

Problème 1 Le nombre de représentations irréductibles à isomorphisme près d'un groupe fini G est égal au nombre de ses classes de conjugaison. Le nombre des classes de conjugaison de \mathcal{S}_n est égal au nombre de partitions de n . Donc, a) \mathcal{S}_3 en possède 3, b) \mathcal{S}_5 en possède 7 (correspondant à $5, 4 \geq 1, 3 \geq 2, 3 \geq 1 \geq 1, 2 \geq 2 \geq 1, 2 \geq 1 \geq 1 \geq 1$ et enfin $1 \geq 1 \geq 1 \geq 1 \geq 1$). Pour le cas c), on rappelle que $\mathbb{Z}/3\mathbb{Z}$ (comme il est abélien) possède 3 représentations irréductibles et donc G possède $3 \times 7 \times 3 = 63$ correspondant aux produit tensoriel des représentations irréductibles de chacun des groupes $\mathcal{S}_3, \mathcal{S}_5, \mathbb{Z}/3\mathbb{Z}$.

Problème 2 1. En caractéristique 2, on a $X^4 + 1 = (X + 1)^4$.

2. On suppose $a = bc$ avec c entier. Alors, dans $\mathbb{Z}/a\mathbb{Z} : \bar{c}, 2\bar{c}, \dots, k\bar{c}, \dots, (b-1)\bar{c}$ sont tous non nuls (puisque $0 < kc < a$) et $b\bar{c} = \bar{a}$ est nul, donc \bar{c} est bien d'ordre b .
3. On sait que $\mathbb{F}_{p^2}^*$ est cyclique d'ordre $p^2 - 1 = (p-1)(p+1)$. Or, comme p est impair $(p-1)$ et $(p+1)$ sont pairs et un des deux est multiple de 4. Donc $\mathbb{F}_{p^2}^*$ est cyclique d'ordre multiple de 8. D'après la question qui précède, il possède un élément d'ordre 8.

On écrit $X^8 - 1 = (X^4 + 1)(X^4 - 1)$ dans $\mathbb{F}_{p^2}[X]$. Soit α un élément d'ordre 8 de $\mathbb{F}_{p^2}^*$, alors $\alpha^8 = 1$ et $\alpha^4 \neq 1$. Donc, par cette égalité, α est racine de $X^4 + 1$.

4. Soit d le degré du polynôme annulateur minimal Q de α sur \mathbb{F}_p , c'est-à-dire le générateur du noyau du morphisme d'évaluation en α de $\mathbb{F}_p[X]$ sur $\mathbb{F}_p[\alpha]$. Alors, on sait que ce degré est égal au degré $[\mathbb{F}_p[\alpha] : \mathbb{F}_p]$. Par la question précédente, $\alpha \in \mathbb{F}_{p^2}$, donc $d \leq 2$. On en déduit donc que $Q \in \mathbb{F}_p[X]$ divise $X^4 + 1$ et qu'il est de degré inférieur à 2. Il en résulte que $X^4 + 1$ se réduit sur \mathbb{F}_p .
5. On vient de voir que $X^4 + 1$ est toujours réductible sur \mathbb{F}_p (pour p premier pair ou impair); il est donc forcément toujours irréductible sur \mathbb{F}_{p^n} puisque ce dernier contient \mathbb{F}_p .

Problème 3 1. Par le théorème de structure des groupes abéliens finis, il y a, à isomorphisme près 3, groupes abéliens d'ordre 8. Nommément $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^3$.

2. C'est un résultat classique sur les p -groupes. On fait agir G par conjugaison sur lui-même, G est réunion de classes (les classes de conjugaison en fait), et ces classes sont de cardinal qui divise 8. Donc, la réunion des classes de cardinal 1 est forcément pair. Or, cette réunion est égale au centre. Donc, l'ordre du centre est pair et comme ce dernier est non vide, il est non trivial.
3. Si $G/Z(G)$ était cyclique, il pourrait s'écrire comme l'ensemble des classes de la forme $\bar{a}^k, k \in \mathbb{Z}$, pour un a . Soit $b, c \in G$, il vient $b = b_0 a^k, c = c_0 a^h$, avec $b_0, c_0 \in Z(G)$ et on voit alors facilement que b et c commutent, contrairement à l'hypothèse.
4. On en déduit donc que $Z(G)$ est d'ordre 2. En effet, il est non trivial, et il ne peut être d'ordre 4 ou 8 sinon G serait abélien par la question précédente. Maintenant, le quotient $G/Z(G)$ est d'ordre 4 et non cyclique, donc, il est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

5. Si tous les éléments de G vérifiaient $a^2 = e$, alors G serait abélien puisque $(ab)^2 = e$ impliquerait $ab = ba$ pour tout a, b . Par Lagrange, l'ordre d'un élément divise l'ordre du groupe, donc, G possède au moins un élément d'ordre 4 ou 8. Dans les deux cas, il possède un élément d'ordre 4 (on peut aussi remarquer que G ne possède pas d'élément d'ordre 8 sinon il serait abélien).
6. (a) On note tout d'abord que $K := \langle g \rangle$ est un sous-groupe d'indice 2 donc distingué. De plus, $\{e, h\}$ est un sous-groupe d'ordre 2 de G dont l'intersection avec K est triviale. Toutes les conditions sont réunies pour avoir un produit semi-direct $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, c'est à dire le groupe diédral.
 - (b) (i) Le groupe G contient $K := \langle g \rangle$ qui est un sous-groupe qui possède un unique élément d'ordre 2. Supposons qu'il existe un élément d'ordre 2 hors de K . Alors, par la question précédente, le groupe G est isomorphe au groupe diédral et dans ce cas, tous les éléments hors de K sont d'ordre 2, ce qui est contraire à l'hypothèse. Il existe donc un unique élément d'ordre 2.
 - (ii) Il suffit de donner explicitement l'isomorphisme qui envoie respectivement $e, g, g^2, g^3, h, hg, hg^2, hg^3$ sur $1, i, -1, -i, k, i, -k, -j$.
7. On a en conclusion deux groupes non abéliens d'ordre 8 : le groupe diédral D_4 et le groupe quaternionique H_8 . Il ne sont pas isomorphes sinon ils auraient le même nombre d'éléments d'ordre 2. Or, D_4 en possède 5 et H_8 n'en possède qu'un seul.

Problème 4 1. Si ϕ et ψ sont les caractères respectifs des représentations V et W , alors $\phi\psi$ est le caractère de la représentation $V \otimes W$.

2. On a $(\psi, \psi) = (\overline{\psi}, \overline{\psi})$, pour la forme G -invariante, puisque pour tout g de G , $|\psi(g)|^2 = |\overline{\psi(g)}|^2$. On en déduit le résultat voulu par le critère d'irréductibilité des caractères par les normes.
3. Comme ψ est de degré 1, on peut assimiler le caractère et la représentation (on prend la trace d'une matrice de taille 1). Pour tout g de G , $\psi(g)$ est une racine de l'unité par Lagrange, et en particulier, $|\psi(g)| = 1$ et donc, $|\phi(g)\psi(g)|^2 = |\phi(g)|^2$. On en déduit $(\phi\psi, \phi\psi) = (\phi, \phi)$, et encore une fois, le résultat provient du critère d'irréductibilité des caractères par les normes.
4. On a

$$(\psi\overline{\psi}, 1) = \frac{1}{|G|} \sum_{g \in G} \psi(g)\overline{\psi(g)} = (\psi, \psi).$$

On a donc $(\psi\overline{\psi}, 1) \geq 1$, ce qui signifie que $\psi\overline{\psi}$ contient la représentation triviale.

Comme ψ est de degré strictement supérieur à 1, il en est de même de $\psi\overline{\psi}$ et donc elle ne peut pas être isomorphe à la représentation triviale. Comme elle la contient, elle ne peut pas être irréductible.

5. Comme ϕ est irréductible de degré d et que ψ est de degré 1, il en résulte que $\phi\psi$ est encore irréductible de degré d . Donc, égal à ϕ par unicité. Il vient donc pour tout g l'égalité $\phi(g)\psi(g) = \phi(g)$. D'où l'assertion demandée.