Examen M1-Algèbre Janvier 2017.

1

Pb 1.

1) Le nombre n_{11} de 11-Sylow vérifie $n_{11} \mid 3$ et $n_{11} \equiv 1\ [11]$. Donc $n_{11} = 1$. De m., $n_3 \equiv 1\ [3]$ et $n_3 \mid 11$ donc $n_3 = 1$.
On a donc un 11-Sylow S_{11} distingué et un 3-Sylow distingué, S_3.
On a, par le théorème des PSD que le groupe H est isomorphe à
$S_{11} \times S_3 \simeq \mathbb{Z}/_{11\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}} \simeq \mathbb{Z}/_{33\mathbb{Z}}$ par le lemme chinois.

2) De m. le nombre n_{11} de 11-Sylow de G vérifie $n_{11} \mid 6$ et $n_{11} \equiv 1\ [11]$, donc $n_{11} = 1$ et G contient un unique 11-Sylow, d'ordre 11, et donc distingué.

3) Le groupe quotient est d'ordre $66/_{11} = 6$. Il possède donc un 3-Sylow, d'ordre 3 et distingué, appelons le N_0.
Soit π la projection canonique de $G \twoheadrightarrow G/_M$ et $N = \pi^{-1}(N_0)$
Comme N_0 est distingué dans $G/_M$, N est distingué dans G.
De plus, il est clair que N contient $\ker \pi = M$. Donc le morphisme π_N :
$\pi^{-1}(N_0) = N \longrightarrow N_0$, vérifie $|N|/_{|\ker \pi_N|} \simeq |\mathrm{Im}\, \pi_N|$,
ce qui implique, par surjectivité (de π) : $|N| = |M| \times 3 = 11 \times 3 = 33$.

4) (*)

5) Le sous groupe N est d'indice $\frac{66}{33} = 2$ dans G. Il est distingué et donc, le théorème des PSD donne $G \simeq N \rtimes \mathbb{Z}/_{2\mathbb{Z}}$, avec $N \simeq \mathbb{Z}/_{33\mathbb{Z}}$, par 1), et $\mathbb{Z}/_{2\mathbb{Z}}$ représenté par un 2-Sylow de G.

(*) D'après 1), N possède un unique ss groupe K d'ordre 3, car $|N| = 33$.
Soit S_3 un 3-Sylow de G. Alors, par un théorème de Sylow, $\exists g \in G$ tq $K = g S_3 g^{-1}$. Or, comme N est distingué dans G, on a

que $S_3 = g^{-1}Kg \subset N$. Par unicité, $S_3 = K$. Donc G possède un unique 3-Sylow (et celui-ci est distingué).

6) a) $\text{Aut}(\mathbb{Z}/33\mathbb{Z}) \simeq \mathbb{Z}/33\mathbb{Z}^* \simeq (\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})^*$

$$\simeq \mathbb{Z}/11\mathbb{Z}^* \times \mathbb{Z}/3\mathbb{Z}^* \simeq \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

b) Compter les éléments d'ordre 2 dans $\text{Aut}(\mathbb{Z}/33\mathbb{Z})$ revient à compter les éléments d'ordre 2 dans $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il y en a un dans $\mathbb{Z}/10\mathbb{Z}$, disons a et un dans $\mathbb{Z}/2\mathbb{Z}$ disons b (en fait $a=5$ et $b=1$). Les éléments d'ordre 2 sont donc $(0,b), (a,0), (a,b)$. Il y en a 3.

c) Les morphismes de $\mathbb{Z}/2\mathbb{Z}$ dans $\text{Aut}(\mathbb{Z}/33\mathbb{Z})$ doivent envoyer $\bar{1}$ sur un élément annulé par 2, donc le neutre ou un des 3 éléments d'ordre 2.
Ces morphismes sont entièrement déterminés par l'image de $\bar{1}$, on a donc déterminé les 4 morphismes possibles.

Pb 2. 1) On suppose que P se réduit en $P = QR$.

Soit q_d, resp. $r_{d'}$, le coefficient dominant de Q, resp. de R.
Alors $q_d r_{d'} = a_n \Rightarrow \overline{q_d}\,\overline{r_{d'}} = \overline{a_n} \neq \overline{0}$ dans $\mathbb{Z}/_{p}\mathbb{Z}$. Comme p est premier, il en résulte que $\overline{q_d} \neq 0$ et $\overline{r_{d'}} \neq 0$ et donc $\overline{Q}$ et $\overline{R}$ sont de degré respectifs d et d'.
Comme $\overline{P} = \overline{Q}\,\overline{R}$, l'irréductibilité de $\overline{P}$ implique $d = \deg(\overline{Q}) = 0$ ou $d' = \deg(\overline{R}) = 0$. Ce qui implique que P est irréductible car $d = \deg Q$ et $d' = \deg(R)$.

2) $\overline{X^3 - X + 2} = X^3 - X - 1 \mod 3$.

Or, ce polynôme est de degré 3 et ne possède pas de racine dans $\mathbb{Z}/_{3}\mathbb{Z}$. Donc il est irréductible. Ceci implique que $X^3 - X + 2$ est irréductible dans $\mathbb{Z}$, par 1).

3) Soit $Y = X - 1$ et ϕ' le polynôme tel que $\phi'(Y) = \phi(X)$. On a donc clairement ϕ irréd sur $\mathbb{Z}$ $\Leftrightarrow$ ϕ' irréd sur $\mathbb{Z}$.

$$\phi(X) = X^4 + 1 = (Y+1)^4 + 1 = Y^4 + 4Y^3 + 6Y^2 + 4Y^2 + 2 = \phi'(Y)$$

donc ϕ' est 2-Eisenstein, il est irréductible et ϕ l'est également.

4) Si $p = 2$ $\quad X^4 + 1 = (X+1)^4$ donc $\overline{\phi}$ est réductible.

5) $\mathbb{F}_{p^2}^*$ est d'ordre $p^2 - 1 = (p-1)(p+1)$, et comme $p-1$, $p+1$ sont deux pairs consécutifs, le produit est multiple de $8 = 2 \times 4$.
Donc $\mathbb{F}_{p^2}^*$ est un groupe cyclique d'ordre divisible par 8. Il possède donc un élément d'ordre 8. Or $x^8 = 1$ et $x^4 \neq 1$ $\Rightarrow x^4 = -1$.

6) On en déduit que le corps de rupture de $\overline{\Phi}$ est inclus dans $\mathbb{F}_{p^2}$. Or, si $\overline{\Phi}$ est irréductible, alors son corps de rupture est ~~de~~ degré $\deg \overline{\Phi} = 4$ sur $\mathbb{F}_p$. Absurde. Donc $\overline{\Phi}$ se réduit modulo p, pour tout p.

4

Pb 3 :

1) $D(\mathfrak{S}_n)$ est distingué dans $\mathfrak{S}_n$, de plus, comme il est engendré par des commutateurs, il est dans $\mathcal{A}_n$. Donc $D(\mathfrak{S}_n)$ est distingué dans $\mathcal{A}_n$. Comme $\mathcal{A}_n$ est simple, $D(\mathfrak{S}_n) = e$ ou $\mathcal{A}_n$. Mais dans le premier cas, on aurait $\mathfrak{S}_n$ abélien $(n \geqslant 5)$, c'est impossible.

Donc $D(\mathfrak{S}_n) = \mathcal{A}_n$

Soit $\alpha : \mathfrak{S}_n \longrightarrow \mathbb{C}^*$ une représentation de degré 1.

$D(\mathfrak{S}_n) \subset \operatorname{Ker} \alpha$ car $\mathbb{C}^*$ est abélien.

Par passage au quotient, on voit que α fournit un morphisme de $\mathfrak{S}_n / \mathcal{A}_n \rightarrow \mathbb{C}^*$, c'est à dire de $\mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{C}^*$.

On n'a que 2 tels morphismes.

Donc $\alpha = \mathbb{1}_{Triv}$ ou $\alpha = \varepsilon$.

2) Montrons que $g \longmapsto \varepsilon(g)\varphi(g)$ est une représentation

On a : $\varepsilon(gh)\varphi(gh) = \varepsilon(g)\varepsilon(h)\varphi(g)\varphi(h)$

$= \varepsilon(g)\varphi(g)\,\varepsilon(h)\varphi(h)$, car $\varepsilon(h)$ est un scalaire.

Donc c'est bien un morphisme de groupes.

On peut par exemple montrer l'irréductibilité par les caractères :

$$\langle \varepsilon\varphi, \varepsilon\varphi \rangle_G = \frac{1}{|G|} \sum_{g \in G} \overline{\varepsilon(g)}\,\overline{\varphi(g)}\,\varepsilon(g)\varphi(g) = \left(\sum_{g\in G} \overline{\varphi(g)}\,\varphi(g)\right)\frac{1}{|G|}$$

$= 1$ car φ est irréductible

car $\varepsilon(g) = \pm 1$.

$\mathrm{Tr}\left(\varepsilon(g)\,\varphi(g)\right) = \varepsilon(g)\,\mathrm{Tr}\left(\varphi(g)\right)$ car $\varepsilon(g)$ est un scalaire. Donc $\chi_{\varepsilon\varphi} = \varepsilon\,\chi_\varphi$.

3) Le sous-groupe $\langle \mathcal{A}_n, t\rangle$ engendré par $\mathcal{A}_n$ et t vérifie

$\mathcal{A}_n \subsetneq \langle \mathcal{A}_n, t\rangle \subset \mathcal{S}_n$, car $t \notin \mathcal{A}_n$.

Donc, c'est un sous-groupe d'indice < 2 de $\mathcal{S}_n$.

C'est donc un sous groupe d'indice 1. C'est $\mathcal{S}_n$.

$\mathcal{S}_n$ est la réunion de $\mathcal{A}_n$ et de la classe $\mathcal{A}_n t$

Soit g dans $\mathcal{S}_n$. Si $\boxed{g \in \mathcal{A}_n}$, alors.

$$\rho(g)\left(w + \rho(t)w'\right) = \rho(g)w + \rho(g)\rho(t)w'$$
$$= \rho(g)w + \rho(gt)w'$$

avec $\rho(g)w \in W$ et $\rho(gt)w' = \rho(t\,t^{-1}gt)w'$
$$= \rho(t)\rho(t^{-1}gt)w'$$
$$\in \rho(t)W$$

car $\mathcal{A}_n \lhd \mathcal{S}_n$ et que W est stable par $\mathcal{A}_n$.

$\boxed{\text{Si } g \notin \mathcal{A}_n}$, alors $g = g_0 t$ avec $g_0 \in \mathcal{A}_n$.

$$\rho(g)\left(w + \rho(t)w'\right) = \rho(g_0 t)w + \rho(g_0 t^2)w' = \rho(t\,t^{-1}g_0 t)w + \rho(g_0)w'$$

Or $\rho(g_0)w' \in W$ et $\rho(t\,t^{-1}g_0 t)w = \rho(t)\rho(t^{-1}g_0 t)w \in \rho(t)W$

On a bien la stabilité demandée.

4) Si W est stable par $\rho(t)$ alors, l'ensemble $\{w + \rho(t)w'\}$ est W lui-même. Comme il est stable par $\mathfrak{S}_n$, et que V est irréductible, on a $V = W$.

Si W n'est pas stable par $\rho(t)$, alors, $\rho(t)W \neq W$.
Alors $\rho(t)W \cap W$, qui est stable par $\mathfrak{S}_n$ est forcément nul, car V est irréductible.

Donc $V = W + \rho(t)W = W \oplus \rho(t)W$.

5) a) $\rho'(g)\,\Theta(x)\,\rho'(g)^{-1} = \rho'(g)\rho'(x)\rho'(g^{-1})$

$$= \rho'(gxg^{-1}) = \Theta(gxg^{-1})$$

de m̄ $\rho(g)\,\Theta(x)\,\rho(g)^{-1} = \Theta(gxg^{-1})$

d'où l'égalité.

b) On a donc, que, pour tout g, $\rho'(g)^{-1}\rho(g)$ commute à Θ. Comme Θ est irréductible, le lemme de Schur dit que $\rho'(g)\rho(g)^{-1} = \lambda(g) \in \mathbb{C}$ est un scalaire, forcément non nul.

c) Comme ρ et ρ' sont des morphismes, il vient.

$$\lambda(gh)\rho(gh) = \rho'(gh) = \rho'(g)\rho'(h) = \lambda(g)\rho(g)\lambda(h)\rho(h)$$
$$= \lambda(g)\lambda(h)\rho(g)\rho(h) = \lambda(g)\lambda(h)\rho(gh).$$

et donc $\lambda(gh) = \lambda(g)\lambda(h)$. Donc $\lambda = 1$ ou ε.

6) a) Si $g \in t_n$, alors $\mathrm{Tr}(g|_V) = \mathrm{Tr}(g|_W) + \mathrm{Tr}(g|_{\rho(t)W})$.
Or $\mathrm{Tr}(g|_W) = \chi_\Theta(g)$ et $\mathrm{Tr}(g|_{\rho(t)W}) = \chi_\Theta(t^{-1}gt)$, d'après 3).
Or comme la trace est stable par conjugaison, $\chi_\Theta(t^{-1}gt) = \chi_\Theta(g)$

et donc $\chi_\rho(g) = \chi_\theta(g) + \chi_\theta(g) = 2\chi_\theta(g)$

Soit $g \notin A_n$. On a vu en 3) que g envoie W sur $\rho(t)W$ et $\rho(t)W$ sur W. Donc $\rho(g)$ a une matrice de la forme $\begin{pmatrix} 0 & \boxed{///} \\ \boxed{///} & 0 \end{pmatrix}$, de trace nulle.

b) Si $\rho|_{A_n} = \rho'|_{A_n}$, alors, en posant θ' l'analogue de θ pour ρ', il vient $\theta = \theta'$ et donc
$\chi_\theta = \chi_{\theta'} \Rightarrow 2\chi_\theta = 2\chi_{\theta'} \Rightarrow \chi_\rho = \chi_{\rho'}$ et donc $\rho \simeq \rho'$.

7) On peut, d'après ce qui précède scinder $\mathrm{Irr}\,\mathcal{S}_n$ en deux parties

$(\mathrm{Irr}\,\mathcal{S}_n)_1$ des ρ tq $\rho|_{A_n} \simeq \theta$ est irréductible

$(\mathrm{Irr}\,\mathcal{S}_n)_2$ des ρ tq $\rho|_{A_n} \simeq \theta \oplus \theta$ se scinde en deux irréductibles isomorphes.

D'où une application $f : \mathrm{Irr}\,\mathcal{S}_n \to \mathrm{Irr}\,A_n$ tq $f(\rho) = \theta$

Or, on a vu que f est injective sur $(\mathrm{Irr}\,\mathcal{S}_n)_2$ (par 6 b)).

$f(\rho) = f(\rho') \Rightarrow \rho' = \rho$ ou $\varepsilon\rho$ sur $(\mathrm{Irr}\,\mathcal{S}_n)_1$.

$f^{-1}(\theta)$ a au plus 3 éléments (1 dans $(\mathrm{Irr}\,\mathcal{S}_n)_2$ et 2 dans $(\mathrm{Irr}\,\mathcal{S}_n)_1$).

D'où $b_n \geq \dfrac{a_n}{3}$.

8) Le nombre de classes de conjugaison = nombre d'irréductibles !