Corrigé de l'examen partiel du

Vendredi 12 novembre 2010

Exercice 1 1. (a) Soit H un p-Sylow. Son ordre est la puissance de p maximale divisant $|G|$, donc p. Un p-Sylow est donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$, et il est engendré par n'importe lequel de ses éléments $a \neq 1$. Si deux p-Sylow H_1 et H_2 ont un élément $a \neq 1$ en commun, c'est un générateur pour chacun d'eux. On a donc $H_1 = \langle a \rangle = H_2$. Dans le cas contraire, on a $H_2 \cap H_1 = \{1\}$.

[Mieux : $H_1 \cap H_2$ est un sous-groupe de H_1, donc son ordre divise p. Si c'est p, alors $H_1 \cap H_2 = H_1$, c'est-à-dire $H_1 \subset H_2$. Comme ces deux ensembles ont même cardinal, $H_1 = H_2$. Si au contraire l'ordre est 1, alors $H_1 \cap H_2 = \{1\}$.]

(b) Les éléments $a \neq 1$ des p-Sylow sont d'ordre p. Réciproquement, tout $a \in G$ d'ordre p engendre un sous-groupe $\langle a \rangle$ d'ordre p, c'est-à-dire un p-Sylow. La réunion des p-Sylow regroupe donc 1 et tous les éléments d'ordre p.

Soit n_p le nombre de p-Sylow de G. Puisque les éléments d'ordre p n'appartiennent qu'à un seul p-Sylow, leur nombre est égal au produit de n_p par le nombre $p-1$ d'éléments $a \neq 1$ dans un sous-groupe d'ordre p.

Si $n_p = 1$, l'unique p-Sylow H de G est distingué, car si $g \in G$ alors gHg^{-1} est encore d'ordre p, donc est égal à H. Comme G est simple, on en déduit $G = H$, ce qui contredit l'hypothèse que $|G|$ n'est pas premier. [Attention : même si c'est vrai, il ne sert à rien de dire ici que tous les p-Sylow sont conjugués.]

Donc $n_p > 1$. Comme $n_p \equiv 1$ modulo p, on obtient $n_p \geq p+1$. Finalement, le nombre d'éléments d'ordre p est au moins $(p+1)(p-1) = p^2 - 1$).

2. (a) Le nombre n_r de r-Sylow est $\geq r+1$ et divise pqr, donc pq (car $n_r \equiv 1$ modulo r). Comme $p, q < r$ et les diviseurs de pq sont $1, p, q, pq$, on a donc $n_r = pq$. D'après la première question, [et comme tout élément d'ordre r est dans un r-Sylow (le sous-groupe qu'il engendre),] le nombre d'éléments d'ordre r est $pq(r-1)$.

(b) Il y a au moins $p^2 - 1$ éléments d'ordre p et $q^2 - 1$ d'ordre q, ainsi que l'élément neutre. Sans compter les éléments d'ordre composite pq, etc ..., on a déjà $p^2 - 1 + q^2 - 1 + pq(r-1) + 1$ éléments distincts. On a donc

$$p^2 - 1 + q^2 - 1 + pq(r-1) + 1 \leq pqr,$$

c'est-à-dire

$$p^2 - pq + q^2 \leq 1.$$

Ceci s'écrit aussi $(p - q/2)^2 + 3q^2/4 \leq 1$, ce qui entraine $3q^2 \leq 4$, ce qui est absurde car $q \geq 3$.

Il n'existe donc pas de groupe simple d'ordre pqr avec p, q, r premiers distincts.

3. (a) À nouveau, $n_q \geq q+1$ divise $4p$. Les diviseurs de $4p$ étant $1, 2, 4, p, 2p, 4p$, on en déduit (puisque $q \geq 5$) $n_q = 2p$ ou $4p$. Le nombre d'éléments d'ordre q de G est donc $2p(q-1)$ dans un cas, $4p(q-1)$ dans l'autre.

   (b) Le nombre n_2 de 2-Sylow de G est au moins $2+1 = 3$. Soit A, B, C trois 2-Sylow distincts. Ce sont des groupes d'ordre 4. L'intersection de deux d'entre eux est un 2-groupe strictement plus petit, donc contient au plus deux éléments.

   L'intersection de tous les 2-Sylow est distinguée (valable en remplaçant 2 par un autre nombre premier), car le conjugué d'un 2-Sylow en est un autre. Comme G est simple, cette intersection est réduite à $\{1\}$. On peut donc choisir A, B et C de façon que $A \cap B \cap C = \{1\}$.

   On a alors

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| \\ &\quad + |A \cap B \cap C| \\ &= 3 \cdot 4 - |A \cap B| - |B \cap C| - |C \cap A| + 1 \geq 7. \end{aligned}$$

   Les éléments $a \neq 1$ de $A \cap B \cap C$ sont d'ordre 2 ou 4, et il y en a au moins 6.

   (c) En classant les éléments de G selon leur ordre, on en trouve au moins $n_q(q-1)$ d'ordre q, $p^2 - 1$ d'ordre p, six d'ordre 2 ou 4 et un d'ordre 1, ce qui donne

$$n_q(q-1) + p^2 - 1 + 6 + 1 \leq 4pq.$$

   Si $n_q = 4p$, cela donne $p^2 - 4p + 6 \leq 0$, c'est-à-dire $(p-2)^2 + 2 \leq 0$, ce qui est absurde. Si G est un groupe simple d'ordre $4pq$ avec p, q premiers impairs distincts, on aura donc $n_q = 2p$.

   (d) On suppose donc que $n_q = 2p$. Comme $p \leq q - 2$, on a $n_q \leq 2q - 4$. Comme $n_q \equiv 1$ modulo p et $n_q > 1$, il s'ensuit $n_q = q + 1$. Ceci donne $q = 2p - 1$.

   Comptons maintenant le nombre n_p de p-Sylow. Il est de la forme $kp + 1$ ($k \geq 1$ par simplicité de G) et divise $2q = 4p - 2$. On a donc $k = 1, 2$ ou 3, ce qui donne respectivement $p \leq 1, \frac{3}{2}$ ou 3. La seule possibilité reste donc $p = 3$, auquel cas $q = 2p - 1 = 5$.

   (e) On a montré qu'un groupe simple d'ordre $4pq$ avec p, q premiers impairs distincts ne peut être que d'ordre $4 \cdot 3 \cdot 5 = 60$. D'après le DM d'octobre, l'unique groupe simple d'ordre 60 est $\mathfrak{A}_5$.

Exercice 2 1. Soit $g \in Z(G)$. Si $h \in G$, alors $\rho(g)\rho(h) = \rho(gh) = \rho(hg) = \rho(h)\rho(g)$. On a donc $\rho(g) \in \mathrm{Hom}_G(V)$. D'après le Lemme de Schur, comme V est irréductible, $\rho(g) = \lambda \mathrm{id}_V$. On a $\lambda = \frac{1}{\dim V}\chi_V(g)$.

Comme $\rho(gh) = \rho(g)\rho(h)$ pour tout $g, h \in Z(G)$ (et même $\in G$), λ est bien un caractère linéaire de $Z(G)$.

2. Soit ρ une représentation de G irréductible et fidèle. Si $g \in Z(G)\backslash\{1\}$, on a par hypothèse $\rho(g) \neq \mathrm{id}_V$ et donc $\lambda(g) \neq 1$. Le caractère linéaire $\lambda : Z(G) \to \mathbb{T}$ est donc un morphisme injectif ($\mathbb{T}$ le cercle unité de $\mathbb{C}^\times$). Ainsi $Z(G)$ est isomorphe à un sous-groupe de $\mathbb{T}$. Soit n l'ordre de $Z(G)$. Si $g \in Z(G)$, on a $g^n = 1$ et donc $\lambda(g)^n = \lambda(g^n) = \lambda(1) = 1$, donc $\lambda(g) \in \mathbb{U}_n$, le groupe des racines n-ièmes de l'unité. Alors $\lambda : Z(G) \to \mathbb{U}_n$ est un morphisme injectif entre deux groupes de même ordre, donc est bijectif. Comme $\mathbb{U}_n$ est cyclique, $Z(G)$ est donc cyclique.

Exercice 3 1. Puisque $\mathbf{UT}_3(\mathbb{F}_3)$ est un espace affine de dimension $d = 3$ sur le corps à $n = 3$ éléments, son cardinal est $n^d = 27$.

Les matrices concernées étant triangulaires de diagonale $(1, 1, 1)$, elles ont toutes le même polynôme caractéristique, à savoir $P(X) = (X - 1)^3$. Par le théorème de Cayley-Hamilton, elles satisfont donc $(A - I_3)^3 = 0_3$. Cependant $(X-1)^3 = X^3 - 3X^2 + 3X - 1 = X^3 - 1$ en caractéristique 3. On a donc toujours $A^3 = I_3$.

2. Le produit de deux matrices du groupe vaut

$$\begin{aligned} M(a,b,c)M(x,y,z) &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+x & b+y+az \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix} \\ &= M(a+x, b+y+az, c+z). \end{aligned}$$

Ces deux matrices commutent si et seulement si $az = cx$. $M(a, b, c)$ est donc dans le centre du groupe si et seulement si $az = cx$ pour tout x, y, z, c'est-à-dire $a = c = 0$. Le centre est donc composé des matrices $M(0, b, 0)$. Il est d'ordre 3, isomorphe à $\mathbb{F}_3$.

3. Le calcul ci-dessus montre que $M(a, b, c)M(0, y, 0) = M(a, b + y, c)$. La classe $M(a, b, c)Z$ est donc égale à $M(a, \mathbb{F}_3, c)$. Comme $M(a, \mathbb{F}_3, c)M(x, \mathbb{F}_3, z) = M(a + x, \mathbb{F}_3, c + z)$, l'application $M(a, \mathbb{F}_3, c) \mapsto (a, c)$ est un morphisme de groupe entre $\mathbf{UT}_3(\mathbb{F}_3)/Z$ et $(\mathbb{F}_3)^2$, évidemment bijectif.

Attention. On ne peut pas s'appuyer sur la remarque que

$$AX - XA = \begin{pmatrix} 0 & 0 & \cdot \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

car on est dans un groupe, pas dans une algèbre.

Puisque tous les éléments de $\mathbf{UT}_3(\mathbb{F}_3)$ sont d'ordre 1 ou 3 (question 1), il en est de même dans $\mathbf{UT}_3(\mathbb{F}_3)/Z$. Prenons un élément a d'ordre 3 puis $b \neq 1, a, a^2$. Alors $a \neq b, b^2$ et donc le sous-groupe $\langle a, b\rangle$ de $\mathbf{UT}_3(\mathbb{F}_3)/Z$ est un produit direct $\langle a\rangle\langle b\rangle$, isomorphe à $(\mathbb{Z}/3\mathbb{Z})^2$. Comme $\mathbf{UT}_3(\mathbb{F}_3)/Z$ est d'ordre $27/3 = 9$, ce sous-groupe d'ordre 9 lui est égal. Donc $\mathbf{UT}_3(\mathbb{F}_3)/Z$ est isomorphe à $(\mathbb{Z}/3\mathbb{Z})^2$.

4. Les caractères linéaires de $\mathbb{Z}/3\mathbb{Z}$ forment un groupe L_3 qui lui est isomorphe. Ceux de $(\mathbb{Z}/3\mathbb{Z})^2$ forment un groupe isomorphe à $(L_3)^2$ *via*
$$(\chi_1, \chi_2) \mapsto \lambda, \qquad \lambda(z,t) := \chi_1(z)\chi_2(t).$$
   Il y a donc 9 caractères linéaires sur le quotient $\mathbf{UT}_3(\mathbb{F}_3)/Z$. Par composition de morphismes
$$\mathbf{UT}_3(\mathbb{F}_3) \to \mathbf{UT}_3(\mathbb{F}_3)/Z \to \mathbb{C}^\times,$$
   on obtient un groupe à 9 éléments de caractères linéaires sur $\mathbf{UT}_3(\mathbb{F}_3)$. Par construction, ils valent 1 sur Z. Réciproquement, si χ est un caractère linéaire sur $\mathbf{UT}_3(\mathbb{F}_3)$ qui vaut 1 sur Z, ce qui signifie $Z \subset \ker\chi$, alors χ se factorise sous la forme $\lambda \circ \pi$ où π est la projection sur $\mathbf{UT}_3(\mathbb{F}_3)/Z$ et λ est un caractère linéaire du quotient.
5. $Z(M)$ est l'ensemble des matrices commutant à M. Si $M = M(x,y,z)$, alors $M(a,b,c)M = MM(a,b,c)$ équivaut à $az = cx$. Lorsque $M \notin Z$, on a $(x,z) \neq (0,0)$ (question 2). L'équation $az = cx$ définit donc un plan affine (sous-espace affine de codimension 1 dans un espace de dimension 3), dont le nombre d'éléments est $n^2 = 9$.

   La classe de conjugaison d'un $M \notin Z$ est donc de cardinal
$$(\mathbf{UT}_3(\mathbb{F}_3) : Z(M)) = 27/9 = 3.$$
   Les $27 - 3 = 24$ éléments de $\mathbf{UT}_3(\mathbb{F}_3) \setminus Z$ se répartissent donc en 8 classes de conjugaison de cardinal 3. Il y a par ailleurs trois classes à un élément, une pour chaque $a \in Z$. Au total, cela fait 11 classes de conjugaison.
6. Le nombre de caractères irréductibles de $\mathbf{UT}_3(\mathbb{F}_3)$ est donc 11, parmi lesquels on en connaît 9 de degré un (question 4). Soit p et q les degrés des deux autres. On a $27 = |\mathbf{UT}_3(\mathbb{F}_3)| = 1^2 + \cdots + 1^2 + p^2 = q^2$, c'est-à-dire $p^2 + q^2 = 18$. La seule solution est $p = q = 3$.
7. Soit α un caractère linéaire. Alors $\alpha\chi_+$ est un caractère, irréductible et de degré 3, donc est égal à χ_+ ou à χ_-. De même $\alpha^2\chi_+ = \chi_\pm$.

   Si on a $\alpha\chi_+ = \chi_-$ **et** $\alpha^2\chi_+ = \chi_-$, alors $\alpha\chi_+ = \alpha^2\chi_+$; mais puisque $|\alpha| \equiv 1$, on peut simplifier et obtenir $\alpha\chi_+ = \chi_+$, ce qui est contradictoire. Donc $\alpha\chi_+ = \chi_+$ ou $\alpha^2\chi_+ = \chi_+$.
8. La description de la question 4 montre qu'il existe un caractère linéaire λ sur $\mathbf{UT}_3(\mathbb{F}_3)/Z$ tel que $\lambda(\dot{c}) \neq 1$. Comme les caractères sur $\mathbb{Z}/3\mathbb{Z}$ sont des racines cubiques de l'unité, on a $\lambda(\dot{c}) = j$ ou j^2. Quitte à conjuguer, on obtient un caractère tel que $\lambda(\dot{c}) = j$. Alors $\alpha = \lambda \circ \pi$ répond à la question.

   Par la question 7, on a donc $(j^m - 1)\chi_+(c) = 0$ avec $m = 1$ ou 2. Ceci entraine $\chi_+(c) = 0$.
9. Soit ρ_+ une représentation, de degré 3, de caractère χ_+. Comme $A^3 = I_3$, on a $\rho(A)^3 = \mathrm{id}_V$. Les valeurs propres f, g et h de $\rho(A)$ sont donc des racines cubiques de l'unité $1, j$ ou j^2. On $\chi_+(A) = \mathrm{Tr}\rho(A) = f + g + h$. Il en est de même pour I_3 et B, et pour χ_-. En particulier, $|\chi_+(A)| \leq 3$, avec égalité si et seulement si $f = g = h$.

Écrivons que $\langle \chi_+, \chi_+ \rangle = 1$ (par irréductibilité), en utilisant le fait que $\chi_+ \equiv 0$ en dehors de Z (question 8) :

$$1 = \frac{1}{27}(|\chi_+(I_3)|^2 + |\chi_+(A)|^2 + |\chi_+(B)|^2),$$

c'est-à-dire $|\chi_+(A)|^2 + |\chi_+(B)|^2 = 18$. Comme $|\chi_+(A)| \leq 3$ (idem pour B), on obtient $|\chi_+(A)| = |\chi_+(B)| = 3$. Par le cas d'égalité ci-dessus, $\chi_+(A)$ et $\chi_+(B)$ valent $3j$ ou $3j^2$.

10. On a vu que si $a, b \in \mathbf{UT}_3(\mathbb{F}_3)$ alors $aba^{-1}b^{-1} \in Z(G)$. Ceci montre que $\pi(a) = \pi(bab^{-1})$. Les classes $c_1, \ldots, c_8$ à trois éléments se projettent donc chacune sur un des huit éléments non nuls du quotient $\mathbf{UT}_3(\mathbb{F}_3)/Z \sim (\mathbb{Z}/3\mathbb{Z})^2$. Avec les questions 4 et 8, ceci nous permet de remplir presque toute la table :

	I_3	A	B	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8
$\mathbf{1}$	1	1	1	1	1	1	1	1	1	1	1
χ_1	1	1	1	j	j^2	1	1	j	j	j^2	j^2
χ_2	1	1	1	j^2	j	1	1	j^2	j^2	j	j
χ_3	1	1	1	1	1	j	j^2	j	j^2	j	j^2
χ_4	1	1	1	j	j^2	j	j^2	j^2	1	1	j
χ_5	1	1	1	j^2	j	j	j^2	1	j	j^2	1
χ_6	1	1	1	1	1	j^2	j	j^2	j	j^2	j
χ_7	1	1	1	j	j^2	j^2	j	1	j^2	j	1
χ_8	1	1	1	j^2	j	j^2	j	j	1	1	j^2
χ_+	3	3α	3β	0	0	0	0	0	0	0	0
χ_-	3	3γ	3δ	0	0	0	0	0	0	0	0

Enfin, la table

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \beta \\ 1 & \gamma & \delta \end{pmatrix}$$

est celle des caractères irréductibles de $Z \sim \mathbb{Z}/3\mathbb{Z}$. On a donc, à permutation près de A et B, $\alpha = \delta = j$ et $\beta = \gamma = j^2$.