**Examen Algèbre 1**
**18 janvier 2017 - 3 heures**

Le polycopié 2016-2017 du cours est autorisé. Les résultats du cours (hors Remarques) peuvent être utilisés sans être redémontrés.

**A. Caractères du groupe dicyclique d'ordre 12.**
Soit $G$ un groupe d'ordre 12. Soit $S_2$ (resp. $S_3$) un 2-sous-groupe (resp. un 3-sous-groupe) de Sylow de $G$.
**A.1** Si $S_2$ et $S_3$ sont normaux dans $G$, décrire $G$ à isomorphisme près.
**A.2** Si $S_3$ n'est pas normal dans $G$, montrer que $G$ est isomorphe au groupe alterné $A_4$.
**A.3** Si $S_2$ n'est pas normal dans $G$, montrer qu'il existe exactement deux classes d'isomorphismes de groupes d'ordre 2 données par le groupe diédral $D_6$ et le groupe dit dicyclique admettant la présentation par deux générateurs $a, b$ et 3 relations

$$a^3 = b^4 = 1, bab^{-1} = a^2.$$

**A.4** Donner tous les groupes d'ordre 12 à isomorphisme près.

Dorénavant, nous supposons que $G$ est le groupe dicyclique.
**A.5** Quel est le centre de $G$ ? Quel est le groupe dérivé de $G$ ? En déduire les représentations complexes irréductibles de dimension 1 de $G$.
**A.6** Exhiber toutes les classes de conjugaison de $G$.
**A.7** Combien le groupe $G$ admet-il de représentations à valeurs complexes irréductibles non équivalentes ? Quelles sont leurs dimensions ?
**A.8** Déterminer les trois 2-sous-groupes de Sylow de $G$. Montrer que l'action de $G$ par conjugaison sur ses 2-sous-groupes de Sylow définit une représentation $\rho$ de $G$.
**A.9** Donner le caractère de $\rho$. La représentation $\rho$ est-elle irréductible ?
**A.10** En déduire la table des caractère de $G$.

**A.11** Montrer que les deux matrices suivantes

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

engendrent un sous-groupe $H$ du sous-groupe spécial unitaire complexe $\mathrm{SU}(2, \mathbf{C})$ isomorphe à $G$.
**A.12** Montrer que $H$ définit une représentation de $G$ de dimension 2. Quel est son caractère ?

**B. Représentations de** $\mathrm{GL}_2(\mathbb{F}_p)$.

Soit $p > 2$ un nombre premier, nous notons, $\mathbb{F}_p$ le corps à $p$ éléments, $\mathbb{F}_p^*$ le groupe de ses éléments inversibles et $\mathrm{GL}_2(\mathbb{F}_p)$ le groupe linéaire de dimension 2 à coefficients dans $\mathbb{F}_p$.

**B.1** Montrer que les éléments

$$\begin{pmatrix} x & \varepsilon \\ 0 & x \end{pmatrix}, x \in \mathbb{F}_p^*, \varepsilon \in \{0,1\}$$

définissent $2(p-1)$ classes de conjugaison distinctes de $\mathrm{GL}_2(\mathbb{F}_p)$. Quel est le cardinal de chacune d'entre elle ?

**B.2** Soient $x, y$ deux éléments non nuls de $F_p$. Combien d'éléments appartiennent à la classe de conjugaison de

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}, x, y \in \mathbb{F}_p^*, x \neq y \text{ ?}$$

**B.3** Soit $\eta \in \mathbb{F}_p - \mathbb{F}_p^2$ un élément de $\mathbb{F}_p$ qui n'est pas un carré. Combien d'éléments appartiennent à la classe de conjugaison de

$$\begin{pmatrix} x & \eta y \\ y & x \end{pmatrix}, x \in \mathbb{F}_p, y \in \mathbb{F}_p^* \text{ ?}$$

Combien de classes de conjugaison distinctes de $\mathrm{GL}_2(\mathbb{F}_p)$ admettent-elles un représentant de cette forme ?

**B.4** En déduire une famille de représentants des classes de conjugaison de $\mathrm{GL}_2(\mathbb{F}_p)$.

**B.5** Déterminer les représentations complexes de dimension 1 de $\mathrm{GL}_2(\mathbb{F}_p)$.

**B.6** Soit $B$ le sous-groupe de $\mathrm{GL}_2(\mathbb{F}_p)$ des matrices triangulaires supérieures. Quel est le cardinal de $B$ ? Quel est le groupe dérivé $D(B)$ de $B$ ?

**B.7** Soit $\lambda : B \longrightarrow \mathbb{C}^*$ l'homomorphisme complexe défini par

$$\lambda \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \lambda_1(a)\lambda_2(c)$$

pour $\lambda_1, \lambda_2 : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*$. Quelle est la dimension de la représentation induite

$$\rho = \mathrm{Ind}_B^G \lambda \text{ ?}$$

**B.8** Calculer le caractère de la représentation $\rho$.

**B.9** Si $\lambda_1 = \lambda_2$, montrer que $\rho$ est la somme de deux représentations irréductibles dont on déterminera les dimensions.

**B.10** Si $\lambda_1 \neq \lambda_2$, montrer que $\rho$ est irréductible.

**C. Groupe symplectique sur $\mathbb{F}_2$.**
Soit $\nu \geq 2$.
**C.1** Soit $b$ une forme symplectique -alternée non dégénérée- sur un $\mathbb{F}_2$-espace vectoriel de dimension $2\nu$. Montrer qu'il existe une base dans laquelle la matrice de $b$ s'écrit

$$J_{2\nu} = \begin{pmatrix} 0 & I_\nu \\ I_\nu & 0 \end{pmatrix}.$$

Nous notons alors

$$\mathrm{Sp}(2\nu, \mathbb{F}_2) = \{M \in \mathrm{GL}_{2\nu}(\mathbb{F}_2) | M^t J_{2\nu} M = J_{2\nu}\}$$

et $\mathrm{PSp}(2\nu, \mathbb{F}_2)$ le quotient de $\mathrm{Sp}(2\nu, \mathbb{F}_2)$ par son centre.
**C.2** Quel est l'ordre de $\mathrm{PSp}(2\nu, \mathbb{F}_2)$ ?

Soit $E$ un ensemble à $2\nu + 2$ éléments et $S_E$ le groupe de ses permutations. Soit $P$ l'ensemble de toutes les parties $A$ de $E$ telles que le cardinal $|A|$ est pair. Pour $A, A'$ deux parties de $E$, nous notons

$$A + A' = (A \cup A') - (A \cap A').$$

**C.3** Montrer que $P$ est muni d'une structure de groupe abélien. Notons $V$ le quotient de $P$ par le sous-groupe $H =< E >$. Montrer que $V$ peut être muni d'une structure de $\mathbb{F}_2$-espace vectoriel de dimension $2\nu$.
**C.4** En déduire un morphisme injectif de groupes

$$\iota : S_E \longrightarrow \mathrm{GL}(V).$$

**C.5** Munir $V$ d'une structure symplectique. En déduire que $\mathrm{Sp}(2\nu, \mathbb{F}_2)$ contient un sous-groupe isomorphe au groupe des permutations d'un ensemble à $2\nu + 2$ éléments.
**C.6** En déduire que $\mathrm{PSp}(4, \mathbb{F}_2)$ n'est pas simple.

**Correction**

**A. Caractères du groupe dicyclique d'ordre 12**.
**A.1** Tous les sous-groupes de Sylow de $G$ sont normaux, donc $G$ est produit direct de ses sous-groupes de Sylow. Ici $S_3$ est d'ordre 3 donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et $S_2$ est d'ordre $4 = 2^2$ donc abélien. Il y a donc deux classes d'isomorphismes :

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \text{ et } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

**A.2** Si $S_3$ n'est pas normal, le nombre des 3-sous-groupes de Sylow de $G$ vaut 4. L'action de $G$ par conjugaison sur ses 3-sous-groupes de Sylow induit un morphisme de groupes $\varphi : G \longrightarrow \mathfrak{S}_4$. Le noyau de $\varphi$ est l'intersection des stabilisateurs de chaque 3-sous-groupe de Sylow. Comme l'action de $G$ est transitive, le stabilisateur d'un 3-sous-groupe de Sylow $S$ est d'ordre $|G|/4 = 3$ et contient $S$ donc coïncide avec $S$. Donc le noyau de $\varphi$ est réduit à l'élément neutre de $G$ et $\varphi$ est injectif. Par conséquent $G$ est un sous-groupe d'indice 2 (donc normal) de $\mathfrak{S}_4$. Donc $G$ est isomorphe à $A_4$.
**A.3** Si $S_2$ n'est pas normal alors $S_3$ est normal. En effet sinon $G$ possède 8 éléments d'ordre 3, donc au plus 3 éléments d'ordre différents de 1 et 3, et par conséquent un unique 2-sous-groupe de Sylow qui est normal.
Ainsi $G$ est produit semi-direct (non direct) du 3-sous-groupe normal de Sylow $S_3 = \mathbb{Z}/3\mathbb{Z}$ et de $S_2$. Il est défini par un morphisme non trivial

$$\tau : S_2 \to \operatorname{Aut} \mathbb{Z}/3\mathbb{Z}$$

Si $S_2 = \mathbb{Z}/4\mathbb{Z}$, $G$ est donc isomorphe au groupe dicyclique, si $S_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $G$ est isomorphe au groupe diédral $D_6$.
**A.4** D'après les questions **A 1-3**, si $G$ est un groupe d'ordre 12, alors, il est isomorphe à un groupe abélien $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ ou $\mathbb{Z}/12\mathbb{Z}$, au groupe alterné $A_4$, au groupe diédral $D_6$ ou au groupe dicyclique.
**A.5** Le centre de $G$ est $< b^2 >$, le sous-groupe dérivé de $G$ est $< a >$. Ceci induit quatre représentations irréductibles complexes de dimension 1 déterminées par l'image de $b$, qui doit être une racine 4-ième de l'unité.
**A.6** Les classes de conjugaison des éléments qui n'appartiennent pas au centre sont :

$$\{a, a^2\}, \{ab^2, a^2b^2\}, \{b, ab, a^2b\}, \{b^3, ab^3, a^2b^3\}.$$

Donc $G$ admet 6 classes de conjugaison.
**A.7** Ainsi $12 = 1+1+1+1+2^2+2^2$ est la seule façon d'écrire 12 comme la somme de six carrés dont 4 égaux à 1. Donc $G$ admet six représentations irréductibles complexes, quatre de dimension 1 et deux de dimension 2.
**A.8-9** Le groupe $G$ a trois sous-groupes de 2-Sylow :

$$S_1 =< b >, S_2 = \{1, b^2, ab, ab^3\}, S_3 = \{1, b^2, a^2b, a^2b^3\}.$$

L'étude de la représentation $\rho$ définie par conjugaison sur les trois 2-sous-groupes de Sylow, conduit au caractère $\chi_3$ :

| G | 1 | $(b^2)$ | $(a)_2$ | $(ab^2)_2$ | $(b)_3$ | $(b^3)_3$ |
|---|---|---|---|---|---|---|
| $\chi_3$ | 3 | 3 | 0 | 0 | 1 | 1 |

Comme $< \chi_3, \chi_3 >= 2 = 1 + 1$, nous en déduisons $\chi_3 = \chi_2 + \mathrm{triv}$, où $\chi_2$ est irréductible de degré 2.

**A.10** Le second caractère de degré 2 se déduit de $\chi_2$ par tensorisation avec un caractère de degré 1 (nous pouvons aussi l'obtenir par passage au quotient à partir du caractère de degré 2 de $D_3 = G/Z(G)$). La table des caratères de $G$ est donc

| $G$ | 1 | $(b^2)$ | $(a)_2$ | $(ab^2)_2$ | $(b)_3$ | $(b^3)_3$ |
|---|---|---|---|---|---|---|
| $\chi_{\mathrm{triv}}$ | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_1$ | 1 | 1 | 1 | 1 | -1 | -1 |
| $\chi_1'$ | 1 | -1 | 1 | -1 | i | -i |
| $\chi_1''$ | 1 | -1 | 1 | -1 | -i | i |
| $\chi_2$ | 2 | 2 | -1 | -1 | 0 | 0 |
| $\chi_2'$ | 2 | -2 | -1 | 1 | 0 | 0 |

**A.11** Nous pouvons vérifier que le sous-groupe du groupe spéciale unitaire $\mathrm{SU}_2$ engendré par les deux matrices

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

est isomorphe à $G$.

**A.12** La repésentation de $G$ de dimension 2 ainsi définie a pour caractère $\chi_2'$.

**B. Représentations de** $\mathrm{GL}_2(\mathbb{F}_p)$.

**B.1** Le centre de $\mathrm{GL}_2(\mathbb{F}_p)$ est composé des matrices scalaires qui définissent $p-1$ classes de conjugaison distinctes de $\mathrm{GL}_2(\mathbb{F}_p)$ réduites à 1 éléments.

Les éléments qui commutent avec

$$T_x = \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix}$$

sont les $p(p-1)$ éléments de la forme

$$\begin{pmatrix} u & v \\ 0 & u \end{pmatrix}, u \neq 0$$

Donc le nombre d'éléments dans la classe de conjugaison de $T_x$ est

$$|\,\mathrm{GL}_2(\mathbb{F}_p)|/p(p-1) = p^2 - 1.$$

Si $x \neq x'$, $T_x$ et $T_{x'}$ ne sont pas dans la même classe de conjugaison, ils définissent donc $p-1$ classes distinctes.

**B.2** Les éléments qui commutent avec

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}, x \neq y, xy \neq 0$$

sont les $(p-1)^2$ éléments de la forme

$$\begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix}, uv \neq 0.$$

Nous obtenons ainsi $\frac{1}{2}(p-1)(p-2)$ classes différentes (deux matrices diagonales sont semblables si si seulement si elles ont les mmes valeurs propres) chacune de cardinal $p^2+p$.

**B.3** Les éléments de la forme

$$\begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix}, y \neq 0$$

ne sont pas trigonalisables donc ne sont pas dans les classes de conjugaison précédentes. Ils commutent avec les $p^2-1$ éléments de la forme

$$\begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix},$$

donc définissent $p(p-1)/2$ classes de conjugaison distinctes de cardinal $p^2-p$.

**B.4** La réunion des classes de conjugaison décrites dans les questions **B.1-3** contient les

$$(p-1)+(p-1)(p^2-1)+\frac{1}{2}(p-1)(p-2)(p^2+p)+\frac{1}{2}p(p-1)(p^2-p) = (p^2-1)(p^2-p)$$

éléments de $\mathrm{GL}_2(\mathbb{F}_p)$. Par conséquent, nous les avons toutes décrites. Nous avons donc une famille de représentants des classes de conjugaison de $\mathrm{GL}_2(\mathbb{F}_p)$ :

- $\begin{pmatrix} x & \varepsilon \\ 0 & x \end{pmatrix}, \varepsilon \in \{0,1\}, x \in \mathbb{F}_p^*$,
- $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}, x \neq y, x, y \in \mathbb{F}_p^*$,
- $\begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix}, y \in \mathbb{F}_p^*, x \in \mathbb{F}_p$.

**B.5** Le groupe dérivé de $\mathrm{GL}_2(\mathbb{F}_p)$ est $\mathrm{SL}_2(\mathbb{F}_p)$ ; ainsi

$$G/[G,G] \xrightarrow{\simeq} \mathbb{F}_p^*, \ g \mapsto \det g.$$

Les représentations de $\mathrm{GL}_2(\mathbb{F}_p)$ de dimension 1 sont donc de la forme

$$\rho_\tau(g) = \tau(\det(g)), g \in \mathrm{GL}_2(\mathbb{F}_p)$$

pour $\tau : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*$ un homomorphisme. Nous obtenons donc $p-1$ représentations complexes de $\mathrm{GL}_2(\mathbb{F}_p)$ de dimension 1.

**B.6** Le cardinal de $B$ est $|B| = p(p-1)^2$ et

$$D(B) = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}.$$

**B.7** Pour alléger les notations, nous notons $G = \mathrm{GL}_2(\mathbb{F}_p)$. La dimension de $\rho = \mathrm{Ind}_B^G \lambda$ est $|G|/|B| = p+1$.

**B.8** Le caractère de la représentation induite est donné par

$$\chi(g) = \frac{1}{|B|} \sum_{g' \in G, g'^{-1}gg' \in B} \lambda(g'^{-1}gg'), g \in G.$$

Pour $g = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$, $g'^{-1}gg' \in B$ implique $g' \in B$, donc

$$\chi(g) = \lambda_1(x)\lambda_2(x).$$

Pour $g = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$, $g'^{-1}gg' \in B$ implique $g' \in B$ ou $g'$ est le multiple d'un élément de $B$ et d'une transposition, donc

$$\chi(g) = \lambda_1(x)\lambda_2(y) + \lambda_1(y)\lambda_2(x).$$

Pour $g = \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix}$, $x \neq y$, $y \neq 0$, alors pour tout $g' \in B$, $g'^{-1}gg' \notin B$, donc

$$\chi(g) = 0.$$

Comme $\chi$ est constant sur les classes de conjugaison, les calculs précédents déterminent $\chi(g)$ pour tout $g \in G$.
**B.8** D'après **B.7**, nous avons

$$\begin{aligned} < \chi, \chi >= & \tfrac{1}{|G|}\Big((p+1)^2(p-1) + (p^2-1)(p-1) \\ & +(p^2+p)\textstyle\sum_{x \neq y}(\lambda_1(x)\lambda_2(y) + \lambda_1(y)\lambda_2(x))(\overline{\lambda_1(x)\lambda_2(y) + \lambda_1(y)\lambda_2(x)})\Big) \end{aligned}$$

$$\begin{aligned} < \chi, \chi >= & \tfrac{1}{|G|}\Big(2(p^2+p)(p-1) + 2(p^2+p)\tfrac{1}{2}(p-1)(p-2) \\ & +(p^2+p)\textstyle\sum_{x \neq y} \lambda_1(x)\lambda_2(y)\overline{\lambda_1(y)\lambda_2(x)}\Big). \end{aligned}$$

$$< \chi, \chi >= \frac{1}{(p^2-p)(p^2-1)}(p^2+p)\Big((p-1)p + \sum_{x \neq y} \lambda_1(x)\lambda_2(y)\overline{\lambda_1(y)\lambda_2(x)}\Big).$$

**B.9** Si $\lambda_1 = \lambda_2 = \lambda$, alors

$$\sum_{x \neq y} \lambda(x)\lambda(y)\overline{\lambda(y)\lambda(x)} = (p-1)(p-2)$$

et

$$< \chi, \chi >= \frac{1}{(p-1)^2}\Big((p-1)p + (p-1)(p-2)\Big) = 2.$$

Donc $\rho = \rho_\lambda \oplus W_\lambda$ est la somme de deux représentations irréductibles avec $\rho_\lambda$ de dimension 1 (voir **B.5**). Comme $\rho$ est de dimension $p+1$, $W_\lambda$ est de dimension $p$.
**B.10** Si $\lambda_1 \neq \lambda_2$, alors en posant $z = xy^{-1}$, nous obtenons

$$\sum_{x \neq y} \lambda_1(x)\lambda_2(y)\overline{\lambda_1(y)\lambda_2(x)} = (p-1)\sum_{z \neq 1} \frac{\lambda_1}{\lambda_2}(z)$$

Or $\sum_{x\in\mathbb{F}_p^*}\frac{\lambda_1}{\lambda_2}(x)=0$, car il s'agit de la somme de toutes les racines de l'unité d'un ordre donné. D'où,

$$(p-1)\sum_{z\neq 1}\frac{\lambda_1}{\lambda_2}(z)=-(p-1)\frac{\lambda_1}{\lambda_2}(1)=-(p-1).$$

D'où

$$<\chi,\chi>=\frac{1}{(p-1)^2}\Big((p-1)p-(p-1)\Big)=1.$$

Donc $\rho$ est irréductible.

**C. Groupe Symplectique sur $\mathbb{F}_2$.**

**C.1** Soit $V$ un espace vectoriel de dimension $2\nu$ sur $\mathbb{F}_2$. Alors $V$ se décompose en somme directe orthogonale de plans hyperboliques :

$$V=P_1\oplus\cdots\oplus P_\nu.$$

Par conséquent à isométrie près, il n'y a qu'une seule forme alternée non dégénérée sur $V$.
En prenant des paires hyperboliques engendrant les plans hyperboliques $P_i$, nous obtenons une base dans laquelle la matrice de $b$ est $J_{2\nu}$.
**C.2** Le cardinal $|\mathrm{PSp}(2\nu,\mathbb{F}_2)|=|\operatorname{Sp}(2\nu,\mathbb{F}_2)|=2^{\nu^2}\prod_{j=1}^{\nu}(2^{2j}-1)$.
**C.3** L'ensemble $V$ est muni d'une structure d'espace vectoriel via la multiplication scalaire canonique et l'addition sur les parties (les deux représentants dans $P$ d'un élément $[A]$ de $V$ est la partie $A$ et son complémentaire). Le cardinal de $V$ est $2^{2\nu}$ donc $V$ est de dimension $2\nu$ sur $\mathbb{F}_2$.
**C.4** Le groupe $S_E$ agit sur $V$ via $g[A]=[gA]$ pour $g\in S_E$ et $A\in P$. Cette action induit un morphisme de groupes injectif

$$\iota : S_E\longrightarrow \mathrm{GL}(V).$$

**C.5** La forme

$$b:V^2\longrightarrow\mathbb{F}_2,\ \ b([A],[B])\mapsto|A\cap B|\mod 2$$

est bien définie, alternée non dégénérée donc symplectique. L'image de $\iota$ est un sous-groupe isomorphe à $S_E$ inclus dans $\mathrm{Sp}(V,b)$. Donc $\mathrm{Sp}(2\nu,\mathbb{F}_2)$ contient un sous-groupe isomorphe au groupe des permutations d'un ensemble à $2\nu+2$ éléments.
**C.6** $\mathrm{PSp}(4,\mathbb{F}_2)\simeq\mathrm{Sp}(4,\mathbb{F}_2)$ est de cardinal 6! et contient un sous-groupe isomorphe à $\mathfrak{S}_6$. Donc $\mathrm{PSp}(4,\mathbb{F}_2)\simeq\mathfrak{S}_6$ qui n'est pas simple.

**Remarque** Pour E ensemble des points de Weierstrass d'une courbe hyperelliptique, $V$ est le noyau de la multiplication par 2 sur la jacobienne de la courbe et la forme $b$ correspond à l'accouplement de Weil.