Vincent Beck

Examen du 12 janvier 2011

La clarté de l'argumentation de même que la qualité de la rédaction seront des éléments importants dans l'appréciation de la copie.

Les seuls documents autorisés sont les notes personnelles (cours et TD), les transparents de cours et les feuilles de TD.

Les résultats **démontrés** *en cours et en TD peuvent être utilisés librement en citant précisément la référence.*

L'examen est composé de trois exercices indépendants. Le premier est consacré aux représentations des groupes et étudie les représentations du groupe affine sur un corps fini. Les deux autres exercices mélangent théorie de Galois et représentation de groupes. L'exercice 2 étudie un exemple concret tandis que l'exercice 3 est plus théorique.

Exercice 1 – Groupe affine sur un corps fini. Soit p un nombre premier et $q = p^n$ une puissance de p. On considère $\mathbb{F}_q$ un corps à q éléments et on considère l'ensemble des applications de la forme

$$\varphi_{a,b} \colon \begin{cases} \mathbb{F}_q \longrightarrow \mathbb{F}_q \\ x \longmapsto ax + b \end{cases}$$

où $a, b \in \mathbb{F}_q$.

a) Montrer que $\varphi_{a,b}$ est bijective si et seulement si $a \in {\mathbb{F}_q}^\times$. Dans ce cas, décrire la bijection inverse.

b) Pour $a, b, c, d \in \mathbb{F}_q$, calculer $\varphi_{c,d} \circ \varphi_{a,b}$. En déduire que l'ensemble des $\varphi_{a,b}$ pour $a \in \mathbb{F}_q^\times$, $b \in \mathbb{F}_q$ forme un sous-groupe du groupe des bijections de $\mathbb{F}_q$. On le note G.

c) Déterminer $|\mathrm{G}|$ (on pourra montrer que l'application $(a, b) \mapsto \varphi_{a,b}$ est injective).

d) Construire un morphisme surjectif de groupes de G dans ${\mathbb{F}_q}^\times$ (on pourra se servir du calcul de la question **b**).

On suppose dans la suite de l'exercice que $q \neq 2$ c'est-à-dire qu'il existe un élément a dans $\mathbb{F}_q$ qui est à la fois non nul et distinct de 1.

e) Déterminer le groupe dérivé de G (on donnera les couples (a, b) tels que $\varphi_{a,b} \in \mathrm{D}(\mathrm{G})$).

f) Déterminer un isomorphisme entre $\widehat{\mathrm{G}}$ le groupe des caractères linéaires de G à valeurs dans $\mathbb{C}^\times$ et un groupe bien connu.

g) Déterminer les classes de conjugaison de G (pour un élément de la forme $\varphi_{a,b}$, on donnera les couples de (a', b') tel que $\varphi_{a',b'}$ est un conjugué de $\varphi_{a,b}$).

h) Montrer que G admet une unique classe d'isomorphisme de représentations irréductibles de dimension strictement plus grande que 1. On la note V.

i) Décrire une action de G sur $\mathbb{F}_q$. En déduire une représentation P de G sur $\mathbb{C}$ de dimension q.

j) Calculer χ_{P} et $\langle \chi_{\mathrm{P}}, \mathbf{1} \rangle_{\mathrm{G}}$. En déduire la multiplicité de la représentation triviale dans P.

k) En déduire que $\chi = \chi_{\mathrm{P}} - \mathbf{1}$ est un caractère de G puis que χ est un caractère irréductible de G. En déduire que $\chi = \chi_{\mathrm{V}}$.

l) Pour γ un caractère linéaire de G, décomposer $\mathrm{V} \otimes \gamma$ en représentations irréductibles.

m) Déterminer les multiplicités des irréductibles dans $\mathrm{V} \otimes \mathrm{V}$ (on pourra remarquer que $\mathrm{V}^* \overset{\text{G-mod.}}{\simeq} \mathrm{V}$).

n) Dresser la table de caractère de G lorsque $q = 5$.

Exercice 2 – Représentation d'un groupe de Galois. On considère $\mathrm{P} = \mathrm{X}^3 - 5 \in \mathbb{Q}[\mathrm{X}]$. Soit K le corps de décomposition de P sur $\mathbb{Q}$.

a) Montrer que P est irréductible sur $\mathbb{Q}$.

b) Montrer que K est une extension galoisienne de $\mathbb{Q}$ dont on déterminera la dimension.

c) Déterminer un isomorphisme entre $\mathrm{G} := \mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ et $\mathfrak{S}_3$ (on pourra considérer les racines de P dans K).

d) Déterminer l'ensemble des sous-$\mathbb{Q}$-extensions de K, leur degré et un élément primitif de chacun. Parmi ces sous-corps, lesquels sont des extensions galoisiennes de $\mathbb{Q}$.

e) Montrer que K est une représentation linéaire sur $\mathbb{Q}$ de G.

f) Calculer χ_{K}. En déduire que K est G-isomorphe à la représentation régulière de G : $\mathbb{Q}\mathrm{G}$.

g) Montrer qu'une sous-extension L de K est un sous-G-module de K si et seulement si L est une extension galoisienne de $\mathbb{Q}$.

h) Déterminer pour chacune des sous-extensions galoisiennes L de K les multiplicités des G-modules irréductibles dans L.

On rappelle pour cela que $\mathfrak{S}_3$ admet trois représentations irréductibles sur $\mathbb{Q}$ et que la table de caractère est donnée par

	id	Transposition	$3-$cycle
1	1	1	1
ε	1	-1	1
V	2	0	-1

i) Montrer que $\mathbb{Q}(j)$ est un sous-G-module de K. Déterminer tous les sous-G-modules de $\mathbb{Q}(j)$.

Exercice 3 – Un théorème de Burnside. Soit $n \in \mathbb{N}^*$. On note ζ_n une racine n^{e} primitive de l'unité dans $\mathbb{C}$ (c'est-à-dire un élément d'ordre exactement n dans le groupe $\mathbb{C}^\times$).

a) Montrer que $\mathbb{Q}(\zeta_n)$ est une extension galoisienne de $\mathbb{Q}$.

b) Soit $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Montrer qu'il existe m premier avec n tel que $\sigma(\zeta_n) = {\zeta_n}^m$.

c) En déduire un morphisme injectif de groupes de $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

On considère à présent un groupe fini G de cardinal n et χ un caractère de G sur $\mathbb{C}$ et on définit

$$\mathrm{N}(\chi) = \prod_{g \in \mathrm{G}} |\chi(g)|^2$$

d) Montrer que, pour tout $g \in \mathrm{G}$, $\chi(g) \in \mathbb{Q}(\zeta_n)$ et que $\chi(g)$ et $\overline{\chi(g)}$ sont entiers sur $\mathbb{Z}$.

e) En déduire que $\mathrm{N}(\chi)$ est entier sur $\mathbb{Z}$.

f) Montrer que si m est premier avec n alors l'application $g \mapsto g^m$ est une bijection de G.

g) En déduire que $\sigma(\mathrm{N}(\chi)) = \mathrm{N}(\chi)$ pour tout $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

h) En déduire que $\mathrm{N}(\chi) \in \mathbb{Q}$ puis que $\mathrm{N}(\chi) \in \mathbb{N}$.

On suppose à présent que χ est un caractère **irréductible** de G et on rappelle l'inégalité arithmético-géométrique qui découle immédiatement de la stricte concavité de la fonction ln : soit $(a_1, \ldots, a_n) \in \mathbb{R}_+$ alors

$$\frac{a_1 + \cdots + a_n}{n} \geqslant (a_1 \cdots a_n)^{1/n}$$

avec égalité si et seulement si $a_1 = \cdots = a_n$.

i) Montrer que $\mathrm{N}(\chi) \leqslant 1$ avec égalité si et seulement si $|\chi(g)| = 1$ pour tout $g \in \mathrm{G}$.

j) En déduire que si χ n'est pas un caractère linéaire alors χ s'annule en un élément de G.