UNIVERSITÉ DE BORDEAUX
M1, Théorie de Galois et représentations des groupes finis
2024-2025

Corrigé de l'examen du 10 janvier 2024.

Durée 3h. Documents non-autorisés.

Partout dans ce sujet, p désigne un nombre premier $\geqslant 3$. L'hypothèse de primalité de p n'est vraiment nécessaire que pour une partie des questions. Les deuxième, troisième et quatrième parties sont indépendantes entre elles, mais dépendent toutes de la première partie du sujet.

Première partie : le groupe Aff_p.

Pour $a \in (\mathbf{Z}/p\mathbf{Z})^*$ et $b \in \mathbf{Z}/p\mathbf{Z}$, on note $f_{a,b}\colon \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ l'application affine : $x \mapsto ax + b$. Soit Aff_p l'ensemble de ces applications. On définit la loi de composition usuelle sur Aff_p en posant :

$$(f_{a,b} \circ f_{c,d})(x) = f_{a,b}(f_{c,d}(x)), \qquad \forall x \in \mathbf{Z}/p\mathbf{Z}.$$

Si M et N sont deux parties de Aff_p, on pose $MN = \{m \circ n \mid m \in M, n \in N\}$. On note $e = f_{1,0}$ l'application identité sur $\mathbf{Z}/p\mathbf{Z}$.

Rappelons que si P est un sous-groupe d'un groupe G, on appelle *normalisateur de P* le sous-groupe

$$N(P) = \{g \in G \mid g^{-1}Pg \subset P\}.$$

On en déduit facilement que $N(P)$ est le plus grand sous-groupe de G dans lequel P est distingué.

(1) Montrer que Aff_p est un groupe pour la composition $\circ$, d'ordre $p(p-1)$.

Solution. a) Il est clair que Aff_p contient $|(\mathbf{Z}/p\mathbf{Z})^*| \cdot |\mathbf{Z}/p\mathbf{Z}| = (p-1)p$ éléments.

b) Pour montrer que Aff_p est un groupe, on remarque que

$$(f_{a,b} \circ f_{c,d})(x) = f_{a,b}(cx + d) = (ac)x + (ad + b) = f_{ac,ad+b}(x).$$

Donc $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$. En particulier, $\circ$ est une loi de composition interne. Comme la composition d'applications est associative, $\circ$ est associative. En utilisant la formule précédente, on obtient que $f_{a,b} \circ f_{1,0} = f_{a,b}$ et $f_{1,0} \circ f_{a,b} = f_{a,b}$. Donc $f_{1,0}$ est un élément neutre pour $\circ$. Si $f_{c,d}$ est l'inverse de $f_{a,b}$, on doit avoir

$$f_{a,b} \circ f_{c,d} = f_{ac,ad+b} = f_{1,0}.$$

On en déduit que $ac = 1$ et $ad + b = 0$, d'où $c = a^{-1}$ et $d = -ba^{-1}$. Donc $f_{a,b}^{-1} = f_{a^{-1},-ba^{-1}}$. On conclut que Aff_p est un groupe.

(2) Montrer que l'ensemble des translations $T := \{t_b\colon x \mapsto x + b,\ b \in \mathbf{Z}/p\mathbf{Z}\}$ est un sous-groupe distingué de Aff_p isomorphe à $\mathbf{Z}/p\mathbf{Z}$. Montrer que l'ensemble des homothéties $H := \{h_a\colon x \mapsto a \cdot x,\ a \in (\mathbf{Z}/p\mathbf{Z})^*\}$ est un sous-groupe de Aff_p isomorphe à $(\mathbf{Z}/p\mathbf{Z})^*$.

Solution. a) Soient $t_{b_1}, t_{b_2} \in T$. Alors $t_{b_1} \circ t_{b_2}^{-1} = t_{b_1} \circ t_{-b_2} = t_{b_1 - b_2} \in T$. Donc T est un sous-groupe de Aff_p. Pour tous $f_{a,b} \in \mathrm{Aff}_p$ et $t_c \in T$, on a

$$f_{a,b}^{-1} \circ t_c \circ f_{a,b} = f_{a^{-1},-ba^{-1}} \circ f_{a,b+c} = f_{1,a^{-1}c} = t_{a^{-1}c} \in T.$$

Donc T est un sous-groupe distingué. Il est facile de voir que l'application

$$\mathbf{Z}/p\mathbf{Z} \to T, \qquad b \mapsto t_b$$

est un isomorphisme.

b) Pour tous $h_a, h_b \in H$, on a

$$h_a \circ h_b^{-1} = f_{a,0} \circ f_{b,0}^{-1} = f_{a,0} \circ f_{b^{-1},0} = f_{ab^{-1},0} = h_{ab^{-1}}.$$

Donc H est un sous-groupe. On voit facilement que l'application

$$(\mathbf{Z}/p\mathbf{Z})^* \to H, \qquad a \mapsto h_a$$

est un isomorphisme.

(3) Montrer que $T \cap H = \{e\}$ et que $\mathrm{Aff}_p = TH$. *Rappelons que, avec la question (2), cela implique que* Aff_p *est le produit semi-direct de* T *et* H.

Solution. a) Soit $f_{a,b} \in T \cap H$. Alors $a = 1$ et $b = 0$, donc $f_{a,b} = f_{1,0} = e$.

b) On voit facilement que $f_{a,b} = f_{1,b} \circ f_{a,0} = t_b \circ h_a$. Donc $f_{a,b} \in TH$.

(4) On a une bijection entre $I_p = \{1, 2, \ldots, p\}$ et $\mathbf{F}_p$ qui à tout $m \in I_p$ associe la classe de m modulo p. On considère le morphisme

$$\varphi : \mathrm{Aff}_p \to S_p$$

à valeurs dans le groupe symétrique S_p qui à toute fonction $f_{a,b} \in \mathrm{Aff}_p$ associe l'application $\varphi(f_{a,b}) : I_p \to I_p$ donnée par la formule $(\varphi(f_{a,b}))(m) = f_{a,b}(m)$. Prouver que cette bijection identifie Aff_p avec le normalisateur $N(P)$ du groupe cyclique P engendré par le p-cycle $(1, 2, \ldots, p)$. Indication : montrer d'abord que le normalisateur du sous-groupe cyclique engendré par le p-cycle $(1, 2, \ldots, p)$ est d'ordre $p(p-1)$.

Solution. a) Soit $\sigma \in S_p$. Alors $\sigma \in N(P)$ si et seulement si $\sigma \circ (1, 2, \ldots, p)\sigma^{-1} = (1, 2, \ldots, p)^k$ pour certain $1 \leqslant k \leqslant p-1$. Comme

$$\sigma \circ (1, 2, \ldots, p)\sigma^{-1} = (\sigma(1), \sigma(2), \ldots, \sigma(p)),$$

on obtient que $\sigma \in N(P)$ si et seulement si

$$(\sigma(1), \sigma(2), \ldots, \sigma(p)) = (1, 2, \ldots, p)^k.$$

Pour un k fixé posons $(a_{k,1}, a_{k,2}, \ldots a_{k,p}) = (1, 2, \ldots, p)^k$. Alors on voit qu'il existe exactement p permutations σ vérifiant $(\sigma(1), \sigma(2), \ldots, \sigma(p)) = (a_{k,1}, a_{k,2}, \ldots a_{k,p})$, à savoir :

σ_1 définit par $\sigma_1(1) = a_{k,1}$, $\sigma_1(2) = a_{k,2}, \ldots, \sigma_1(p) = a_{k,p}$;

σ_2 définit par $\sigma_2(1) = a_{k,2}$, $\sigma_2(2) = a_{k,3}, \ldots, \sigma_2(p) = a_{k,1}$;

.....

σ_p définit par $\sigma_p(1) = a_{k,p}$, $\sigma_p(2) = a_{k,1}, \ldots, \sigma_p(p) = a_{k,p-1}$.

Comme k parcourt $p-1$ valeurs, on trouve que $|N(P)| = (p-1)p$.

b) L'application φ envoie t_1 sur le cycle $(1, 2, \ldots, p)$. Comme T est distingué dans Aff_p, l'image $\varphi(\mathrm{Aff}_p)$ de Aff_p est contenue dans $N(P)$. D'autre part, $|\mathrm{Aff}_p| = p(p-1) = |N(P)$. Donc φ établit un isomorphisme entre Aff_p et $N(P)$.

Deuxième partie : le corps de décomposition de $X^p - a$.

Soit maintenant K un corps de caractéristique nulle et $a \in K$. On considère un corps de décomposition E du polynôme $P(X) = X^p - a \in K[X]$.

(1) Montrer que E contient une racine p-ième de a, qu'on note α, et une racine p-ième primitive de l'unité, qu'on note ζ et que $E = K[\alpha, \zeta]$.

Solution. Soit α une racine de $P(X)$. Alors α est une racine $p$ème de l'unité et les autres racines de $P(X)$ sont de la forme $\zeta^i\alpha$, où ζ est une racine fixée d'ordre p de l'unité et $0 \leqslant i \leqslant p-1$. On en déduit que

$$E = K[\alpha, \zeta\alpha, \ldots, \zeta^{p-1}\alpha] \subset K[\zeta, \alpha].$$

D'autre part, comme $\zeta = (\zeta\alpha)\alpha^{-1}$, on voit que $K[\zeta, \alpha] \subset E$. Donc $K[\zeta, \alpha] = E$.

(2) Soit $\sigma \in \mathrm{Gal}(E/K)$. Montrer que σ envoie ζ sur une de ses puissances $\zeta^{a(\sigma)}$, avec $a(\sigma) \in (\mathbf{Z}/p\mathbf{Z})^*$. Montrer que σ envoie α sur $\zeta^{b(\sigma)}\alpha$, pour un $b(\sigma) \in \mathbf{Z}/p\mathbf{Z}$.

Solution. a) Les racines du polynôme $X^p - 1$ sont de la forme ζ^i, $0 \leqslant i \leqslant p-1$. D'après le cours, on a $\sigma(\zeta) = \zeta^{a(\sigma)}$ pour certain $a(\sigma) \not\equiv 0 \pmod{p}$. Ici $a(\sigma)$ est défini de façon unique modulo p et pour simplifier la notation, nous allons écrire $a(\sigma)$ aussi pour sa classe dans $(\mathbf{Z}/p\mathbf{Z})^*$.

b) L'action de σ permute les racines de $X^p - a$, donc $\sigma(\alpha) = \zeta^{b(\sigma)}\alpha$ pour certain $b(\sigma) \in \mathbf{Z}/p\mathbf{Z}$.

(3) Montrer que l'application $\psi\colon \sigma \mapsto f_{a(\sigma),b(\sigma)}$ définit un morphisme injectif de groupes de $\mathrm{Gal}(E/K)$ dans Aff_p.

Solution. Comme E est engendré sur K par ζ et α, tout $\sigma \in \mathrm{Gal}(E/K)$ est complètement défini par son action sur ces deux éléments. On en déduit que l'application $\psi\colon \sigma \mapsto f_{a(\sigma),b(\sigma)}$ est injective. Pour montrer qu'elle est un morphisme de groupes, on calcule l'action du produit $\sigma\tau$ ($\sigma, \tau \in \mathrm{Gal}(E/K)$) sur ζ et α :

$$\sigma\tau(\zeta) = \sigma(\zeta^{a(\tau)}) = \sigma(\zeta)^{a(\tau)} = \zeta^{a(\sigma)a(\tau)};$$

$$\sigma\tau(\alpha) = \sigma(\alpha\zeta^{b(\tau)}) = \sigma(\alpha)\sigma(\zeta^{b(\tau)}) = \alpha\zeta^{b(\sigma)+a(\sigma)b(\tau)}.$$

Donc

$$\psi(\sigma\tau) = f_{a(\sigma)a(\tau),a(\sigma)b(\tau)+b(\sigma)} = f_{a(\sigma),b(\sigma)} \circ f_{a(\tau),b(\tau)} = \psi(\sigma) \circ \psi(\tau).$$

(4) Lorsque $K = \mathbf{Q}$ et $a = 2$, montrer que l'application ψ de la question précédente est un isomorphisme.

Solution. Comme $X^p - 2$ est un polynôme d'Eisenstein, $[\mathbf{Q}[\alpha] : \mathbf{Q}] = p$. D'autre part, on sait que $[\mathbf{Q}[\zeta] : \mathbf{Q}] = p - 1$. Par le théorème de la base télescopique, on en déduit que les entiers p et $p - 1$ divisent $[E : \mathbf{Q}]$, d'où on tire que $p(p - 1)$ divise $[E : \mathbf{Q}]$. D'autre part, $[E : \mathbf{Q}] \leqslant p(p - 1)$. Donc $[E : \mathbf{Q}] = p(p - 1)$. On en déduit que $\mathrm{Gal}(E/K)$ est d'ordre $p(p - 1)$. On en déduit que ψ est surjectif, donc un isomorphisme.

Troisième partie : certaines extensions résolubles.

Dans cette partie, on considère un polynôme irréductible $f(X) \in K[X]$ de degré p et l'on note K_f son corps de décomposition. On suppose que $f(X)$ possède la propriété suivante : $K_f = [\alpha_1, \alpha_2]$, où α_1 et α_2 sont deux racines distinctes de $f(X)$. On pose $G = \mathrm{Gal}(K_f/K)$. Rappelons que l'action de G sur les racines de $f(X)$ permet de voir G comme un sous-groupe de S_p. *Dans cette partie, l'hypothèse de primalité de p est cruciale.*

(1) Montrer que p divise $[K_f : K]$ et que $[K_f : K] \leqslant p(p - 1)$.

Solution. a) Comme $[K[\alpha_1] : K] = \deg(f) = p$, le nombre p divise $[K_f : K] = [K_f : K[\alpha_1]] \cdot [K[\alpha_1] : K]$.

b) On écrit $f(X)$ sous la forme $f(X) = (X - \alpha_1)g(X)$, où $g(X)$ est un polynôme à coefficients dans $K[\alpha_1]$. Comme α_2 est une racine de $g(X)$, on trouve que $[K[\alpha_1, \alpha_2] : K[\alpha_1]] \leqslant p - 1$. Donc

$$[K_f : K] = [K[\alpha_1, \alpha_2] : K[\alpha_1]] \cdot [K[\alpha_1] : K] \leqslant (p - 1)p.$$

(2) Montrer que G possède un unique p-sous-groupe de Sylow.

Solution. Par la question précédente, $|G| = [K_f : K] \leqslant p(p - 1)$.

Soit n_p le nombre de p-sous-groupes de Sylow de G. Par un théorème de Sylow, $n_p \equiv 1 \pmod p$. D'autre part, n_p divise $|G|$. On en déduit facilement que $n_p = 1$.

(3) En utilisant la question (4) de la première partie, prouver que G est isomorphe à un sous-groupe du groupe Aff_p. En déduire que l'extension K_f/K est résoluble.

Solution. On peut voir G comme un sous-groupe de S_p (les éléments de G permutent les racines de f). Soit P le groupe de Sylow de G. Il est d'ordre p, donc cyclique. Comme les éléments d'ordre p de S_p sont les p-cycles, P est engendré par un p-cycle. Comme tout conjugué de P est un sous-groupe de Sylow, il découle de la question précédente que $\sigma^{-1}P\sigma = P$ pour tout $\sigma \in G$. On en déduit que $G \subset N(P)$ dans S_p. Or $N(P)$ est isomorphe à Aff_p, d'où le résultat.

Quatrième partie. Les représentations du groupe Aff_p. Dans cette partie, on étudie les représentations linéaires de Aff_p.

(1) Déterminer les classes de conjugaison de Aff_p (il y en a p).

Solution. On utilise la formule

$$f_{b,c}^{-1} \circ h_a \circ f_{b,c} = f_{b^{-1},-cb^{-1}} \circ f_{ab,ac} = f_{a,b^{-1}c(a-1)}.$$

Si $a \neq 1$, on voit que la classe de conjugaison de h_a est $C(h_a) = \{f_{a,d} \mid d \in \mathbf{Z}/p\mathbf{Z}\}$. En particulier, elle contient p éléments. En utilisant la formule (cf. question 2) de la première partie) $f_{a,b}^{-1} \circ t_c \circ f_{a,b} = t_{a^{-1}c}$, on trouve que $C(t_1) = \{t_a \mid a \in (\mathbf{Z}/p\mathbf{Z})^*\}$. Aussi $C(e) = \{e\}$. Ça nous donne au total

$$(p-2)p + (p-1) + 1 = p(p-1) = |G|$$

éléments. Donc on a trouvé toutes les classes de conjugaison de Aff_p, à savoir $C(h_a)$ ($a \in (\mathbf{Z}/p\mathbf{Z})^* \setminus \{1\}$), $C(t_1)$ et $C(e)$.

(2) Décrire $p-1$ représentations de degré 1 de Aff_p. Indication : déterminer d'abord le groupe dérivé de Aff_p.

Solution. a) Calculons le commutateur $[t_c, f_{a,b}]$:

$$[t_c, f_{a,b}] := t_c^{-1} \circ f_{a,b}^{-1} \circ t_c \circ f_{a,b} = t_{-c} \circ t_{a^{-1}c} = t_{c(a^{-1}-1)}.$$

On en déduit que tout élément de t_d de T s'écrit sous la forme $[t_c, f_{a,b}]$ (il faut choisir $a \neq 1$ et c tels que $c(a^{-1}-1) = d$). Donc T est contenu dans le groupe dérivé $D(\mathrm{Aff}_p)$ de Aff_p. Réciproquement, comme T est un sous-groupe normal et le groupe quotient Aff_p/T est abélien, on a $D(\mathrm{Aff}_p) \subset T$. Donc $D(\mathrm{Aff}_p) = T$.

b) On a $\mathrm{Aff}_p/D(\mathrm{Aff}_p) = \mathrm{Aff}_p/T \simeq H$. Comme les représentations de degré 1 de Aff_p correspondent aux caractères de $\mathrm{Aff}_p/D(\mathrm{Aff}_p)$, on conclut que ces représentations sont classifiées par les caractères du groupe H. Comme $|H| = p-1$, il existe, à un isomorphisme près, exactement $p-1$ représentations de Aff_p de degré 1.

(3) Montrer qu'il n'existe (à isomorphisme près) qu'une représentation irréductible de degré > 1 de Aff_p, appelons-là ρ, et déterminer son degré n_ρ.

Solution. Le nombre de représentations irréductibles de Aff_p est égal au nombre de classes de conjugaison de Aff_p. Comme Aff_p admet $p-1$ représentations de degré 1 et p classes de conjugaison, il existe une unique représentation irréductible ρ de degré > 1 de Aff_p. Pour calculer n_ρ utilisons la formule

$$\sum_\chi n_\chi^2 = |\mathrm{Aff}_p|.$$

Dans notre cas, elle s'écrit :

$$n_\rho^2 + (p-1) \cdot 1^2 = p(p-1),$$

d'où $n_\rho = p-1$.

(4) Dresser la table des caractères de Aff_p.

Solution.

(5) Notons V le $\mathbf{C}$-espace vectoriel des applications de $\mathbf{F}_p$ dans $\mathbf{C}$. Montrer qu'il est naturellement muni d'une action de Aff_p, et décomposer V en somme de représentations irréductibles de Aff_p.

Solution. Soit g un générateur fixé du groupe cyclique H et soit ζ_{p-1} une racine primitive d'ordre $p-1$ de l'unité. Alors les caractères du groupe H sont de la forme $\psi_i(g^k) = \zeta_{p-1}^{ik}$ où $0 \leqslant i \leqslant p-2$. Soit χ_i le caractère du groupe Aff_p associé à ψ_i, i.e. χ_i est la composition de la projection canonique $\mathrm{Aff}_p \to \mathrm{Aff}_p/T \simeq H$ avec $\psi_i : H \to \mathbf{C}^*$. Alors les valeurs de χ_i sur les classes de conjugaison sont :

$\chi_i = 1$ sur $C(e) = \{e\}$, $\chi_i = 1$ sur $C(t_1)$, $\chi_i = \psi_i(g^k) = \zeta_{p-1}^{ik}$ sur les classes $C(h_{g^k})$, $1 \leqslant k \leqslant p-1$.

Pour déterminer χ_ρ pour l'unique représentation ρ de degré $p-1$ il suffit de trouver une fonction centrale orthogonale aux χ_i et telle que $\sum_{g \in \mathrm{Aff}_p} |\chi_\rho(g)|^2 = |\mathrm{Aff}_p| =$

$p(p-1)$. En outre, on sait que $\chi_\rho(e) = p-1$. Alors on voit qu'en posant $\chi_\rho = -1$ sur $C(t_1)$ et $\chi_i = 0$ sur les classes $C(h_{g^k})$, $1 \leqslant k \leqslant p-1$, on obtient la fonction voulue.

(6) Notons V le $\mathbf{C}$-espace vectoriel des applications de $\mathbf{F}_p$ dans $\mathbf{C}$. Montrer qu'il est naturellement muni d'une action de Aff_p, et décomposer V en somme de représentations irréductibles de Aff_p.

Solution. a) Pour toute application $F : \mathbf{F}_p \to \mathbf{C}$, posons

$$(\sigma F)(x) = F(\sigma^{-1}(x)), \qquad \sigma \in \mathrm{Aff}_p, \quad x \in \mathbf{F}_p.$$

Alors pour tous $\sigma, \tau \in \mathrm{Aff}_p$ on a

$$((\sigma\tau)F)(x) = F(\tau^{-1}\sigma^{-1}(x)) = (\sigma(\tau F))(x).$$

Donc $(\sigma\tau)F = \sigma(\tau F)$, et l'espace V est muni d'une action à gauche de Aff_p. Il est facile de voir que V est une représentation de Aff_p pour cette action. Les fonctions

$$F_a(x) = \begin{cases} a, & \text{si } x = a, \\ 0, & \text{sinon,} \end{cases} \qquad a \in \mathbf{F}_p$$

forment une base de V sur $\mathbf{C}$, donc $\dim_{\mathbf{C}}(V) = p$.

b) Supposons que U est une sous-représentation de V de degré 1. Alors Aff_p agit sur U par un caractère χ. En particulier, pour tout $t_b \in T$ on doit avoir $t_b(F) = \chi(t_b)F = F$ puisque $T \subset \ker(\chi)$. Or $t_b(F) = F(x+b)$, d'où on tire que $F(x+b) = F(x)$ pour tout $b \in \mathbf{F}_p$. On en déduit que l'espace des fonctions constantes C est l'unique sous-représentation de degré 1 de Aff_p. L'action de Aff_p sur C est triviale. Comme V se décompose en somme directe de représentations irréductibles et ρ est l'unique (à isomorphisme près) représentation irréductible de degré > 1, on en déduit que V se décompose en somme directe de la représentation triviale de dimension 1 et de ρ.

FIN.