Université Paris 7-Denis Diderot
Maîtrise de mathématiques et informatique

Algèbre
Année 2004-05
L. Merel - P. Perrin

EXAMEN PARTIEL du 14 décembre 2004

Durée : 2 h

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

Soit q une puissance d'un nombre premier. Soit $\mathbf{F}_q$ un corps à q éléments. On rappelle que le groupe $PSL_2(\mathbf{F}_q)$ est $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbf{F}_q)/\det M = 1\}/\{\mathrm{id}, -\mathrm{id}\}$ et qu'il est d'ordre $q(q-1)(q+1)/2$.

I

1. Soit G un groupe d'ordre 360. Donner l'ordre de ses p-sous-groupes de Sylow, lorsque p parcourt les nombres premiers.
2. Quels sont, à isomorphisme près, les groupes d'ordre 360 qui sont abéliens ? Donner dans chaque cas les p-sous-groupes de Sylow.
3. Démontrer qu'un groupe d'ordre 360 possède un nombre n_3 de 3-sous-groupes de Sylow avec $n_3 \leq 40$. Démontrer que $n_3 \in \{1, 4, 10, 40\}$.
4. Donner des exemples de groupes d'ordre 360 qui ne sont pas abéliens. Y a-t-il parmi eux des produits semi-directs, des groupes alternés, des groupes de la forme $PSL_2(\mathbf{F}_q)$, où $\mathbf{F}_q$ est un corps à q éléments ? Indiquer parmi eux un groupe simple d'ordre 360.
5. Quels sont les éléments d'ordre 3 du groupe alterné $\mathcal{A}_6$? Quels sont les 3-sous-groupes de Sylow dans $\mathcal{A}_6$?
6. Montrer que, lorsque $a \in \mathbf{F}_9 - \{0\}$ la matrice $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ est d'ordre 3 dans $PSL_2(\mathbf{F}_9)$ et que les matrices de cette forme constituent (en adjoignant $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$) des sous-groupes d'ordre 9 de $PSL_2(\mathbf{F}_9)$. En déduire, en conjuguant les groupes qui viennent d'être considérés, que $PSL_2(\mathbf{F}_9)$ possède au moins 10 3-sous-groupes de Sylow, puis qu'il possède exactement 10 tels sous-groupes.

II

Soit $P \in \mathbf{Q}[X]$ un polynôme irréductible de degré 6. Soit L un sous-corps de $\mathbf{C}$ qui est un corps de décomposition de P sur $\mathbf{Q}$.

1. Montrer que l'extension $L|\mathbf{Q}$ est galoisienne.
2. Montrer que le groupe $\mathrm{Gal}(L/\mathbf{Q})$ opère sur les racines de P dans L. En déduire qu'il s'identifie à un sous-groupe du groupe symétrique $\mathcal{S}_6$.
3. Démontrer que la conjugaison complexe τ définit un élément d'ordre 2 de $\mathrm{Gal}(L/\mathbf{Q})$. Démontrer que c'est un produit de n transpositions, où $2n$ est le nombre de racines non réelles de P.
4. Si $\mathrm{Gal}(L/\mathbf{Q}) = \mathcal{A}_6$, montrer que P possède 2 ou 6 racines réelles.
5. Si $\mathrm{Gal}(L/\mathbf{Q}) = \mathcal{A}_6$, y a-t-il un élément d'ordre 6 dans $\mathrm{Gal}(L/\mathbf{Q})$?