UPMC
D. Bertrand

Master M1 de mathématiques 12-13
MM014 - Groupes finis

Examen partiel du 13 Mars 2013
Durée: 2 heures

L'usage du polycopié du cours et des feuilles d'exercices est autorisé.
Les 3 énoncés sont indépendants.

I (4 points)

On considère le groupe $G = (\mathbb{Z}/N\mathbb{Z})^*$, où $N = 2013$. On rappelle que 61 est un nombre premier.

1°/ Calculer l'ordre de G, et déterminer ses facteurs invariants.

2°/ Combien G a-t-il d'éléments d'ordre 3 ? d'ordre 5 ? d'ordre 2 ?

II (7 points)

Soit G un groupe d'orde 7×13^2. On note H un de ses 13-sous-groupes de Sylow, et K un de ses 7-sous-groupes de Sylow.

1°/ i) Calculer le nombre s_{13} de 13-Sylows de G.

ii) Montrer que G est un produit semi-direct $H \rtimes_\tau K$, où τ désigne un homomorphisme de K dans $Aut(H)$.

2°/ On suppose ici que $H \simeq \mathbb{Z}/13^2\mathbb{Z}$ est cyclique. Montrer que le produit semi-direct est direct, et que G est cyclique.

3°/ On suppose maintenant que $H \simeq (\mathbb{Z}/13\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z})$.

i) Calculer l'ordre du groupe $GL_2(\mathbb{F}_{13})$, et montrer qu'il existe au moins un groupe non commutatif G d'ordre 7×13^2.

ii) Calculer pour un tel groupe G le nombre s_7 de 7-Sylows de G.

III (10 points)

Soit p un nombre premier, $p \neq 2$. On considère le groupe $G = PGL_2(\mathbb{F}_p)$, quotient du groupe $GL_2(\mathbb{F}_p)$ par son centre $\mathbb{F}_p^*.\mathbf{I}_2 = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, \lambda \in \mathbb{F}_p^* \right\}$.

On note $X = \mathbb{P}_1(\mathbb{F}_p)$ l'ensemble des $(p+1)$ droites de l'espace vectoriel $(\mathbb{F}_p)^2$. Il est constitué de la droite $D_\infty = \mathbb{F}_p.\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et des droites $D_x = \mathbb{F}_p.\begin{pmatrix} x \\ 1 \end{pmatrix}$, où x parcourt $\mathbb{F}_p$. On identifie ainsi X à l'ensemble $\{0, 1, 2, .., p-1, \infty\}$ et le groupe symétrique $\mathbf{S}_X$ à $\mathbf{S}_{p+1}$, dont on note $\mathbf{A}_X = \mathbf{A}_{p+1}$ le sous-groupe des permutations paires.

1°/ Justifier brièvement les assertions suivantes.

i) L'action naturelle (à gauche) du groupe $GL_2(\mathbb{F}_p)$ sur l'espace vectoriel $(\mathbb{F}_p)^2$ induit une action de son quotient $G = PGL_2(\mathbb{F}_p)$ sur l'ensemble X.

ii) L'homomorphisme correspondant $\sigma : G \hookrightarrow \mathbf{S}_{p+1}$ est injectif.

On peut ainsi identifier G à un sous-groupe de $\mathbf{S}_{p+1}$. On se propose de caractériser les éléments g de G tels que $\sigma(g) \in \mathbf{A}_{p+1}$.

2°/ Soit t la classe dans G de la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

i) Calculer l'ordre de t dans G.

ii) Pour tout $x = 0, 1, ..., p-1, \infty$, déterminer l'image $D_y = t.D_x$ de D_x sous l'action de t. Combien t admet-il de points fixes ?

iii) Montrer que $\sigma(t)$ est un cycle, et qu'il appartient à $\mathbf{A}_{p+1}$.

3°/ Soient α un générateur du groupe cyclique $\mathbb{F}_p^*$, et γ la classe dans G de la matrice $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$.

i) Calculer l'ordre de γ dans G.

ii) Pour tout $x = 0, 1, ..., p-1, \infty$, déterminer l'image $D_y = \gamma.D_x$ de D_x sous l'action de γ. Combien γ admet-il de points fixes ?

iii) Montrer que $\sigma(\gamma)$ est un cycle, et qu'il n'appartient pas à $\mathbf{A}_{p+1}$.

4°/ Soit c la classe dans G de la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

i) Calculer l'ordre de c dans G.

ii) Pour tout $x = 0, 1, ..., p-1, \infty$, déterminer l'image $D_y = c.D_x$ de D_x sous l'action de c. Combien c admet-il de points fixes ?

iii) Montrer que $\sigma(c)$ appartient à $\mathbf{A}_{p+1}$ si et seulement si $p \equiv 1 \pmod{4}$.

5°/ On note $\mathbb{F}_p^{*2} = \{\lambda \in \mathbb{F}_p^*, \exists \mu \in \mathbb{F}_p^*, \lambda = \mu^2\}$ le sous-groupe de $\mathbb{F}_p^*$ formé par les carrés d'éléments de $\mathbb{F}_p^*$.

i) Montrer que le déterminant induit un homomorphisme $\delta : G \to \mathbb{F}_p^*/\mathbb{F}_p^{*2}$.

ii) Montrer qu'un élément λ de $\mathbb{F}_p^*$ est un carré si et seulement si $\lambda^{\frac{p-1}{2}} = 1$.

6°/ On admet que G est engendré par les trois éléments t, γ et c ci-dessus. Montrer que

$$\forall g \in G \ : \ \sigma(g) \in \mathbf{A}_{p+1} \Leftrightarrow \delta(g) = 1.$$

Esquisse de corrigé

I. 1/ $N = 3 \times 11 \times 61$, donc $|G| = \phi(N) = 2 \times 10 \times 60$. De plus, $G \simeq \mathbb{F}_3^* \times \mathbb{F}_{11}^* \times \mathbb{F}_{61}^* \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/10\mathbb{Z}) \times (\mathbb{Z}/60\mathbb{Z})$, et $2|10|60$, donc les facteurs invariants de G sont $\{2, 10, 60\}$.
2/ Par le lemme chinois, $G \simeq (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/4\mathbb{Z})$, donc G a $|\mathbb{F}_3^*| = 2$ éléments d'ordre 3, $card\{(\mathbb{F}_5)^2 \setminus 0\} = 24$ d'ordre 5, et $card\{(\mathbb{F}_2)^3 \setminus 0\} = 7$ d'ordre 2.

II. 1/ i) $s_{13} \equiv 1$ mod. 13 et $s_{13}|7$, donc $s_{13} = 1$. ii) Donc H est normal dans G, et G est le produit semi-direct (interne) $H \rtimes K$, où K agit sur H par conjugaison, i.e. $\tau(k) = Int(k)_{|H}$.
2/ $Aut(H) = (\mathbb{Z}/13^2\mathbb{Z})^*$, d'ordre 13×12, n'a pas d'élément d'ordre 7, donc le seul morphisme τ de K dans $Aut(H)$ est trivial, et $G \simeq H \times K$ est un produit direct. D'après le lemme chinois, on a alors $G \simeq \mathbb{Z}/(7 \times 13^2)\mathbb{Z}$.
3/ i) Cet ordre $(13^2 - 1)(13^2 - 13)$ est divisible par 7, donc $Aut(H) \simeq GL_2(\mathbb{F}_{13})$ admet par Cauchy un élément d'ordre 7, et il existe un morphisme non trivial τ de $(\mathbb{Z}/7\mathbb{Z})$ vers $Aut(H)$. Le produit semi-direct $G_\tau := (\mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/13) \rtimes_\tau (\mathbb{Z}/7\mathbb{Z})$ répond à la question. ii) $s_7 \equiv 1 \pmod 7$ divise 13^2, donc vaut 1 ou 169, et ne vaut pas 1, sans quoi G_τ serait abélien.

III. 1/ i) et ii) Par $\mathbb{F}_p$-linéarité, $GL_2(\mathbb{F}_p)$ envoie une droite de $(\mathbb{F}_p)^2$ sur une droite, d'où un morphisme $\breve{\sigma} : GL_2(\mathbb{F}_p) \to \mathbf{S}_X$. Une matrice admettant tout vecteur non nul pour vecteur propre est scalaire. Donc $Ker(\breve{\sigma}) = \mathbf{F}_p^*.\mathbf{I}_2$, et $\breve{\sigma}$ induit $\sigma : GL_2(\mathbb{F}_p)/(\mathbf{F}_p^*.\mathbf{I}_2) \hookrightarrow \mathbf{S}_X$.
2/ i) $t^p = 1$ et $t \neq 1$ donc t est d'ordre p. ii) $t.D_x = D_{x+1}$ pour $x \in \mathbb{F}_p$, et $t.D_\infty = D_\infty$, seul point fixe de t. iii) De la formule sur $t.D_x$, on déduit que $\sigma(t) = (0, 1, ..., p-1)$ est un cycle de longueur p (comme $\sigma(t)$ est d'ordre premier p et que $p + 1 < 2p$, cela se voit d'ailleurs directement), donc la signature de $\sigma(t)$ est $(-1)^{p-1} = 1$.
3/ i) γ est d'ordre $p - 1$. ii) $\gamma.D_x = D_{\alpha x}$ pour $x \in \mathbb{F}_p$, et $\gamma.D_\infty = D_\infty$, donc les seuls points fixes de γ sont D_0 et D_∞. iii) Comme α engendre $\mathbb{F}_p^* = X \setminus \{0, \infty\}$, la formule montre que $\sigma(\gamma)$ est le cycle $(1, \alpha, ..., \alpha^{p-2})$, dont la signature vaut $(-1)^{p-2} = -1$.
4/ i) c est d'ordre 2. ii) c permute D_0 et D_∞, tandis que pour $x \in \mathbf{F}_p^*$, on a $c.D_x = D_{1/x}$. Donc les seuls points fixes de c sont D_1 et $D_{-1} = D_{p-1}$. iii) Comme c permute les autres droites par couples, $\sigma(c)$ est le produit de $\frac{p-1}{2}$ transpositions, et appartient à $\mathbf{A}_X$ si et slt si ce nombre est pair, i.e. $p \equiv 1$ mod 4.
5/ i) Le déterminant d'une matrice scalaire est un carré. ii) L'ordre de λ divise $\frac{p-1}{2}$ si et slt si λ appartient à l'unique sous-groupe d'ordre $\frac{p-1}{2}$ du groupe cyclique $\mathbb{F}_p^*$. Ce sous-groupe est engendré par α^d, où $d = (p-1)/\frac{p-1}{2} = 2$, et coïncide donc avec $\mathbb{F}_p^{*2}$.
6/ Soit $\chi : \mathbf{S}_X \to \{\pm 1\}$ le morphisme de signature, et ε l'isomorphisme $\mathbb{F}_p/\mathbb{F}_p^{*2} \simeq \{\pm 1\}$. L'énoncé revient à montrer que les applications $\chi \circ \sigma$ et $\varepsilon \circ \delta$ de G dans $\{\pm 1\}$ coïncident. Comme ce sont des morphismes de groupes, il suffit de le vérifier sur un système de générateurs de G. D'après 2/ et 3/, on a bien $\chi(\sigma(t)) = 1 = \varepsilon(\delta(t))$ et $\chi(\sigma(\gamma)) = -1 = \varepsilon(\delta(\gamma))$ (car α n'est pas un carré). Enfin, d'après 4/, $\chi(\sigma(c)) = (-1)^{\frac{p-1}{2}}$, qui, d'après 5/, vaut 1 si et seulement si $-1 \in \mathbb{F}_p^{*2}$, i.e. si et slt si $\varepsilon(\delta(c)) = 1$.