookrightarrow \mathfrak{S}(G/H) \simeq \mathfrak{S}_4$, ce qui contredit $|G| = 168$. En particulier $\langle N, \gamma\rangle = G$.

(22) (a) x_0 est l'unique point fixe de β opérant sur $\mathbb{P}$. Donc, il faut voir que $\beta \cdot \gamma S = \gamma S$ puis $\gamma \cdot \gamma S = S$. La deuxième égalité résulte immédiatement du fait que γ est d'ordre 2. Pour la première, on a $\gamma^{-1}\beta\gamma = \beta^{-1} \in N$ donc $\gamma^{-1}\beta\gamma S = S$.

(b) On a $\beta = (1,2,4)(3,6,5)$ et

$$(1,4,2)(3,5,6) = \beta^{-1} = \gamma\beta\gamma^{-1} = (\gamma(1),\gamma(2),\gamma(4))(\gamma(3),\gamma(5),\gamma(6)),$$

ce qui montre que nécessairement γ stabilise ou permute les orbites de β agissant sur $\mathbb{P}$. Dans le premier cas, comme γ est d'ordre 2, γ aurait au moins deux points fixes (un dans chaque orbite de β agissant sur $\mathbb{P}$) donc serait conjugué à un élément de N, ce qui est impossible puisque $2 \not| 21$.

(c) Comme β^{-1} est l'homothétie de rapport 2 on a $2\gamma(2i) = \beta^{-1}\gamma(2i) = \gamma(\beta(2i)) = \gamma(i)$ d'où

$$\gamma(2i) = \frac{\gamma(i)}{2}$$

Donc $\gamma(2) = \frac{\gamma(1)}{2}$, $\gamma(4) = \frac{\gamma(2)}{2} = \frac{\gamma(1)}{4}$, *etc.*

(d) Comme $\lambda \in \{3,5,6\}$ on a $-\lambda \in \{4,2,1\} = (\mathbb{F}_7^\times)^2$, donc on peut écrire $\lambda = -\mu^2$. On a alors

$$\frac{\lambda}{i} = -\frac{\mu^2}{i} = -\frac{\mu}{\mu^{-1}i}$$

et "$ad - bc = -(-\mu)\mu^{-1} = 1$". Cela montre que γ est bien une homographie.

Exercice 1

(1) On va construire explicitement l'isomorphisme. Ensemblistement, on a une bijection

$$\begin{array}{rccc} s\colon & N \times Q & \to & G \\ & (b,a) & \to & v \to av + b. \end{array}$$

Si on calcule la composée $s(b',a') \circ s(b,a)$ on trouve

$$s(b',a') \circ s(b,a) = s(a'b + b', a'a).$$

Munissons donc $N \times Q$ de la structure de produit semidirect $N \rtimes Q$ défini par le morphisme

$$\begin{array}{rccc} \phi\colon & Q & \to & \mathrm{Aut}_{Grp}(N) \\ & a & \to & b \to ab. \end{array}$$

On a alors par définition du produit semidirect

$$(b',a') \cdot_\phi (b,a) = (b' + \phi(a')(b), a'a) = (b' + a'b, a'a).$$

Cela montre que la bijection ensembliste $s : N \times Q \tilde{\to} G$ est en fait un isomorphisme de groupes $s : N \rtimes_\phi Q \tilde{\to} G$.

(2) Comme $\mathbb{F}_q$ est de caractéristique p, tous les élément du groupe $(\mathbb{F}_q, +)$sont d'ordre 0 ou p. Par le théorème de structure des groupes abéliens de type fini $(\mathbb{F}_q, +)$ est donc isomorphe à $(\mathbb{Z}/p)^{\oplus r}$.

(3) Soit ℓ un nombre premier divisant $q - 1 = |Q|$ et S un ℓ-Sylow de Q. Disons $|S| = \ell^s$. Si tous les éléments de S sont d'ordre $< \ell^s$, il existe $s' < s$ tel que tous les éléments de S soient solution de l'équation $x^{\ell^{s'}} - 1 = 0$ dans $\mathbb{F}_q$. Mais cette équation a au plus $\ell^{s'}$ solution, d'où une contradiction. Comme Q est abélien, il est produit direct de ses Sylow et la conclusion résulte alors du lemme Chinois.

(4) Déjà Q est un quotient abélien de G donc, par la propriété universel de l'abélianisé on a une factorisation

$$G \twoheadrightarrow G^{ab} \twoheadrightarrow Q,$$

ce qui montre que $D(G)$ est contenu dans le noyau $\ker(G \twoheadrightarrow Q) = N$. Inversement, calculons le commutateur $[(1,1),(0,a)]$:

$$[(1,1),(0,a)] = (1,1)(0,a)(-1,1)(0,a^{-1}) = (1-a,1)$$

Ce qui montre que $N = D(G)$. Choisissons un générateur x de $\mathbb{F}_q^\times$. Les représentations irréductibles de dimension 1 de G sont donc les morphismes

$$\begin{array}{rccc} \chi_i\colon & N \rtimes Q & \to & \mathbb{C}^\times \\ & (b, x^k) & \to & \zeta_{q-1}^{ik}, \end{array}$$

où ζ_{q-1} est une racine primitive $(q-1)$-ème de l'unité.

(5) On identifie N à $(\mathbb{Z}/p)^{\oplus r}$ en choisissant une $\mathbb{F}_p$-base $e_1, \ldots, e_r$. Les représentations irréductibles de N sont alors les morphismes de groupes

$$\begin{array}{rccc} \chi_{i_1,\ldots,i_r}\colon & N & \to & \mathbb{C}^\times \\ & (a_1,\ldots,a_r) & \to & \zeta_p^{\sum_{1\le k\le r} i_k a_k}, \end{array}$$

où ζ_p est une racine primitive p-ème de l'unité.
Considérons la base $a \otimes 1$, $a \in Q$ de $\mathbb{C}[G] \otimes_{\mathbb{C}[N]} (\mathbb{C}, \chi_{i_1,\ldots,i_r})$ Alors, par définition de l'induite

$$(b', a') \cdot a \otimes 1 = \chi_{i_1,\ldots,i_r}(b') a' a \otimes 1.$$

Donc $\mathrm{Ind}_N^G(\chi_{i_1,\ldots,i_r})(b', a') = 0$ si $a' \neq 1$ et $\mathrm{Ind}_N^G(\chi_{i_1,\ldots,i_r})(b', 1) = (q-1)\chi_{i_1,\ldots,i_r}(b')$.

(6) Notons $\chi := \mathrm{Ind}_N^G(\chi_{i_1,\ldots,i_r})$. On a

$$(\chi,\chi)_G = \frac{1}{q(q-1)} \sum_{(a_1,\ldots,a_r)\in(\mathbb{Z}/p)^{\oplus r}} (q-1)\zeta_p^{i_1a_1+\cdots+i_ra_r}\zeta_p^{-i_1a_1-\cdots-i_ra_r} = \frac{1}{q} \sum_{(a_1,\ldots,a_r)\in(\mathbb{Z}/p)^{\oplus r}} 1 = 1$$

donc les représentations $\mathrm{Ind}_N^G(\mathbb{C}, \chi_{i_1,\ldots,i_r})$ sont irréductibles. Comme elles sont de dimension $q-1$, l'égalité

$$|G| = (q-1) \times 1^2 + (q-1)^2$$

montre qu'elles sont toutes isomorphes et que les représentations irréductibles de G sont exactement ses représentations de dimension 1 et l'une (n'importe laquelle) des induites $\mathrm{Ind}_N^G(\mathbb{C}, \chi_{i_1,\ldots,i_r})$.

Exercice 2

(1) Supposons que V s'écrive comme réunion de r sous $\mathbb{C}$-espaces vectoriels stricts $V_1, \ldots, V_r \subset V$Pour chaque $i = 1, \ldots, r$ choisissons un hyperplan $H_i := \ker(f_i)$ contenant V_i. Ici $f_i \in V^\vee$ donc on peut l'écrire

$$f_i = \sum_{1\le j\le n} a_{i,j} e_j^\vee.$$

En identifiant V à $\mathbb{C}^n$ au moyen de la $\mathbb{C}$-base $e_1, \ldots, e_n$ on voit que la fonction polynomiale $k^n \to k$

$$\prod_{1\le i\le r} \sum_{1\le j\le n} a_{i,j} x_j$$

est nulle. En substituant X^j à X_j, on en déduit en particulier que la fonction polynomiale $k \to k$

$$\prod_{1\le i\le r} \sum_{1\le j\le n} a_{i,j} x^j$$

est nulle. Ce qui est impossible puisque le polynôme

$$\prod_{1\le i\le r} \sum_{1\le j\le n} a_{i,j} X^j \in \mathbb{C}[X]$$

ne l'est pas et que $\mathbb{C}$ est infini.

(2) Comme (V,θ) est fidèle, pour tout $e_G \neq g_v \in G$ le sous $\mathbb{C}$-espace vectoriel $V_g := \ker(g_v - Id_V) \subsetneq V$ est strict donc d'après (1) on a

$$\bigcup_{e_G \neq g \in G} V_g \subsetneq V.$$

(3) On introduit le morphisme de $\mathbb{C}$-espaces vectoriels

$$\begin{array}{rccc} \Phi_v\colon & S(V^\vee) & \to & \mathbb{C}[G] \\ & e_1^{\vee\alpha_1}\cdots e_n^{\vee\alpha_n} & \to & \sum_{g\in G}(e_1^{\vee\alpha_1}\cdots e_n^{\vee\alpha_n})(gv)g \end{array}$$

(a) Par $\mathbb{C}$-linéarité, il suffit de le vérifier sur les éléments de la base $e_1^{\vee\alpha_1}\cdots e_n^{\vee\alpha_n}$, $\underline{\alpha} \in \mathbb{Z}^n_{\geq 0}$. Or, pour tout $g_0 \in G$

$$\Phi_v(g_0 \cdot e_1^{\vee\alpha_1}\cdots e_n^{\vee\alpha_n}) = \Phi_v(e_1^{\vee\alpha_1}\cdots e_n^{\vee\alpha_n}(g_0^{-1}-)) = \sum_{g\in G}(e_1^{\vee\alpha_1}\cdots e_n^{\vee\alpha_n})(g_0^{-1}gv)g$$

et le changement de variables $\gamma = g_0^{-1}g$ nous donne bien

$$\sum_{g\in G}(e_1^{\vee\alpha_1}\cdots e_n^{\vee\alpha_n})(g_0^{-1}gv)g = g_0 \cdot \Phi_v(e_1^{\vee\alpha_1}\cdots e_n^{\vee\alpha_n}).$$

(b) Par $\mathbb{C}$-linéarité, il suffit de montrer que les éléments $g \in \mathbb{C}[G]$ sont dans l'image de Φ_v. Or d'après (2), les éléments gv, $g \in G$ sont deux à deux distincts. Ecrivons donc $G = \{g_1, \ldots, g_N\}$ et

$$g_i v = \sum_{1\leq j\leq n} a_{i,j}e_j.$$

Pour chaque $1 \leq i_0 \neq i \leq N$ il existe $1 \leq j(i) \leq n$ tel que $a_{i_0,j(i)} \neq a_{i,j(i)}$. Introduisons donc

$$P_{i_0} = \prod_{1\leq i\neq i_0\leq N}(X_{j(i)} - a_{i,j(i)}) / \prod_{1\leq i\neq i_0\leq N}(a_{i_0,j(i)} - a_{i,j(i)})$$

Par construction on a

$$\Phi_v(P_{i_0}(e_1^\vee, \cdots, e_n^\vee)) = g_{i_0}.$$

(4) On sait que

$$\mathbb{C}[G] = \bigoplus_{(W,\tau)\in\widehat{\mathbb{C}[G]}} (W,\tau)^{\oplus n_\tau}$$

comme $\mathbb{C}[G]$-modules (où $n_\tau = \dim(W)$)). En particulier, les projections fournissent des morphismes surjectifs de $\mathbb{C}[G]$-modules

$$\mathbb{C}[G] \twoheadrightarrow (W,\tau).$$

En composant avec Φ_v, on obtient un morphisme surjectif de $\mathbb{C}[G]$-modules

$$S(V^\vee) \twoheadrightarrow (W,\tau)$$

donc il existe $d_{\tau\geq 0}$ tel que $S(V^\vee) \twoheadrightarrow (W,\tau)$ induise par restriction un morphisme $\mathbb{C}[G]$-modules non nul

$$S_{d_\tau}(V^\vee) \to (W,\tau).$$

Comme (W,τ) est irréductible, ce morphisme est automatiquement surjectif par le lemme de Schur.

(5) Comme on travaille sur $\mathbb{C}$, tout $\mathbb{C}[G]$-module est semisimple. En particulier, il existe un sous $\mathbb{C}[G]$-module $\tilde{W} \subset S_{d_\tau}(V^\vee)$ tel que

$$S_{d_\tau}(V^\vee) = \tilde{W} \oplus \ker(S_{d_\tau}(V^\vee) \twoheadrightarrow (W,\tau)).$$

Par construction, $\tilde{W}$ est isomorphe à (W,τ) comme $\mathbb{C}[G]$-module.

anna.cadoret@math.polytechnique.fr
Centre de Mathématiques Laurent Schwartz - Ecole Polytechnique,
91128 PALAISEAU, FRANCE.