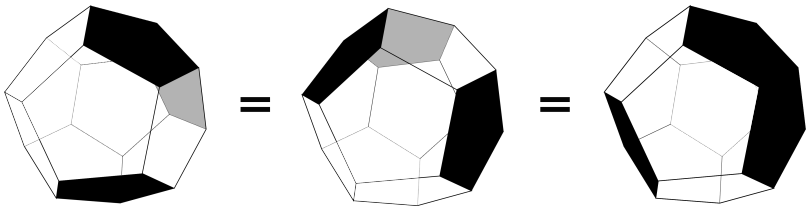
Examen du cours d'Algèbre 1, ENS Ulm, 16 Janvier 2024

Aucun document n'est autorisé. Temps de composition : 3h. Il n'est pas nécessaire de traiter toutes les questions pour avoir le maximum des points. On soignera la rédaction.

Problème 1. (Dodécaèdres noirs et blancs) *Soit* D *un dodécaèdre régulier. On se propose de déterminer le nombre de façons de colorier chaque face de* D *en noir ou en blanc, sachant que l'on identifie deux coloriages s'ils se déduisent l'un de l'autre par une rotation de* D.



(i) Déterminer le nombre de 3*-cycles, de doubles-transpositions, et de* 5*-cycles, dans* A_5.

Il y a $\binom{5}{2} \cdot 2 = 20$ *3-cycles :* $\binom{5}{2}$ *possibilités pour les deux points fixes, et il y a deux trois-cycles dans* S_3. *De même, il y a* $5 \cdot 3 = 15$ *doubles-transpositions :* 5 *possibilités pour le point fixe, et il y a* 3 *doubles-transpositions dans* S_4 *(ou* K_4*). Enfin, tout* 5*-cycle s'écrit de manière unique sous la forme* $(1\,a\,b\,c\,d)$ *avec* $\{a,b,c,d\} = \{2,3,4,5\}$*, il y en a donc* $4! = 24$.

Soit G *un groupe agissant sur un ensemble fini* X*, et soit* E *un ensemble fini de cardinal* m. *Pour* $g \in G$ *et* $\phi : X \to E$*, on définit* $g.\phi : X \to E$ *par la formule* $(g.\phi)(x) = \phi(g^{-1}x)$.

(ii) Vérifier que $(g, \phi) \mapsto g.\phi$ *est une action de* G *sur l'ensemble* E^X.

Soient $\phi \in E^X$ *et* $x \in X$. *On a* $(1.\phi)(x) = \phi(x)$ *et donc* $1.\phi = \phi$. *Pour* $g, h \in G$*, on a* $(g.(h.\phi))(x) = (h.\phi)(g^{-1}x) = \phi(h^{-1}(g^{-1}x) = \phi((gh)^{-1}x) = ((gh).\phi)(x)$ *et donc* $g.(h.\phi) = (gh).\phi$.

(iii) Soit $g \in G$. *Montrer que le nombre de points fixes de* g *dans* E^X *est de la forme* $m^{\mathrm{r}_X(g)}$*, où* $\mathrm{r}_X(g)$ *est un entier que l'on exprimera en fonction du type de la décomposition en cycles de* g *sur* X.

La fonction $\phi : X \to E$ *est fixe par* $g \in G$*, si et seulement si, on a* $\phi(g^{-1}x) = \phi(x)$ *pour tout* $x \in X$*, ou ce qui revient même,* $\phi(gx) = \phi(x)$ *pour tout* x *dans* X *(changement de variables* $x \mapsto gx$*). Autrement dit, il faut et suffit que* ϕ *soit constante sur les orbites de l'action de* $\langle g \rangle$ *sur* X*, c'est-à-dire sur les cycles intervenant dans la décomposition en cycles de* g *sur* X. *Il y a* $|E| = m$ *valeurs de* ϕ *possibles sur chaque cycles, et sur chaque point fixe. Ainsi* g *a* m^r *points fixes dans* E^X*, avec* $r := \mathrm{r}_X(g)$ *le nombre de cycles de* G *sur* X*, incluant les points fixes (« cycles de longueur 1 »).*

On suppose désormais que G *est le groupe des isométries directes d'un dodécaèdre régulier, et que* X *est l'ensemble des* 12 *faces de ce dodécaèdre, muni de l'action naturelle de* G.

(iv) Soit $g \in G \smallsetminus \{1\}$ *possédant un point fixe dans* X. *Justifier brièvement pourquoi* g *est d'ordre* 5 *et possède exactement deux points fixes dans* X.

Prenons l'origine de l'espace au centre O *du dodécaèdre donné* D. *On sait alors que* G *est un sous-groupe de* $\mathrm{SO}(3)$ *permutant les sommets de* D. *Si* $g \in G$ *fixe une face* F*, il fixe donc le centre* C

de cette face, qui est l'isobarycentre des sommets. Il fixe aussi la face $-F$ et son centre $-C$. Comme un élément non trivial de $\mathrm{SO}(3)$ n'a qu'une droite fixe, et que $-F$ est la seule de D face parallèle à F, g fixe exactement deux faces et a donc 2 points fixes dans X. Comme g induit une isométrie directe du pentagone régulier F, c'est une rotation de ce pentagone, nécessairement d'ordre 5 par le cours.

(v) *En déduire que l'action de G sur E^X a exactement $\frac{1}{60}(m^{12} + 15\,m^6 + 44\,m^4)$ orbites.*

On applique la formule de Burnside-Frobenius à cette action. Par le (iii), le nombre d'orbites est $\frac{1}{|G|}\sum_{g\in G} m^{\mathrm{r}_X(g)}$. On sait que l'on a $G \simeq \mathrm{A}_5$, donc $|G| = 60$. D'après le (i), le groupe G a 15 éléments d'ordre 2, 20 éléments d'ordre 3 et 24 éléments d'ordre 5 (avec le neutre cela fait bien $1+15+30+24 = 60$). On a $\mathrm{r}_X(1) = |X| = 12$. Par le (iv), les éléments $g \in G$ d'ordre $p = 2$ ou 3 sont sans points fixes sur X, et donc de décomposition en cycles de type $p+p+..+p = 12$: on a $\mathrm{r}_X(g) = 12/2 = 6$ pour g d'ordre 2, $\mathrm{r}_X(g) = 12/3 = 4$ pour g d'ordre 3. Enfin, pour $g \in G$ d'ordre 5, l'unique décomposition en cycles possible sur X est de type $5+5+1+1 = 12$ par le (iv), donc on a $\mathrm{r}_X(g) = 4$. Au final, on a 1 fois $\mathrm{r}_X(g) = 12$, 15 fois $\mathrm{r}_X(g) = 6$, et $20+24 = 44$ fois $\mathrm{r}_X(g) = 4$.

(vi) *Conclure.*

Un coloriage en Noir ou Blanc des faces de D est une fonction $f : X \to \{N, B\}$. Par définition, deux coloriages f, f' sont considérés équivalents si et seulement s'il existe $g \in G$ avec $g.f = f'$. Le nombre de coloriages en Noir ou Blanc non équivalents de D est donc la quantité du (v) pour $E = \{N, B\}$, i.e. *$m = 2$, puis $\frac{2^4}{60}(2^8 + 15\cdot 2^2 + 44) = \frac{4}{15}(256+60+44) = \frac{4\cdot 360}{15} = 4\cdot 24 = 96$.*

Problème 2. (Groupes auto-transitifs et critère de simplicité de Rotman) *On commence par une question préliminaire. Soit G un groupe agissant k-transitivement*[1] *sur un ensemble X, avec $k \geq 2$, et soit $x \in X$.*

(o) *Vérifier que G_x agit $(k-1)$-transitivement sur $X \smallsetminus \{x\}$.*

C'est le (i) de l'exercice corrigé 4.23.

Partie I : groupes auto-transitifs

On s'intéresse aux groupes finis G tels que l'action naturelle du groupe $\mathrm{Aut}\,G$ sur l'ensemble $G \smallsetminus \{1\}$, $(\alpha, g) \mapsto \alpha(g)$, est transitive. Dans les questions (i) à (iii) on fixe un tel groupe $G \neq \{1\}$, et on choisit un nombre premier p divisant $|G|$.

(i) *Montrer que tout élément non trivial de G est d'ordre p.*

D'après Cauchy, il existe un élément $g \in G$ d'ordre p. Soit $h \in G \smallsetminus \{1\}$. Par hypothèse, il existe $\alpha \in \mathrm{Aut}\,G$ avec $\alpha(g) = h$. Comme h est un isomorphisme $G \to G$, h et g ont même ordre p.

(ii) *Montrer $\mathrm{Z}(G) = G$.*

Le groupe G est un p-groupe. En effet, si on a ℓ premier divisant $|G|$, alors g possède un élément d'ordre ℓ par Cauchy, et donc $\ell = p$ par le (i). On sait que le centre d'un p-groupe non trivial est non trivial, donc $\mathrm{Z}(G)$ est non trivial. Fixons $x \in \mathrm{Z}(G)$ non trivial. Soit $g \in G \smallsetminus \{1\}$. Montrons $g \in \mathrm{Z}(G)$. Par hypothèse il existe $\alpha \in \mathrm{Aut}G$ avec $g = \alpha(x)$. Soit $h \in G$, comme α est bijectif il existe $y \in G$ avec $\alpha(y) = h$, puis $gh = \alpha(x)\alpha(y) = \alpha(xy) = \alpha(yx) = \alpha(y)\alpha(x) = hg$, et $g \in \mathrm{Z}(G)$.

1. On rappelle que notre convention est que si un groupe agit k-transitivement sur un ensemble X alors on a $|X| \geq k$.

(iii) En déduire que l'on a $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ avec $n \geq 1$.

Par (i) et (ii), le groupe G est abélien p-élémentaire, on conclut par le cours.

(iv) Réciproquement, montrer que pour p premier et $n \geq 1$, le groupe $(\mathbb{Z}/p\mathbb{Z})^n$ a la propriété requise.

On sait que le groupe $G = (\mathbb{Z}/p\mathbb{Z})^n$ est canoniquement un espace vectoriel $G^\sharp$ sur $\mathbb{Z}/p\mathbb{Z}$, et qu'une application $G \to G$ est un morphisme si, et seulement si, elle est $\mathbb{Z}/p\mathbb{Z}$-linéaire. Le groupe $\operatorname{Aut} G$ coïncide avec le groupe $\mathrm{GL}(G^\sharp)$ des bijections $\mathbb{Z}/p\mathbb{Z}$-linéaires de $G^\sharp$. Mais si V est un espace vectoriel de dimension finie (disons) sur un corps K, et si v et w sont deux vecteurs non nuls, on peut toujours trouver $g \in \mathrm{GL}(V)$ avec $g(v) = w$: compléter v en une base $v_1 = v, v_2, ..., v_n$, et w en une base $w_1 = w, w_2, \ldots, w_n$, et considérer l'unique g envoyant v_i sur w_i pour $i = 1, \ldots, n$.

On se donne enfin un entier $k \geq 2$ et un groupe fini G tels que l'action naturelle de $\operatorname{Aut} G$ sur $G \smallsetminus \{1\}$ est k-transitive.

(v) On suppose $k = 2$. Montrer que l'on a soit $G \simeq \mathbb{Z}/3\mathbb{Z}$, soit $G \simeq (\mathbb{Z}/2\mathbb{Z})^n$ et $n \geq 2$.

L'hypothèse sur G et $k \geq 1$ implique que $\operatorname{Aut} G$ agit transitivement $G \smallsetminus \{1\}$, donc on a $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ par le (iii). On a vu au (iv) que G peut être vu naturellement comme un K-espace vectoriel V de dimension n sur le corps $K = \mathbb{Z}/p\mathbb{Z}$, et qu'alors on a $\operatorname{Aut} G = \mathrm{GL}(V)$. Par hypothèse, le groupe $\mathrm{GL}(V)$ agit 2-transitivement sur $V \smallsetminus \{0\}$. Soit $v \in V$ non nul. Alors $\mathrm{GL}(V)_v$ agit transitivement sur $V \backslash \{0, v\}$ par le (o). Mais $\mathrm{GL}(V)_v$ préserve la droite Kv et agit trivialement sur cette droite par linéarité. On en déduit que si $Kv \smallsetminus \{0, v\}$ est non vide, i.e. $p = |K| > 2$, alors on a $V = Kv$ et $|Kv| = 3 = p$. Sinon, c'est que l'on a $Kv = \{0, v\}$ et donc $|K| = p = 2$. Dans ce cas, la convention $|G - \{1\}| \geq 2$ force $n \geq 1$.

(vi) On suppose $k \geq 3$. Montrer $k = 3$ et $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

On a $|G - \{1\}| \geq 3$ et donc $|G| \geq 4$. Par le (v), et reprenant les notations ci-dessus, G est le groupe additif d'un espace vectoriel V de dimension $n \geq 2$ sur $K = \mathbb{Z}/2\mathbb{Z}$, et on sait $\operatorname{Aut} G = \mathrm{GL}(V)$. Soient $e_1, \ldots, e_n$ une base de V. Alors $\mathrm{GL}(V)_{e_1} \cap \mathrm{GL}(V)_{e_2}$ agit transitivement sur $V \smallsetminus \{0, e_1, e_2\}$ par le (o). Mais il fixe l'élément $e_1 + e_2$. On a donc $V = \{0, e_1, e_2, e_1 + e_2\}$, puis $n = 2$.

Partie II : le critère de simplicité de Rotman

Soit G un groupe fini agissant fidèlement et k-transitivement sur un ensemble fini X, avec $k \geq 2$. Supposons qu'il existe $x \in X$ tel que le groupe G_x est simple. Suivant J. Rotman, nous allons démontrer que l'une des assertions suivantes est satisfaite :

(a) *G est simple,*

(b) *on a $k = 3$ et, soit $|X| = 3$ et $G = \mathrm{S}_X$, soit $|X|$ est une puissance de 2,*

(c) *on a $k = 2$ et $|X|$ est une puissance d'un nombre premier.*

On fixe $x_0 \in X$ tel que G_{x_0} est simple. Soit N un sous-groupe distingué de G avec $N \neq \{1\}$ et $N \neq G$.

(i) Montrer que N agit transitivement X. On pourra considérer $x \in X$ tel que $|Nx| > 1$ et montrer $X = Nx$.

Si[2] on a $Nx = \{x\}$ pour tout $x \in X$ alors N agit trivialement sur X, et donc $N = \{1\}$ car l'action de G est supposée fidèle sur X. Donc il existe x tel que $|Nx| > 1$. Vérifions que le sous-ensemble $Nx \subset X$ est stable par G. En effet, pour $g \in G$ on a $gNx = gNg^{-1}x = Nx$ car N est

2. Ce qui suit est le même argument que dans le début de la preuve du critère d'Iwasawa.

distingué dans G. Mais G_x agit transitivement sur $Y := X \smallsetminus \{x\}$ par le (o), et on a $Nx \cap Y \neq \emptyset$ car $|Nx| > 1$, donc $X \smallsetminus \{x\} \subset Nx$, puis $X = Nx$.

(ii) Montrer $N \cap G_{x_0} = \{1\}$.

Comme N est distingué dans G, on constate que $N \cap G_{x_0}$ est distingué dans G_{x_0}. Mais ce dernier est simple par hypothèse, on a donc soit $N \cap G_{x_0} = \{1\}$, soit $N \cap G_{x_0} = G_{x_0}$. Dans ce second cas, on a $G_{x_0} \subset N$. Montrons $N = G$. Soit $g \in G$. On a $gx_0 = nx_0$ pour un certain $n \in N$ par le (i), puis $n^{-1}g \in G_{x_0}$, et donc $g \in nG_{x_0} \in N$.

(iii) Vérifier que l'application $N \smallsetminus \{1\} \longrightarrow X \smallsetminus \{x_0\}, n \mapsto nx_0$, est bien définie et bijective.

L'application est bien définie par le (ii). Elle est surjective par le (i). Enfin, si on a $nx_0 = mx_0$ avec $n, m \in N$, on a $m^{-1}n \in G_{x_0} \cap N = \{1\}$ (par le (ii)), donc $m = n$: l'application est injective.

(iv) En déduire que l'action par conjugaison de G_{x_0} sur $N \smallsetminus \{1\}$ est $(k-1)$-transitive.

L'application $f : N \smallsetminus \{1\} \longrightarrow X \smallsetminus \{x_0\}, n \mapsto nx_0$ est bijective par le (iii). Le groupe G_{x_0} agit naturellement sur $X \smallsetminus \{x_0\}$. Faisons-le aussi agir par conjugaison sur $N \smallsetminus \{1\}$. On constate que f définit un isomorphisme entre ces deux actions. En effet, pour $n \in N \smallsetminus \{1\}$ et $g \in G$ on a $f(gng^{-1}) = gng^{-1}x_0 = gnx_0 = g.f(n)$ car $gx_0 = x_0$. Ainsi, comme l'action de G_{x_0} sur $X \smallsetminus \{x_0\}$ est $(k-1)$-transitive (par le (o)), il en va de même de celle par conjugaison de G_{x_0} sur $N \smallsetminus \{1\}$.

(v) Conclure.

Supposant G non simple, on dispose d'un groupe N comme ci-dessus. L'action par conjugaison de G_{x_0} sur N définit un morphisme $G_{x_0} \to \mathrm{Aut}N$, dont l'image agit $k-1$ transitivement sur $N - \{1\}$ par le (iv). En particulier, $\mathrm{Aut}\, N$ agit $k-1$-transitivement sur $N - \{1\}$. On a aussi $|N| = |X|$ par la question (iii). D'après le (vi) partie I, on a $k - 1 \leq 3$, i.e. $k \leq 4$, et dans le cas $k = 4$ on a $N \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Dans ce second cas on a $|X| = 4$, puis par 4-transitivité de $G \subset \mathrm{S}_X$, $G = \mathrm{S}_X$, ce qui est absurde car alors $G_{x_0} \simeq \mathrm{S}_3$ n'est pas simple. Si on a $k = 3$, le (v) de la partie I montre que soit $|X| = |N|$ est une puissance de 2, soit on a $|N| = |X| = 3$. Dans ce dernier cas on a nécessairement $G = \mathrm{S}_X$ par 3-transitivité. Dans le cas restant $k = 2$, la question (iii) partie I montre $|X| = |N| = p^n$ avec p premier : on est dans le cas (c).

Partie III : deux applications du critère de Rotman

(i) Montrer que la simplicité de A_5 entraîne celle de A_n pour $n \geq 6$.

Par récurrence sur $n \geq 5$. C'est l'hypothèse pour $n = 5$. Pour $n > 5$ on regarde l'action naturelle de A_n sur $\{1, \ldots, n\}$. On sait qu'elle est $n-2$ transitive. Le stabilisateur du point n est A_{n-1} qui est simple par récurrence. Comme $n - 2 > 3$, le critère de Rotman affirme que A_n est simple.

É. Mathieu a construit un sous-groupe G de S_{24} agissant 5-transitivement sur $\{1, 2, \ldots, 24\}$ et vérifiant $G_1 \cap G_2 \cap G_3 \simeq \mathrm{PSL}_3(\mathbb{F}_4)$, où G_i désigne le stabilisateur dans G de l'élément $i \in \{1, 2, \ldots, 24\}$ et $\mathbb{F}_4$ est un corps à 4 éléments. On note respectivement M_{24}, M_{23} et M_{22} les groupes G, G_1 et $G_1 \cap G_2$.

(ii) Montrer que M_{22}, M_{23} et M_{24} sont simples.[3]

3. Ce sont les trois plus gros groupes simples sporadiques découverts par Mathieu.

Par le (o), M_{22} agit 3-transitivement sur l'ensemble $\{3,4,\dots,24\}$ à 22 éléments, et le stabilisateur de 3 est $\mathrm{PSL}_3(\mathbb{F}_4)$, dont on sait qu'il est simple par le cours. Comme 22 n'est pas une puissance de 2, le critère de Rotman assure que M_{22} est simple. Ensuite, M_{23} agit 4-transivement sur l'ensemble $\{2,3,\dots,24\}$ à 23 éléments, et le stabilisateur de $\{2\}$ est le groupe simple M_{22}, donc M_{23} est simple par Rotman. On conclut de même la simplicité de M_{24} à partir de celle de M_{23}

Soient K un corps, V un K-espace vectoriel de dimension finie et u un endomorphisme de V. On rappelle que V_u désigne le $K[X]$-module de K-espace vectoriel sous-jacent V et vérifiant $Xv = u(v)$ pour tout $v \in V$. On note ${}^t u$ l'endomorphisme du dual V^* de V défini par ${}^t u(\varphi) = \varphi \circ u$ pour tout $\varphi \in V^*$ (*transposée* de u).

Problème 3. (Dualité, et actions non isomorphes de représentations de permutation associées isomorphes) *Soient K un corps, V un K-espace vectoriel de dimension finie $n \geq 1$, u un endomorphisme de V. On se propose d'abord de montrer que les $K[X]$-modules V_u et $(V^*)_{{}^t u}$ sont isomorphes.*

(i) On suppose que le $K[X]$-module V_u est isomorphe à $K[X]/(P)$ avec $P \in K[X]$ unitaire. Montrer qu'il existe $v \in V$ tel que $v, Xv, X^2v, \dots, X^{n-1}v$ est une base de V, et aussi $Pv = 0$.

Par unicité du reste de la division euclidienne d'un polynôme par P, le $K[X]$-module $K[X]/(P)$ a pour K-base les classes de 1, X, $\cdots$,X^{n-1}. Soit $f : K[X]/(P) \to V_u$ un isomorphisme $K[X]$-linéaire. On pose $v = f(\overline{1})$. Alors f est K-linéaire, et envoie la base $\overline{X^i} = X^i.\overline{1}$, avec $i = 0, \dots, n-1$, sur la base des $f(X^i.\overline{1}) = X^i f(\overline{1}) = X^i v$, avec $i = 0, \dots, n-1$. On a $Pv = Pf(\overline{1}) = f(P\overline{1}) = f(\overline{P}) = f(0) = 0$.

(ii) (suite) Montrer que le $K[X]$-module $(V^*)_{{}^t u}$ est monogène, et $P\psi = 0$ pour tout $\psi \in V^*$. On pourra considérer une forme linéaire ϕ sur V vérifiant $\phi(X^i v) = 0$ pour $0 \leq i < n-1$, et $\phi(X^{n-1}v) = 1$.

Pour $i = 0, \dots, n-1$ on pose $e_i = X^i v$. Les e_i forment une base de V par le (i). Il y a donc un sens à définir une telle ϕ. Écrivons $P = X^n + \sum_{i=0}^{n-1} a_i X^i$ avec les a_i dans K. Notons e_i^* la base duale des e_i ; on a d'abord $\phi = e_{n-1}^*$. Pour $i = 1, \dots, n-1$ on constate $X^i\phi = e_{n-i-1}^* +$ une combinaison linéaire de e_j^* avec $n-i \leq j \leq n-1$. En effet, pour $j \leq n-i-1$ on a $(X^i\phi)(e_j) = \phi(X^i e_j) = \phi(X^{i+j}v)$ qui vaut 1 pour $i+j = n-1$, 0 pour $i+j < n-1$. On en déduit que $\phi, X\phi, \dots, X^i\phi$ est une base de V^* (système triangulaire par rapport à la base $e_{n-1}^*, e_{n-2}^*, \dots, e_1^*, e_0^*$). Enfin, pour $\phi \in V^*$ et $w \in W$ on a $(P\phi)(w) = \phi(Pw) = \phi(0) = 0$.

(iii) (suite) En déduire un isomorphisme de $K[X]$-modules $(V^*)_{{}^t u} \simeq K[X]/(P)$.

Le $K[X]$-module $(V^*)_{{}^t u}$ est monogène par le (ii), donc isomorphe à $K[X]/(Q)$ pour un certain $Q \in K[X]$ unitaire, par le cours. Le degré de Q est égal à la dimension de $(V^*)_{{}^t u}$ comme K-espace vectoriel, donc $\deg Q = n$. Mais $(V^*)_{{}^t u}$ est annulé par $P \in K[X]$ par le (ii), on a donc $P.\overline{1} = 0$ puis $P \in (Q)$, Q divise P dans $K[X]$, et donc $P = Q$.

(iv) On suppose $V = \oplus_{i=1}^r V_i$ avec $V_i \subset V$ un sous-espace vectoriel stable par u pour tout $i = 1, \dots, r$, et on pose $u_i = u_{|V_i}$. Vérifier que l'on a un isomorphisme de $K[X]$-modules $\oplus_{i=1}^r (V_i^*)_{{}^t u_i} \simeq (V^*)_{{}^t u}$.

Pour $i = 1, \dots, r$ et $\phi \in V_i^*$, on note $f_i(\phi) \in V^*$ l'unique forme linéaire qui coïncide avec ϕ sur V_i et qui est nulle sur V_j avec $j \neq i$. Cela définit une application K-linéaire $f_i : V_i^* \to V^*$. Elle est clairement injective. De plus, on constate que $f_i(\phi) \circ u$ est nulle sur V_j pour $j \neq i$, et vaut $\phi \circ u_i$ sur V_i, c'est donc $f_i(\phi \circ u_i)$. Ainsi, f_i est $K[X]$-linéaire $(V_i^*)_{{}^t u_i} \to (V^*)_{{}^t u}$. Par propriété des sommes directes, il existe une unique application linéaire $f : \oplus_{i=1}^r (V_i^*)_{{}^t u_i} \to (V^*)_{{}^t u}$ envoyant

$\phi = \phi_1 + \cdots \phi_r$, avec les $\phi_i \in (V_i^*)_{{}^t u_i}$, sur $f(\phi) := f_1(\phi_1) + f_2(\phi_2) + \cdots + f_r(\phi_r)$. Cette application linéaire est clairement bijective. Elle est $K[X]$-linéaire car les f_i le sont.

(v) Conclure.

Par le théorème de structure des $K[X]$-modules de dimension finie, on sait que le $K[X]$-module V_u s'écrit $V_u = \oplus_{i=1}^r V_i$, où pour tout $i = 1, \ldots, r$ V_i est un sous-module isomorphe à $K[X]/(P_i)$ avec $P_i \in K[X]$ unitaire. Par définition, on a $V_i = (V_i)_{u_i}$ avec $u_i = u_{|V_i}$ et un léger abus de language. Par le (iii) on a $(V_i)^*_{{}^t u_i} \simeq V_i$ pour tout i, et par le (iv) on a $(V^*)_{{}^t u} \simeq \oplus_{i=1}^r (V_i)^*_{{}^t u_i}$. Cela conclut.

(vi) (Application) Montrer que toute matrice dans $\mathrm{M}_n(K)$ est semblable à sa transposée.

Soient $u \in \mathrm{End}_K(V)$ et $e_1, \ldots, e_n$ une base V. Notons $U = (u_{i,j}) \in \mathrm{M}_n(K)$ la matrice de u dans cette base : pour $1 \leq j \leq n$ on a $u(e_j) = \sum_{i=1}^n u_{i,j} e_i$. Soit $e_1^*, \ldots, e_n^*$ la base duale de V. On constate que l'on a ${}^t u(e_j^*)(e_i) = e_j^*(u(e_i)) = u_{j,i}$, autrement dit la matrice de ${}^t u$ dans cette base duale est ${}^t U$. Le (v) affirme donc exactement que U et ${}^t U$ sont semblables.

On suppose désormais que K est un corps fini. On note X l'ensemble des droites vectorielles de K^n et Y celui des hyperplans de K^n. Ces deux ensembles sont munis d'une action naturelle du groupe $G = \mathrm{GL}_n(K)$.

(vii) Montrer que tout $g \in G$ a le même nombre de points fixes dans X et dans Y.

Le nombre de points fixes de g dans X est le nombre de droites de $V = K^n$ stables par g. Le nombre de points fixes de g dans Y est le nombre d'hyperplans de V stables par g, ou ce qui revient au même, le nombre de droites de V^* stables par ${}^t g$. Mais les $K[X]$-modules V_g et $(V^*)_{{}^t g}$ étant isomorphes par (v), il existe une bijection K-linéaire $f : V \to V^*$ vérifiant $f \circ g = {}^t g \circ f$. Cette bijection induit une bijection entre les droites propres de g dans V et celles de ${}^t g$ dans V^*.

(viii) En déduire que les $\mathbb{C}[G]$-modules $\mathbb{C}\,X$ et $\mathbb{C}\,Y$ sont isomorphes.

On sait que si G agit sur un ensemble fini E, et si $\mathbb{C}\,E$ est le $\mathbb{C}[G]$-module de permutation associé, alors pour tout $g \in G$, le nombre de points fixes de g dans E coïncide avec $\chi_{\mathbb{C}\,E}(g)$. On applique ceci à $E = X$ et $E = Y$. Par le (vii), on a donc l'égalité de caractères $\chi_{\mathbb{C}\,X} = \chi_{\mathbb{C}\,Y}$. Par le cours, on en déduit que les représentations $\mathbb{C}\,X$ et $\mathbb{C}\,Y$ sont isomorphes.

(ix) Montrer que toutefois, les actions de G sur X et sur Y ne sont pas isomorphes pour $n \geq 3$.

On sait que deux actions équivalentes possèdent un stabilisateur en commun. Ainsi, si les actions sur X et Y sont équivalentes, il existe une droite D de $V = K^n$ et un hyperplan $H \subset V$ tels que le stabilisateur respectifs de D et H dans $\mathrm{GL}(V)$ coïncident. Il suffit donc de trouver $g \in \mathrm{GL}(V)$ vérifiant $g(H) = H$ et $g(D) \neq D$. Si $D \cap H = \{0\}$, on peut trouver une base $e_1, \cdots, e_n$ de V avec $e_1, \ldots, e_{n-1} \in H$ et $e_n \in D$. L'élément g défini par $g(e_i) = e_i$ pour $i < n$, et $g(e_n) = e_n + e_{n-1}$ convient. Si $D \subset H$, on peut trouver une base $e_1, \cdots, e_n$ de V avec $e_1, \ldots, e_{n-1} \in H$ et $e_1 \in D$. L'élément g défini par $g(e_1) = e_2$, $g(e_2) = e_1$, et $g(e_i) = e_i$ pour $3 \leq i \leq n$ convient et existe car $n \geq 3$.

Problème 4. (Groupes de l'année) *On se propose de montrer qu'à isomorphisme près, il existe exactement 6 groupes d'ordre $2024 = 2^3 \cdot 11 \cdot 23$ possédant un élément d'ordre 8. Soit*[4] *G un groupe d'ordre 2024.*

4. On utilisera la lettre V pour rappeler Vingt-trois, Q pour Quatre-vingt-huit, O pour Onze et H pour huit.

(i) *Montrer que G possède un unique sous-groupe distingué V d'ordre 23.*

Les sous-groupes d'ordre 23 de G sont ses 23-Sylow. Par Sylow, leur nombre $\mathrm{n}_{23}(G)$ est $\equiv 1 \bmod 23$ et divise $2^3 \cdot 11$. Les diviseurs > 23 de $2^3 \cdot 11$ sont $4 \cdot 11 = 44 \equiv -2 \bmod 23$ et $8 \cdot 11 = 88 \equiv -4 \bmod 23$. Donc G a un unique sous-groupe d'ordre 23, alors nécessairement distingué.

(ii) *En déduire que G possède un sous-groupe Q d'ordre 88, puis que l'on a $G = V \rtimes Q$.*

On a $|G| = 23 \cdot 88$ avec $23 \wedge 88 = 1$, et G a un sous-groupe distingué V d'ordre 23. D'après le théorème de Schur-Zassenhaus, V a un sous-groupe Q d'ordre 88 dans G. Par la remarque dans le cours suivant l'énoncé du théorème de Schur-Zassenhaus, un tel sous-groupe est un complément de V dans G. Ainsi, G est produit semi-direct interne de Q par V.

(iii) *Montrer que Q possède un unique sous-groupe distingué O d'ordre 11.*

On a $|Q| = 2^3 \cdot 11$. Par Sylow, on a $\mathrm{n}_{11}(Q) \equiv 1 \bmod 11$ et $\mathrm{n}_{11}(Q) \mid 8$. On en déduit que Q possède un unique sous-groupe O d'ordre 11, nécesairement distingué.

(iv) *En déduire $Q = O \rtimes H$ pour tout 2-Sylow H de Q.*

Si H est un 2-Sylow de Q, on a $|H| = 8$, puis nécessairement $H \cap O = \{1\}$ par Lagrange, et donc $|OH| = |O||H| = |Q|$ par le cours, et donc H est un complément de O et on est dans une situation de produit semi-direct interne $Q = O \rtimes H$.

(v) *Montrer que le groupe $\mathrm{Aut}\, O$ est cyclique d'ordre 10, et a un unique élément d'ordre 2, à savoir $x \mapsto x^{-1}$. Montrer que le groupe $\mathrm{Aut}\, V$ possède exactement 4 sous-groupes, cycliques et engendrés par les automorphismes $v \mapsto v^i$ avec $i \in \{1, -1, 2, -2\}$. On donne la congruence $2^{11} \equiv 1 \bmod 23$.*

D'après le cours, si C est cyclique d'ordre p, alors $\varphi_C : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathrm{Aut}\, C, \bar{i} \mapsto (x \mapsto x^i)$, est un isomorphisme de groupes. Si p est premier, $\mathrm{Aut}\, C \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ est donc cyclique d'ordre $p-1$, d'après Gauss. En particulier, $\mathrm{Aut}\, C$ a un unique élément d'ordre 2, égal à $x \mapsto x^{-1}$ (i.e. $\varphi_C(-1)$), car -1 est l'élément d'ordre 2 de $(\mathbb{Z}/p\mathbb{Z})^\times$. Cela montre la première assertion ($C = O$, $p = 11$). Un groupe cyclique d'ordre 22 a un unique sous-groupe d'ordre d pour chaque diviseur d de 22, i.e. $d = 1, 2, 11, 22$. On conclut car $1, -1, 2$ et -2 sont d'ordre respectifs 1, 2, 11 (par la donnée) et 22 (par Cauchy) dans $(\mathbb{Z}/23\mathbb{Z})^\times$.

On suppose désormais que G possède un élément d'ordre 8, et on fixe un 2-Sylow H de Q.

(vi) *Montrer $H \simeq \mathbb{Z}/8\mathbb{Z}$.*

Les 2-Sylow de G sont ses sous-groupes d'ordre 8. Ils sont tous conjugués dans G par Sylow, et en particulier tous isomorphes. Si G possède élément d'ordre 8, i.e. un sous-groupe cyclique d'ordre 8, tous ses sous-groupes d'ordre 8 sont donc cycliques. Donc $H \leq Q \leq G$ est cyclique.

On fixe dans ce qui suit un générateur h de H.

(vii) *En considérant un morphisme de groupes $H \to \mathrm{Aut}\, O$ bien choisi, montrer que soit Q est abélien, soit on a $hxh^{-1} = x^{-1}$ pour tout $x \in O$.*

L'action de H par conjugaison sur le sous-groupe distingué O de Q définit un morphisme de groupes $f : H \to \mathrm{Aut}\, O, g \mapsto (x \mapsto gxg^{-1})$. Par le (v), on sait que $\mathrm{Aut}\, O$ est cyclique d'ordre 10 et a $x \mapsto x^{-1}$ pour seul élément d'ordre 2. L'image $f(H) = \langle f(h) \rangle$ est un sous-groupe d'ordre divisant $|H| = 2^8$ et $|\mathrm{Aut}\, O| = 10$, il est donc d'ordre 1 ou 2, et $f(h)$ est donc d'ordre 1 ou 2. On a donc soir $f(h) = 1$, et $Q = O\langle h \rangle$ est abélien, soit $f(h)$ est $x \mapsto x^{-1}$.

(viii) *Montrer que si Q est abélien, il est cyclique.*

Le groupe Q est d'ordre 11, donc cyclique, disons engendré par g. Comme g et h commutent, gh est d'ordre $11 \cdot 8 = 88$ dans Q par Cauchy.

(ix) *On suppose Q cyclique. Montrer qu'il existe un générateur g de Q, et $i \in \{1, -1, 2, -2\}$, tels que pour tout $v \in V$ on a $gvg^{-1} = v^i$.*

On regarde l'action de Q par conjugaison sur le sous-groupe distingué V de G, qui est un morphisme $f : Q \to \operatorname{Aut} V, g \mapsto (v \mapsto gvg^{-1})$. La question (vii) conclut si on observe que si on a un morphisme surjectif $\varphi : C \to C'$ entre groupes cycliques, tout générateur de C' est image d'un générateur de C. En effet, si g est un générateur de C, $\varphi(g)$ engendre C'. Tout autre générateur de C' est de la forme $\varphi(g)^k$ avec $k \wedge |C'| = 1$. Par Bézout, on peut trouver $k' \in \mathbb{Z}$ avec $k' \equiv k \bmod |C'|$ et $k' \equiv 1 \bmod p$ pour tout premier p divisant $|C|$ mais pas $|C'|$. Un tel k' vérifie $k' \wedge |C| = 1$, et le générateur $g^{k'}$ de C convient.

(x) *On suppose Q non cyclique. Montrer qu'il existe $i \in \{1, -1\}$ tel que pour tout $v \in V$, et tout $x \in O$, on a $hvh^{-1} = v^i$ et $xvx^{-1} = v$.*

On regarde encore l'action par conjugaison $f : Q \to \operatorname{Aut} V$ de Q sur V (comme au (viii)). L'élément $f(h)$ est d'ordre 1 ou 2, donc $f(h) = \mathrm{id}$ ou $f(h)$ est $v \mapsto v^{-1}$. Pour $x \in O$ on a $f(x)^{11} = 1$. On a aussi $f(hxh^{-1}) = f(h)f(x)f(h)^{-1} = f(x)$ car $\operatorname{Aut} V$ commutatif, et $f(hxh^{-1}) = f(x^{-1}) = f(x)^{-1}$, donc $f(x)^2 = 1$. Donc $f(x)$ est d'ordre 1, i.e. $f(x) = 1$.

(xi) *Conclure.*

Remarquons que G étant donné, V est l'unique sous-groupe distingué d'ordre 23 de G (donc canonique) et Q étant choisi, la décomposition $G = V \rtimes Q$ montre $G/V \simeq Q$, donc la classe d'isomorphisme de Q est ne dépend que de celle de G. De plus, l'image du morphisme naturel défini par conjugaison $G \to \operatorname{Aut} V$ (trivial sur V) est aussi bien défini à isomorphisme près : on la note I. En particulier, $|I|$ est ne dépend également que de la classe d'isomorphisme de G.

Pour $i = 1, -1, 2, -2$, notons $\varphi_i : \mathbb{Z}/88\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/23\mathbb{Z}$ le morphisme envoyant $\overline{1}$ sur l'automorphisme $x \mapsto ix$ (bien défini car $\overline{i} \in (\mathbb{Z}/23\mathbb{Z})^\times$ est d'ordre 1, 2, 11, 22 respectivement) et posons $G_i = \mathbb{Z}/23\mathbb{Z} \rtimes_{\varphi_i} \mathbb{Z}/88\mathbb{Z}$. Dans ces 4 cas, I est d'ordre 1, 2, 11 et 22 respectivement : les groupes G_i sont 2 à 2 non isomorphes. Si le groupe Q est abélien, donc cyclique par le (viii), alors d'après (ii) et (xi), on a $G \simeq G_i$ pour $i \in \{1, -1, 2, -2\}$.

Dans le cas restant, Q est isomorphe au groupe $Q_0 := \mathbb{Z}/11\mathbb{Z} \rtimes_\varphi \mathbb{Z}/8\mathbb{Z}$ avec $\varphi : \mathbb{Z}/8\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/11\mathbb{Z}$ envoyant $\overline{1}$ sur $x \mapsto -x$, d'après le (vii). Posons $G_0 = \mathbb{Z}/23\mathbb{Z} \rtimes_\psi Q_0$ où $\psi : Q_0 \to \operatorname{Aut} \mathbb{Z}/23\mathbb{Z}$ est le morphisme obtenu en composant la projection canonique $Q_0 \to \mathbb{Z}/8\mathbb{Z}$ et le morphisme $\mathbb{Z}/8\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/23\mathbb{Z}$ envoyant $\overline{1}$ sur $x \mapsto -x$. D'après (ii) et (x), on a soit $G \simeq \mathbb{Z}/23\mathbb{Z} \times Q_0$, soit $G \simeq G_0$. Ces deux groupes ne sont pas isomorphes : pour le premier on a $|I| = 1$, et pour le second $|I| = 2$. On a bien trouvé $4 + 2 = 6$ possibilités pour G.