ALGÈBRE – DEVOIR À LA MAISON I

PROBLÈME 1 — NOMBRES CYCLIQUES. Soit $n \in \mathbb{N}^*$. On dit que n est un *nombre cyclique* si tout groupe de cardinal n est cyclique.

1. Justifier qu'un nombre premier est cyclique et que, pour $p < q$ deux nombres premiers tels que $p \nmid q-1$, pq aussi.

Le reste du problème est consacré à la démonstration du fait que si

$$n \text{ est } \textit{sans facteur carré} \text{ et si pour tout paire de nombres premiers } p < q \text{ divisant } n, \text{ on a } p \nmid q-1, \qquad (*)$$

alors n est cyclique.

On rappelle qu'un entier est *sans facteur carré* s'il n'est divisible par le carré d'aucun nombre premier. On note φ l'indicatrice d'Euler et on rappelle que pour tout entier naturel non nul, $\varphi(n) = \{m \in \{1,\dots,n\} \ : \ \mathrm{pgcd}(m,n) = 1\}$.

2. Établir qu'un entier n satisfait la condition $(*)$ ci-dessus si, et seulement si, $\mathrm{pgcd}(n, \varphi(n)) = 1$.
On pourra montrer que si ℓ et k sont premiers entre eux, $\varphi(\ell k) = \varphi(\ell)\varphi(k)$ et calculer $\varphi(p^\alpha)$ pour p premier et $\alpha \in \mathbb{N}$.

3. On raisonne par récurrence sur les entiers vérifiant la condition $(*)$. On suppose que $n > 1$ et que tous les groupes d'ordre $k < n$ avec k vérifiant $(*)$ sont cycliques. On cherche à montrer que tout groupe d'ordre n avec n satisfaisant $(*)$ est cyclique. Raisonnons alors par l'absurde en considérant un groupe G d'ordre n vérifiant $(*)$ tel que G ne soit pas cyclique.

a) Justifier que tous les sous-groupes et les quotients de G distincts de G sont cycliques.

b) Montrer que G est non abélien et en déduire que $Z(G) = \{e\}$.
On pourra supposer G abélien et construire un élément d'ordre n, puis, on pourra considérer le quotient $G/Z(G)$.

c) On dit qu'un sous-groupe M de G est *maximal* si $M \neq G$ et si pour tout sous-groupe H tel que $M \subseteq H \subseteq G$, alors $H = G$. On définit également pour tout $x \in G$ le *centralisateur* de x comme étant le stabilisateur de x pour l'action de G sur lui-même par conjugaison. Montrer que pour tout $x \in G \setminus \{e\}$, $Z(x)$ est un sous-groupe maximal de G.

d) Soit M un sous-groupe maximal de G. Montrer réciproquement que $M = Z(x)$ pour tout $x \in M \setminus \{e\}$.

e) Montrer que deux sous-groupes maximaux M et M' sont d'intersection triviale.

f) Soit N un sous-groupe propre distingué de G. Montrer que l'action par conjugaison de G sur N fournit un morphisme $\rho : G \longrightarrow \mathrm{Aut}(N)$. Montrer que le cardinal de $G/\mathrm{Ker}(\rho)$ divise à la fois n et $\varphi(n)$. Conclure à la simplicité de G.

g) Soit M un sous-groupe maximal de G. Montrer que le nombre de sous-groupes de la forme gMg^{-1} avec $g \in G$ est donné par $\dfrac{\#G}{\#N_G(M)}$, où $N_G(M) = \left\{g \in G \ : \ gMg^{-1} = M\right\}$ est le *normalisateur* de M dans G. En déduire que

$$1 + \frac{\#G}{2} \leqslant \#\left(\bigcup_{g\in G} gMg^{-1}\right) < \#G.$$

h) On choisit alors $x \in G \setminus \left(\bigcup_{g\in G} gMg^{-1}\right)$ et on pose $M' = Z(x)$. Minorer le cardinal de

$$\left(\bigcup_{g\in G} gMg^{-1}\right) \cup \left(\bigcup_{g\in G} gM'g^{-1}\right).$$

Conclure.

SOLUTION.

1. **(sur 1 point)** Soit p un nombre premier et G d'ordre p. Par le théorème de Lagrange, tout $x \in G \setminus \{e\}$ est d'ordre p et engendre G qui est par conséquent cyclique. Soit G d'ordre pq avec $p < q$ deux nombres premiers et $p \nmid q-1$. Les théorèmes de Sylow garantissent alors qu'on a un unique q-Sylow et un unique p-Sylow. Cela fournit $1 + (p-1) + (q-1) = p+q-1$ éléments d'ordre 1, p ou q. Mais $p + q < 2q \leqslant pq$ donc $p+q \leqslant pq - 1$ et l'égalité est stricte sauf si $p = 2$ et $q = 3$ mais on a alors que $p \mid q-1$. On a donc nécessairement un élément d'ordre pq et G est cyclique.

On peut ainsi déterminer le plus petit entier cyclique non premier. Le premier nombre composé > 1 est 4 qui ne convient pas car $(\mathbf{Z}/2\mathbf{Z})^2$ n'est pas cyclique. On tire du fait que $\mathfrak{S}_3$, $(\mathbf{Z}/2\mathbf{Z})^3$, $(\mathbf{Z}/3\mathbf{Z})^2$ ne sont pas cycliques que le premier entier n cyclique non premier est supérieur à $10 = 2 \times 5$. Comme $2 \mid 5 - 1$, le cours[1] garantit qu'il existe un produit semi-direct non trivial (donc non abélien et non cyclique) $\mathbf{Z}/5\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$, ce qui permet d'exclure 10 tandis que le cas de $(\mathbf{Z}/2\mathbf{Z})^2 \times \mathbf{Z}/3\mathbf{Z}$ exclut 12. On élimine 14 pour les mêmes raisons que 10. On arrive donc à $n = 15 = 3 \times 5$. Comme on a $3 \nmid 5-1$, le cours garantit que tout groupe G d'ordre 15 vérifie $G \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z} \cong \mathbf{Z}/15\mathbf{Z}$, ce qui permet d'en déduire que l'entier cherché vaut 15.

1. Voir par exemple ici pour celles et ceux qui ne sont pas familiers avec le produit semi-direct.

2. **(sur 1 point)** Soient k et ℓ deux entiers premiers entre eux. On sait alors d'après le théorème chinois qu'on a un isomorphisme d'anneaux

$$\mathbf{Z}/(k\ell)\mathbf{Z} \cong \mathbf{Z}/k\mathbf{Z} \times \mathbf{Z}/k\ell\mathbf{Z}$$

qui fournit un isomorphisme de groupes

$$(\mathbf{Z}/(k\ell)\mathbf{Z})^{\times} \cong (\mathbf{Z}/k\mathbf{Z})^{\times} \times (\mathbf{Z}/k\ell\mathbf{Z})^{\times}.$$

On obtient en considérant les cardinaux que $\varphi(k\ell) = \varphi(k)\varphi(\ell)$. On en déduit que si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ est la décomposition de n en produit de facteurs premiers avec $r \in \mathbf{N}$, $p_1, \ldots, p_r$ des nombres premiers distincts et $\alpha_1, \ldots, \alpha_r \in \mathbf{N}^*$, alors d'après ce qui précède

$$\varphi(n) = \prod_{i=1}^{r} \varphi\left(p_i^{\alpha_i}\right).$$

Reste à voir que $\varphi\left(p_i^{\alpha_i}\right) = p_i^{\alpha_i-1}(p_i-1)$. En effet, parmi $\{1,2,3\ldots,p_i^{\alpha_i}\}$, les entiers non premiers à $p_i^{\alpha_i}$ et inférieurs à $p_i^{\alpha_i}$ sont exactement les $p_i k$ pour $k \in \{1,\ldots,p_i^{\alpha_i-1}\}$ si bien que $\varphi\left(p_i^{\alpha_i}\right) = p_i^{\alpha_i} - p_i^{\alpha_i-1}$, ce qui fournit le résultat annoncé. Finalement, on a

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i-1}(p_i-1).$$

Venons-en à présent au fait que n vérifie $(*)$ si, et seulement si, $\mathrm{pgcd}(n,\varphi(n)) = 1$. Supposons donc que n vérifie $(*)$. On a ainsi $n = \prod_{i=1}^{r} p_i$ avec $p_i \not\equiv 1 \pmod{p_j}$ pour tout couple $i \neq j \in \{1,\ldots,r\}$. On a alors

$$\varphi(n) = \prod_{i=1}^{r}(p_i-1)$$

et par définition, pour tout $i \in \{1,\ldots,r\}$, p_i est premier avec $p_j - 1$ pour tout $j \in \{1,\ldots,r\}$ et on a bien $\mathrm{pgcd}(n,\varphi(n)) = 1$. Réciproquement, supposons que $\mathrm{pgcd}(n,\varphi(n)) = 1$. On a alors, grâce à l'expression de $\varphi(n)$ ci-dessus, que n est sans facteur carré et que pour tout $i \in \{1,\ldots,r\}$, p_i est premier avec $p_j - 1$ pour tout $j \in \{1,\ldots,r\}$. Autrement dit n satisfait la condition $(*)$ et on a obtenu l'équivalence souhaitée.

Complément. – On peut en fait établir que la condition $(*)$ est nécessaire. Supposons dans un premier temps qu'il existe un nombre premier p tel que $p^2 \mid n$. On a alors que le groupe $(\mathbf{Z}/p\mathbf{Z})^2 \times \mathbf{Z}/n'\mathbf{Z}$ avec $n = p^2 n'$ est non cyclique[2] de cardinal n. Ainsi le fait que n soit sans facteur carré est nécessaire.

Supposons dans un second temps que $pq \mid n$ avec $p < q$ deux nombres premiers avec $q \equiv 1 \pmod{p}$. Le groupe $(\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}) \times \mathbf{Z}/n'\mathbf{Z}$ avec $n = pqn'$ n'est pas cyclique[3] où l'on a considéré l'unique produit semi-direct non trivial. On obtient alors la conclusion désirée.

3. a) **(sur 0,5 point)** C'est clair par hypothèse de récurrence car le cardinal d'un tel sous-groupe ou d'un tel quotient divise n et tout diviseur d'un entier qui satisfait $(*)$ vérifie également $(*)$ avec strictement moins de facteurs premiers.

b) **(sur 1,5 points)** Raisonnons par l'absurde en supposant G abélien. On pose $n = \prod_{i=1}^{r} p_i$. On sait d'après les théorèmes de Sylow que pour tout $i \in \{1,\ldots,r\}$, qu'il existe un p_i-Sylow de cardinal p_i. Un tel p_i-Sylow est cyclique et un générateur g_i fournit un élément d'ordre[4] p_i. Puisque G a été supposé abélien, alors un résultat classique[5] implique que $g_1 g_2 \cdots g_r$ est d'ordre n, contredisant la non-cyclicité de G. Ainsi, G n'est pas abléien. Noter que l'on pouvait aussi utiliser le théorème de classification des groupes abéliens de type fini.

À nouveau, raisonnons par l'absurde en supposant que $Z(G) \neq \{e\}$. On considère alors le quotient $G/Z(G)$ qui est un quotient non trivial donc cyclique d'après la question précédente. Un résultat du cours implique alors que G est abélien, ce qui est exclu par la première partie de la question. Finalement, $Z(G) = \{e\}$.

c) **(sur 0,5 point)** Soit $x \in G \setminus \{e\}$. On a, par définition, $Z(x) = \{g \in G \ : \ gx = xg\}$ et $Z(x) \neq G$ car sinon $x \in Z(G)$, ce qui contredit la question précédente. Considérons à présent un sous-groupe H strict de G tel que $Z(x) \subseteq H \subsetneq G$. Par hypothèse de récurrence, H est cyclique (donc en particulier abélien) et donc pour tout $h \in H$, comme $x \in Z(x) \subseteq H$, $xh = hx$ et $h \in Z(x)$ de sorte que $H = Z(x)$, ce qui permet de conclure.

2. Par exemple car tout élément est d'ordre divisant pn'.
3. Par exemple car il contient un sous-groupe non cyclique.
4. On pouvait aussi ici faire appel au lemme de Cauchy, voir ici exercice 3 de la section 2.
5. On peut démontrer par récurrence sur r que, dans un groupe abélien, si les g_i sont d'ordre 2 à 2 premiers entre eux, alors $g_1 \cdots g_r$ est d'ordre le produit des ordres. Je vous renvoie ici exercice 11 de la section 1 par exemple pour une démonstration.

d) **(sur 0,5 point)** Soient M un sous-groupe maximal de G et $x \in M \setminus \{e\}$. Par hypothèse de récurrence, M est cyclique, donc abélien, et toute paire d'éléments de M commutent. Ainsi, $M \subseteq Z(x)$. Comme[6] $Z(x) \neq G$, on en déduit que $M = Z(x)$ par maximalité.

e) **(sur 0,5 point)** Soient M et M' deux sous-groupes maximaux distincts de G. Supposons disposer de $x \in M \cap M'$, $x \neq e$. On a alors $M = M' = Z(x)$ d'après la question précédente, ce qui est une contradiction. D'où, $M \cap M' = \{e\}$.

f) **(sur 1,5 point)** Soit $N \lhd G$ que l'on suppose distinct de G. On sait que pour tout $g \in G, gNg^{-1} = N$ (car N est distingué), de sorte que N est stable par conjugaison. D'après le cours, on peut faire agir G sur N par conjugaison, ce qui fournit un morphisme de groupes $\rho : G \longrightarrow \mathfrak{S}(N)$ donné par $g \mapsto \rho_g$ avec $\rho_g : n \mapsto gng^{-1}$ qui est en fait un automorphisme de N d'inverse $n \mapsto g^{-1}ng$. On a ainsi un morphisme $\rho : G \longrightarrow \mathrm{Aut}(N)$. On note K son noyau. Alors, par hypothèse de récurrence, N est cyclique d'ordre $m \mid n$ et $\mathrm{Aut}(N) \cong (\mathbf{Z}/m\mathbf{Z})^\times \cong \mathbf{Z}/\varphi(m)\mathbf{Z}$. Le premier théorème d'isomorphisme couplé au théorème de Lagrange fournit alors que le cardinal de G/K divise $\varphi(m)$ et l'expression obtenue en question **4.** garantit (puisque $m \mid n$) que $\varphi(m) \mid \varphi(n)$. Par ailleurs, le cardinal de G/K divise évidemment le cardinal de G, à savoir n. Finalement, $\#G/K \mid \mathrm{pgcd}(n, \varphi(n)) = 1$ d'après **4.** On en déduit que $K = G$ et que le morphisme ρ est trivial. Cela signifie que pour tous $g \in G$ et $n \in N$, $gn = ng$ soit que $N \subseteq Z(G) = \{e\}$. On en conclut que $N = \{e\}$ et ainsi que G est simple.

g) **(sur 1,5 points)** Soit M un sous-groupe maximal[7] de G. Commençons par remarquer que pour tout $g \in G$, gMg^{-1} est aussi maximal. On peut soit le voir en considérant un sous-groupe $H \neq G$ tel que $gMg^{-1} \subseteq H$ soit $M \subseteq g^{-1}Hg$. Alors par maximalité de M, on obtient que $M = g^{-1}Hg$ soit $gMg^{-1} = H$ et gMg^{-1} est maximal[8]. On fait alors agir G par conjugaison sur l'ensemble de ses sous-groupes. Il est alors clair qu'on cherche le cardinal de l'orbite de M, qui est donnée d'après le cours par le quotient du cardinal de G par celui du stabilisateur de M dans G qui n'est autre que $N(M)$. D'après la question e), pour g non trivial M et gMg^{-1} ont pour intersection $\{e\}$ lorsqu'ils sont distincts et on en déduit que

$$\#\left(\bigcup_{g\in G} gMg^{-1}\right) = 1 + \frac{\#G}{\#N(M)}(\#M - 1)$$

où le 1 correspond à e et où on a utilisé que le cardinal de gMg^{-1} est égal à celui de M. Or, on a clairement que $M \subseteq N(M)$ et $N(M) \neq G$ car cela impliquerait que $M \lhd G$ mais $M \neq G$ et $M \neq \{e\}$ d'après d) ce qui contredirait la simplicité de G établie en f). Par maximalité, il vient $N(M) = M$ et

$$\#\left(\bigcup_{g\in G} gMg^{-1}\right) = 1 + \#G\left(1 - \frac{1}{\#M}\right) \geqslant 1 + \frac{\#G}{2}.$$

Pour la majoration, on utilise le fait que $M \subseteq G$ strictement, de sorte que

$$\#\left(\bigcup_{g\in G} gMg^{-1}\right) = 1 + \#G\left(1 - \frac{1}{\#M}\right) < 1 + \#G\left(1 - \frac{1}{\#G}\right) = \#G,$$

ce qui permet d'obtenir les inégalités attendues.

h) **(sur 1,5 points)** Pour un tel x (qui existe d'après la majoration de la question précédente), la question c) implique que $M' = Z(x)$ est maximal et puisque $x \neq e$, le même raisonnement qu'en question précédente fournit

$$\#\left(\bigcup_{g\in G} gM'g^{-1}\right) \geqslant 1 + \frac{\#G}{2}.$$

Pour conclure, les sous-groupes maximaux gMg^{-1} et $hM'h^{-1}$ pour g et h dans G sont distincts car sinon $x \in M'$ est dans un conjugué de M, ce qui est exclu par hypothèse. Par e), on en déduit que[9]

$$\#\left(\left(\bigcup_{g\in G} gMg^{-1}\right) \cup \left(\bigcup_{g\in G} gM'g^{-1}\right)\right) = 1 + \#\left(\bigcup_{g\in G} gMg^{-1}\right) - 1 + \#\left(\bigcup_{g\in G} gM'g^{-1}\right) - 1 \geqslant 1 + \#G$$

ce qui est absurde. On en déduit que G est cyclique et comme tout groupe d'ordre 1 est cyclique, on peut initialiser notre récurrence et obtenir le résultat.

6. Par le même argument qu'en question précédente.
7. Noter qu'un tel sous-groupe existe bel et bien en général. En effet, on considère l'ensemble $\mathcal{E}$ des sous-groupes stricts de G. C'est un ensemble fini non vide muni de la relation d'ordre donnée par l'inclusion donc admettant un élément maximal (c'est-à-dire tel que quel que soit $H \in \mathcal{E}$ vérifiant $M \subseteq H$, alors $M = H$) M qui n'est autre qu'un sous-groupe maximal de G.
8. On pouvait aussi utiliser qu'il existe x non trivial dans G tel que $M = Z(x)$ et que $gMg^{-1} = Z(g^{-1}xg)$ est maximal d'après c).
9. Les -1 proviennent du fait qu'on retranche l'identité de $\bigcup_{g\in G} gMg^{-1}$ et de $\bigcup_{g\in G} gM'g^{-1}$ pour ne pas le compter plusieurs fois et on le rajoute avec le +1.

Problème 2 — Module de permutation. Soient G un groupe fini et X un ensemble sur lequel G agit. Soit k un corps de caractéristique nulle.

1. Montrer que G agit linéairement sur l'espace vectoriel k^X des applications de X dans k via $(g \cdot f)(x) = f(g^{-1} \cdot x)$ pour tous $x \in X$, $g \in G$ et $f \in k^X$.
2. Montrer que le sous-espace vectoriel $k^{(X)}$ des applications à support fini est un sous-G-module de k^X dont une base est donnée par $(\delta_x)_{x \in X}$ où $\delta_x(y) = 1$ si $y = x$ et 0 sinon pour tout $y \in X$. Vérifier que $g \cdot \delta_x = \delta_{gx}$ pour tous $g \in G$ et $x \in X$.
   On appelle le G-module $k^{(X)}$ *le G-module de permutation* associé à X et on le note X^σ.

On suppose dans le reste du problème que l'ensemble X est **fini.**

3. On note
$$(X^\sigma)^G = \{f \in X^\sigma \ : \ \forall g \in G, \, g \cdot f = f\}.$$
   Calculer $(X^\sigma)^G$ puis $\chi_{X^\sigma}(g)$ pour tout $g \in G$.
4. En déduire la formule de Burnside
$$r = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$
   où r désigne le nombre d'orbites de X sous l'action de G et $X^g = \{x \in X \ : \ g \cdot x = x\}$.

Dans les question **5.** à **9.**, on suppose que $|X| \geqslant 2$ et $|X/G| = 1$.

5. Montrer qu'il existe $g \in G$ sans point fixe.
6. Montrer que les propriétés ci-dessous sont équivalentes :
   (i) L'action de G sur X est doublement transitive, c'est-à-dire que pour tous $x \neq y$ et $x' \neq y'$ dans X, il existe $g \in G$ tel que $x' = g \cdot x$ et $y' = g \cdot y$.
   (ii) L'action de G sur $X \times X$ a deux orbites : la diagonale et son complémentaire.
   (iii) On a $\displaystyle\sum_{g \in G} |X^g|^2 = 2|G|$.
7. Montrer que $(X^\sigma)^G$ admet un unique supplémentaire G-stable, que l'on notera V et que l'on déterminera.
8. Montrer que si les propriétés de la question **6.** sont vérifiées, alors V est un G-module irréductible. En déduire les sous-G-modules de X^σ.
9. Montrer que si V est un G-module irréductible et k est algébriquement clos, alors les propriétés de la question **6.** sont vérifiées.
10. Soit $n \geqslant 2$. En déduire que si k est un corps de caractéristique nulle, alors le $\mathfrak{S}_n$-module k^n obtenu par permutation des coordonnées se décompose en somme directe de deux représentations irréductibles non isomorphes dont l'une est la représentation triviale.
    La seconde s'appelle la *représentation standard*.

Solution.

1. **(sur 0,5 point)** Soient $f \in k^X$, $x \in X$ et $g, g' \in G$. On a
$$g' \cdot (g \cdot f)(x) = F\left(g'^{-1} \cdot x\right)$$
   avec $F(x) = f\left(g^{-1} \cdot x\right)$. Il s'ensuit que (poser $y = g'^{-1} \cdot x$ pour s'en convaincre)
$$g' \cdot (g \cdot f)(x) = f\left(g^{-1} \cdot g'^{-1} \cdot x\right) = f\left((g'g)^{-1} \cdot x\right) = (g'g) \cdot f(x).$$
   Ainsi, on a bien $(g'g) \cdot f = g' \cdot (g \cdot f)$. Par ailleurs, on a bien $e \cdot f = f$ et donc on a bien une action de groupes.
   Cette action est linéaire puisque si l'on prend $f, F \in k^X$, $\lambda \in k$ et $g \in G$, on a pour tout $x \in X$
$$g \cdot (\lambda f + F)(x) = \lambda f + F\left(g^{-1} \cdot x\right) = \lambda f\left(g^{-1} \cdot x\right) + F\left(g^{-1} \cdot x\right) = \lambda g \cdot f(x) + g \cdot F(x).$$
   On a donc une représentation de G.
2. **(sur 0,5 point)** On a bien que les $\delta_x \in k^{(X)}$. Par ailleurs, $k^{(X)}$ est clairement un sous-espace vectoriel de k^X et pour tout $f \in k^{(X)}$, de support $S \subseteq X$ fini,
$$f = \sum_{x \in S} f(x)\delta_x$$
   si bien que la famille est génératrice. On a par ailleurs qu'elle est libre puisque si $(\lambda_x)_{x \in X}$ est une famille presque nulle de k telle que [10]
$$\sum_{x \in X} \lambda_x \delta_x = 0.$$

10. Noter que la somme a bien un sens puisque seuls un nombre fini de λ_x sont non nuls.

En évaluant en x, il vient $\lambda_x = 0$. Reste à vérifier qu'il s'agit d'un sous-G-module, soit que $k^{(X)}$ est G-stable. On a alors pour $g \in G$ et $x, y \in X$ que

$$g \cdot \delta_x(y) = \delta_x\left(g^{-1} \cdot y\right).$$

Cela vaut 1 si $g^{-1} \cdot y = x$ soit $y = g \cdot x$ et 0 sinon de sorte que $g \cdot \delta_x = \delta_{g \cdot x}$ et $k^{(X)}$ est bien G-stable et fournit par conséquent une sous-représentation de k^X.

3. (sur 2 points) Soit

$$f = \sum_{x \in X} \lambda_x \delta_x \in (X^\sigma)^G$$

avec $(\lambda_x)_{x \in X}$ une famille (automatiquement presque nulle puisque X est fini) de k. On a alors pour tout élément $g \in G$ que

$$g \cdot f = \sum_{x \in X} \lambda_x \delta_{g \cdot x}.$$

En comparant le coefficient devant $\delta_{g \cdot x}$, il vient par liberté $\lambda_x = \lambda_{g \cdot x}$. Comme cela est valable pour tout $g \in G$, on en déduit que $x \mapsto \lambda_x$ est constante sur les orbites de l'action de G sur X. On voit déjà que $\dim\left((X^\sigma)^G\right) = |X/G|$ engendré, si on note $r = |X/G|$ et $O_1, \ldots, O_r$ les différentes orbites, par les

$$f_i = \sum_{x \in O_i} \delta_x.$$

On vérifie facilement que ces fonctions sont bien invariantes sous l'action de G car l'action de G sur X se restreint en une action de G sur O_i et alors $x \mapsto g \cdot x$ est une bijection de O_i par définition d'une action de groupe.
On s'inspire alors de l'exercice 6 du TD 2 pour donner un autre point de vue. Cela nous incite à poser

$$p : \left\{ \begin{array}{ccc} X^\sigma & \longrightarrow & X^\sigma \\ f & \longmapsto & \dfrac{1}{|G|} \displaystyle\sum_{g \in G} g \cdot f. \end{array} \right.$$

On a alors pour tout $f \in X^\sigma$ que

$$\begin{aligned} p \circ p(f) &= p\left(\frac{1}{|G|} \sum_{g \in G} g \cdot f\right) \\ &= \frac{1}{|G|^2} \sum_{g, g' \in G} (g'g) \cdot f \end{aligned}$$

où on a utilisé la linéarité de l'action. On effectue alors le changement de variable $h = gg'$ dans la somme sur g' et on utilise le fait qu'à g fixé, $g' \mapsto gg'$ est une bijection de G ce qui fournit

$$p \circ p(f) = \frac{1}{|G|^2} \sum_{g, h \in G} h \cdot f = \frac{1}{|G|} \sum_{h \in G} h \cdot f = p(f).$$

On en déduit que p est un projecteur. Par ailleurs, pour tous $g \in G$ et $f \in X^\sigma$, on a

$$p(g \cdot f) = \frac{1}{|G|} \sum_{h \in G} h \cdot (g \cdot f) = \frac{1}{|G|} \sum_{h \in G} (hg) \cdot f = p(f)$$

car $h \mapsto hg$ est une bijection de G. De même, par linéarité de l'action

$$g \cdot p(f) = \frac{1}{|G|} \sum_{h \in G} (gh) \cdot f = p(f).$$

Cela implique en particulier que p est un G-morphisme et que son image et son noyau sont deux sous-G-modules. On a également que tout $f \in \mathrm{Im}(p)$, il existe F telle que $f = P(F)$ et alors pour tout $g \in G$, il vient $g \cdot f = g \cdot p(F) = p(F) = f$. Ainsi $\mathrm{Im}(p) \subseteq (X^\sigma)^G$. Réciproquement, si $f \in (X^\sigma)^G$, il est clair que $p(f) = f$ et finalement $(X^\sigma)^G = \mathrm{Im}(p)$.
Dans la base $(\delta_x)_{x \in X}$, la matrice de $\rho(g)$ possède uniquement des 0 et des 1 puisque $\rho(g)(\delta_x) = g \cdot \delta_x = \delta_{g \cdot x}$. Or, $\chi_{X^\sigma}(g) = \mathrm{Tr}(\rho(g))$. Il suffit donc de compter les 1 sur la diagonale et cela n'arrive que si, et seulement si, $g \cdot x = x$. On a donc

$$\chi_{X^\sigma}(g) = \#\{x \in X \,:\, g \cdot x = x\} = |X^g|.$$

4. **(sur 1,5 points)** On a vu que $r = |X/G|$. Par ailleurs, puisque p est un projecteur

$$r = \dim(\mathrm{Im}(p)) = \mathrm{Tr}(p) = \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}(f \mapsto g\cdot f) = \frac{1}{|G|}\sum_{g\in G}\chi_{X^\sigma}(g) = \frac{1}{|G|}\sum_{g\in G}|X^g|.$$

Noter qu'on peut démontrer cette formule de Burnside directement et plus simplement (voir par exemple ici) et en déduire le nombre de coloriages d'un cube ou de colliers possédant un nombre donné de perles de couleurs données (par exemple voir ici).

5. **(sur 0,5 point)** La formule de Burnside fournit

$$1 = \frac{1}{|G|}\sum_{g\in G}|X^g|.$$

On sait alors que $X^e = |X| \geqslant 2$. Si maintenant tout les autres éléments de G ont au moins un point fixe, $|X^g| \geqslant 1$ mais alors

$$\sum_{g\in G}|X^g| \geqslant |G| + 1 \quad \text{soit} \quad \frac{1}{|G|}\sum_{g\in G}|X^g| \geqslant 1 + \frac{1}{|G|}$$

ce qui est absurde !

6. **(sur 1 point)** On a évidemment que pour $g \in G$ et $x, y \in X$, $g\cdot(x,y) = (g\cdot x, g\cdot y)$ définit une action de G sur $X \times X$. Notons $\Delta = \{(x,y) \in X\times X \,:\, x = y\}$ la diagonale. Pour tous $g \in G$ et $x, y \in X$, on a alors

$$g\cdot x = g\cdot y \quad\Longleftrightarrow\quad x = y$$

si bien que pour tout $x \in X$, l'orbite de (x,x) est contenue dans Δ. De même, si $(x,y) \in X\times X \smallsetminus \Delta$, l'orbite de (x,y) est incluse dans $X\times X\smallsetminus\Delta$. Enfin, une action doublement transitive est transitive. En effet, soient $x \neq x'$ dans X. En prenant $y = x$ et $y' = x'$, il vient $g \in G$ tel que $x' = g\cdot x$. On a aussi que l'orbite de $(x,y) \in X\times X$ est donnée par

$$\{(g\cdot x, g\cdot y) \,:\, g \in G\}.$$

Supposons alors l'action doublement transitive. Soient $(x,x), (x',x') \in \Delta$. Par transitivité, il existe $g \in G$ tel que $x' = g\cdot x$ soit tel que $(x',x') = g\cdot(x,x)$. Ainsi, la diagonale forme bien une orbite. Soient alors (x,y) et (x',y') deux éléments de $X\times X\smallsetminus\Delta$ qui vérifient donc $x \neq y$ et $x' \neq y'$. Par double transitivité, il existe donc $g \in G$ tel que $g\cdot(x,y) = (x',y')$ et le complémentaire de la diagonale forme une orbite. Réciproquement, si l'action de G n'a que deux orbites la diagonale et son complémentaire et si l'on prend $x \neq y$ et $x' \neq y'$, alors $(x,y), (x',y') \in X\times X\smallsetminus\Delta$ donc ils appartiennent à la même orbite et il existe $g \in G$ tel que $g\cdot(x,y) = (x',y')$ soit $g\cdot x = x'$ et $g\cdot y = y'$. On a donc l'équivalence entre **(i)** et **(ii)**. Supposons alors **(ii)**. La formule de Burnside fournit

$$2|G| = \sum_{g\in G}|(X\times X)^g|$$

avec

$$(X\times X)^g = \{(x,y) \in X\times X \,:\, g\cdot x = x,\ g\cdot y = y\} = X^g\times X^g.$$

Ainsi

$$2|G| = \sum_{g\in G}|X^g|^2.$$

Réciproquement, cette dernière formule implique que

$$2|G| = \sum_{g\in G}|(X\times X)^g|$$

et que donc l'action de G sur $X\times X$ a deux orbites qui sont nécessairement la diagonale et le complémentaire de la diagonale d'après ce qui précède.

7. **(sur 1 point)** Soit V un supplémentaire G-stable de $(X^\sigma)^G$. On a alors que pour tous $g \in G$ et $v \in V$, $g\cdot v \in V$ si bien que par définition de p (voir question **3.**), $p(v) \in V$. Par ailleurs, comme p est un projecteur, $p(v) \in \mathrm{Im}(p) = (X^\sigma)^G$. Il s'ensuit que $p(v) \in V \cap (X^\sigma)^G = \{0\}$. Finalement, $p(v) = 0$ et $v \in \mathrm{Ker}(p)$. On a donc $V \subseteq \mathrm{Ker}(p)$ et on conclut à l'égalité par exemple par dimension puisque $X^\sigma = (X^\sigma)^G \oplus \mathrm{Ker}(p) = \mathrm{Im}(p)\oplus\mathrm{Ker}(p)$ puisque p est un projecteur.

8. **(sur 1,5 points)** On suppose les propriétés de la question **6.** vérifiées. Comme on le verra dans l'exercice 9 du TD 2, en caractéristique nulle, il suffit de vérifier que $\langle\chi_V,\chi_V\rangle = 1$. Or, on a [11]

$$\langle\chi_V,\chi_V\rangle = \frac{1}{|G|}\sum_{g\in G}\chi_V(g)\chi_V(g^{-1}) = \frac{1}{|G|}\sum_{g\in G}\chi_V(g)^2.$$

11. Noter que vous avez vu dans le cours et dans le cas $k = \mathbb{C}$ la forme bilinéaire

$$\langle\chi_V,\chi_W\rangle = \frac{1}{|G|}\sum_{g\in G}\chi_V(g)\overline{\chi_W(g)}.$$

En effet, on constate que $X^g = X^{g^{-1}}$ puisque si $g \cdot x = x$ alors $x = g^{-1} \cdot x$ et réciproquement. On a donc

$$\chi_{X^\sigma}(g) = |X^g| = \left|X^{g^{-1}}\right| = \chi_{X^\sigma}(g^{-1}).$$

Mais, $\chi_{X^\sigma}(g) = \chi_V(g) + \chi_1(g)$ où χ_1 est le caractère de $(X^\sigma)^G$ puisque $X^\sigma = (X^\sigma)^G \oplus V$. On a vu que puisque $r = 1$, $(X^\sigma)^G$ est de dimension 1 donc irréductible. Par ailleurs, pour tous $g \in G$ et $f \in (X^\sigma)^G$, on a par définition $g \cdot f = f$ de sorte que l'action est triviale et $\chi_1(g) = 1$ pour tout $g \in G$. On a donc pour $g \in G$ que

$$\chi_V(g^{-1}) = \chi_{X^\sigma}(g^{-1}) - \chi_1(g^{-1}) = \chi_{X^\sigma}(g) - 1 = \chi_V(g).$$

D'autre part, la propriété **(iii)** de la question **6.** fournit

$$\begin{aligned} 2|G| &= \sum_{g\in G} |X^g|^2 = \sum_{g\in G} \chi_{X^\sigma}(g)^2 \\ &= \sum_{g\in G} (\chi_V(g) + \chi_1(g))^2 = \sum_{g\in G} (\chi_V(g) + 1)^2 \\ &= \sum_{g\in G} \left(\chi_V(g)^2 + 2\chi_V(g) + 1\right) = \sum_{g\in G} \left(\chi_V(g)^2 + 2\chi_V(g)\right) + |G|. \end{aligned}$$

Il s'ensuit que

$$1 = \frac{1}{|G|}\sum_{g\in G} \chi_V(g)^2 + \frac{2}{|G|}\sum_{g\in G} \chi_V(g) = \langle \chi_V, \chi_V\rangle + \frac{2}{|G|}\sum_{g\in G}(\chi_{X^\sigma}(g) - 1).$$

On constate alors que

$$\sum_{g\in G}(\chi_{X^\sigma}(g) - 1) = \sum_{g\in G} \chi_{X^\sigma}(g) - |G| = 0$$

en appliquant la formule de Burnside et en utilisant le calcul de $\chi_{X^\sigma}(g)$ effectué en question **4.** On a donc que $\langle \chi_V, \chi_V\rangle$ et V est bien irréductible et la décomposition $X^\sigma = (X^\sigma)^G \oplus V$ est la décomposition de X^σ comme somme directe de sous-représentations irréductibles.

Déterminons à présent tous les sous-G-modules de X^σ. Soit W un tel sous-G-module. La restriction du projecteur p définie en question **3.** à W (on a bien $p(W) \subseteq W$ puisque W est G-stable) reste un projecteur de W à valeurs dans $(X^\sigma)^G$. On a donc par simplicité de $(X^\sigma)^G$ que l'image de $p_{|W}$ est soit $\{0\}$ soit $(X^\sigma)^G$. Dans le premier cas, $W \subseteq \mathrm{Ker}(p) = V$ et par simplicité $W = \{0\}$ ou $W = V$. Sinon, $\mathrm{Im}(p_{|W}) = (X^\sigma)^G$, et on a (puisque $p_{|W}$ est un projecteur de noyau $V \cap W$) que $W = (X^\sigma)^G \oplus (W \cap V)$. Mais $V \cap W$ est un sous-G-module de V qui est irréductible. Soit $V \cap W = \{0\}$ auquel cas $W = (X^\sigma)^G$ soit $V \cap W = V$ et alors $V \subseteq W$ et on conclut que $X^\sigma = (X^\sigma)^G \oplus V \subseteq W$ soit $W = X^\sigma$. On a donc que les sous-G-modules de X^σ sont $\{0\}$, $(X^\sigma)^G$, V et X^σ.

9. **(sur 0,5 point)** Lorsque k est algébriquement clos et V irréductible, le lemme de Schur garantit que $\dim_k(\mathrm{End}_k(V)) = 1$. Or (voir l'exercice 9 du TD 2),

$$\langle \chi_V, \chi_V\rangle = \frac{1}{|G|}\sum_{g\in G} \chi_V(g)\chi_V(g^{-1}) = \frac{1}{|G|}\sum_{g\in G} \chi_{V\otimes_k V^*}(g) = \frac{1}{|G|}\sum_{g\in G} \chi_{\mathrm{End}_k(V)}(g) = \dim_k(\mathrm{End}_k(V)) = 1.$$

On déduit alors que

$$1 = \langle \chi_V, \chi_V\rangle + \frac{2}{|G|}\sum_{g\in G}(\chi_{X^\sigma}(g) - 1)$$

puis en remontant les calculs de la question précédente

$$2|G| = \sum_{g\in G} |X^g|^2$$

soit **(iii)**.

Sur un corps de caractéristique nulle ou première à l'ordre du groupe, la bonne forme bilinéaire à considérer est

$$\langle \chi_V, \chi_W\rangle = \frac{1}{|G|}\sum_{g\in G} \chi_V(g)\chi_W(g^{-1}).$$

Noter que ces deux définitions sont bien les mêmes dans le cas complexes. En effet, pour un groupe fini G, si $\rho_W : G \to \mathrm{GL}(W)$ est le morphisme associé à la représentation, on a pour tout $g \in G$, si $n = |G|$, $g^n = e$ soit $\rho_W(g)^n = \mathrm{Id}$ si bien que $\rho_W(g)$ annule le polynôme scindé à racines simples sur $\mathbb{C}$ et donc il est diagonalisable et ses valeurs propres sont les racines n-ème de l'unité. On a donc que

$$\overline{\chi_W(g)} = \sum_{\xi\in\mathbb{U}_n} \overline{\xi} = \sum_{\xi\in\mathbb{U}_n} \xi^{-1} = \chi_W(g^{-1}).$$

Je vous renvoie à l'exercice 9 du TD 2 pour plus de détails sur les caractères sur un corps plus général que $\mathbb{C}$.

10. **(sur 1 point)** On pose $G = \mathfrak{S}_n$ et $X = \{1, \ldots, n\}$. On a alors $X^\sigma = k^n$ et l'action correspond à $g \cdot (x_1, \ldots, x_n) = \left(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}\right)$. Vérifions que les hypothèses de de la question **6.** sont satisfaites. On a bien que G agit transitivement sur X de sorte que $r = |G/X| = 1$. L'action est également doublement transitive [12]. En effet, soient $a \neq c$ et $b \neq d$ des éléments de X. On peut alors définir $\mu \in \mathfrak{S}_n$ par $\mu(a) = c$, $\mu(b) = d$ que l'on prolonge par n'importe quelle bijection de $X \smallsetminus \{a, b\} \to X \smallsetminus \{c, d\}$ (noter que ces deux ensembles ont bien même cardinal). On déduit alors bien des questions précédentes que $k^n = (X^\sigma)^G \oplus V$ comme somme directe de sous-G-modules irréductibles. On a déjà vu que $(X^\sigma)^G$ est la représentation triviale et les calculs effectués en question **3.** montre que [13] $(X^\sigma)^G = \mathrm{Vect}(1, 1, \ldots, 1)$. La réprésention V est irréductible de dimension $n-1$ donc non isomorphe à $(X^\sigma)^G$ dès que $n > 2$. On pourrait traiter le cas $n = 2$ à la main en regardant le caractère de V et constater que l'on retrouve la signature.
On peut aussi montrer qu'elle est non triviale, ce qui permet d'obtenir dans tous les cas que les deux sous-G-modules irréductibles obtenus sont non isomorphes. On a vu en question **5.** qu'il existait $g_0 \in G$ sans point fixe. Autrement dit, il existe $x \in X$ tel que $g_0 \cdot x \neq x$ soit $g \cdot \delta_x = \delta_{g \cdot x} \neq \delta_x$. On a donc

$$g_0 \cdot (\delta_x - p(\delta_x)) = \delta_{g_0 \cdot x} - p(\delta_x)$$

puisque $g \cdot p(f) = p(f)$ pour tous $g \in G$ et tout $f \in X^\sigma$. Il s'ensuit que

$$g_0 \cdot (\delta_x - p(\delta_x)) \neq \delta_x - p(\delta_x)$$

avec $\delta_x - p(\delta_x) \in V = \mathrm{Ker}(p)$ si bien que V n'es pas triviale !

12. On peut même montrer que $\mathfrak{A}_n$ est $n-2$ transitif ! Si cela vous intéresse, je vous renvoie au chapitre I du *Cours d'algèbre* de Perrin.
13. En effet, on a que ce sous-G-module est engendré par

$$\sum_{x \in X} \delta_x$$

qui correspond bien à $(1, \ldots, 1)$ via $X^\sigma = k^n$.