Université Paris 7-Denis Diderot
Licence de mathématiques et informatique

Algèbre et Géométrie
Année 2002-03
M. Fouquet, L. Merel

EXAMEN du 16 juin 2003

Durée : 3 h

L'usage des calculatrices, téléphones et de tout document est interdit.

I

Considérons le groupe symétrique $\mathcal{S}_4$ formé par les permutations de l'ensemble $\{1,2,3,4\}$. À titre de rappel, on note $(abcd)$ (resp. $(ab)(cd)$) l'élément σ de $\mathcal{S}_4$ qui vérifie $\sigma(a)=b$, $\sigma(b)=c$, $\sigma(c)=d$ et $\sigma(d)=a$ (resp. $\sigma(a)=b$, $\sigma(b)=a$, $\sigma(c)=d$ et $\sigma(d)=c$) etc. On rappelle que le support d'une permutation σ est $\{x\in\{1,2,3,4\}/\sigma(x)\neq x\}$.
1. Combien $\mathcal{S}_4$ a-t-il d'éléments ? Combien a-t-il d'éléments d'ordre 2, 3, 4, 5, 6 ?
2. On appelle double transposition de $\mathcal{S}_4$ la permutation obtenue comme composée de deux tranpositions de supports disjoints. Combien $\mathcal{S}_4$ a-t-il de doubles transpositions ?
3. Démontrer que le produit de deux doubles transpositions est une double transposition ou l'identité.
4. Donner la liste des éléments du groupe D engendré par les doubles transpositions. Quelles sont leurs signatures ? Le groupe D est-il contenu dans un sous-groupe de $\mathcal{S}_4$ autre que D et $\mathcal{S}_4$ lui-même ?
5. Démontrer que le sous-groupe D est distingué dans $\mathcal{S}_4$.

II

Soit un carré du plan euclidien, de sommets A, B, C et D. On appelle isométrie (resp. déplacement) du carré une isométrie (resp. un déplacement) du plan laissant stable l'ensemble de ces sommets.
1. Démontrer que les isométries (resp. les déplacements) du carré forment un groupe, noté G (resp. G^+).
2. Donner la liste des éléments de G et de G^+.
3. Démontrer qu'on a un homomorphisme de groupes $\phi : G \to \mathcal{S}_4$, obtenu en restreignant à $\{A,B,C,D\}$ (et en identifiant $\{A,B,C,D\}$ à $\{1,2,3,4\}$).
4. L'homomorphisme ϕ est-il injectif ? Son image contient-elle le groupe D étudié en **I** ? Est-il surjectif ?

III

Soit m un entier >1. Soit ζ un élément de $\mathbf{C}^*$ d'ordre m. Pour p nombre premier, on pose $\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$.
1. Démontrer que les racines du polynôme X^m-1 sont distinctes dans $\mathbf{C}$.
2. Soit $P_0\in\mathbf{Z}[X]$ un polynôme unitaire de degré minimal tel que $P_0(\zeta)=0$. Démontrer que P_0 divise le polynôme X^m-1 dans $\mathbf{Z}[X]$. Posons $X^m-1=P_0P_1...P_r$, où P_0,...P_r sont irréductibles dans $\mathbf{Z}[X]$.
3. Soit p un nombre premier ne divisant pas m. Démontrer que ζ^p est un zéro de X^m-1, puis qu'il existe $i\in\{0,1,...,r\}$ tel que $P_i(\zeta^p)=0$. En déduire que le polynôme P_0 divise $P_i(X^p)$.
4. Soit k un corps contenant $\mathbf{F}_p$ comme sous-corps. Quelle est la caractéristique de k ? Démontrer que les racines du polynôme X^m-1 (vu dans $k[X]$) sont distinctes dans k.
5. Notons $\bar{P}_0$,...$\bar{P}_r$ les images de P_0,...P_r dans $\mathbf{F}_p[X]$. Démontrer que les racines de $\bar{P}_0$,...$\bar{P}_r$ dans k sont distinctes.
6. Démontrer que $\bar{P}_0$ divise $\bar{P}_i(X^p)$ dans $\mathbf{F}_p[X]$. En déduire que si $\zeta_p\in\mathbf{F}_p$ est un zéro de P_0, on a $P_i(\zeta_p^p)=0$.
7. Démontrer que $\bar{P}_i(X^p)=\bar{P}_i(X)^p$. En déduire que $\bar{P}_i(\zeta_p)=0$, puis que $P_0=P_i$.
8. Démontrer que, pour tout entier a premier à m, on a $P_0(\zeta^a)=0$. En déduire que le degré de P_0 est $\geq\phi(m)$, où ϕ est la fonction d'Euler, c'est-à-dire on a $\phi(m)=$ ordre de $(\mathbf{Z}/m\mathbf{Z})^*$.